Director of
Central
Intelligence

APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX

The APEX Special Access Control System

A Security Manual for Industry

Confidential

April 1980

Copy 128

National Security Information

Unauthorized Disclosure
Subject to Criminal Sanctions

25X1

Approved For Release 2005/07/12 : CIA-RDP85T00788R000100040001-9

April 1980

An effective date for beginning the use of the APEX Special Access System has not yet been established. This manual is available now—before the start date—in order to allow you to study it, ask questions about its content, and understand what you must do when a firm date for the initiation of the APEX system is established. You will be told when to start to use the manual by your normal chain of command.

Questions about the content of this manual may be directed to the nearest control or security officer for whatever existing SCI system governs your working area or your current access to compartmented intelligence.

The above information is Unclassified.

This manual sets forth the US Government's procedures for safeguarding extra sensitive materials in industry. As such, it merits and warrants the overall classification of CONFIDENTIAL in its totality. Individual paragraphs may be excised for use at the unclassified level.

Contents

The APEX Special Access Control System

Introduction

1. This manual describes the Special Access 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. (U)

2. This manual will serve as the basic guide for the control of APEX material in industrial facilities. 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directives and regulations governing the protection and control of Sensitive Compartmented Information (SCI) will be superseded or revised, if necessary, to be in accordance with this manual.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 consistent with this manual. (U)

3. 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. (U)

Organizational Structure

4. Senior Intelligence Officers of the Intelligence Community, program managers, 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. Whenever the term SIO is used in this manual, it means the SIO or his/her designated representative unless it is specifically stated that the responsibility must personally be performed by the SIO. (U)

5. 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. Copies of such directives will be provided to the APEX Steering Group. (U)

6. 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 Special Access Control System. (U)

7. To assist in carrying out the precepts dictated by the APEX Special Access 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 at the appropriate management echelon to ensure executive-level support within each firm. 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. (U)

8. SIOs are responsible for the establishment, accreditation, and annual inspection 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. Government guidance and assistance should be solicited prior to construction of a CACF. (U)

9. All APEX information will be transmitted and maintained within the APEX Special Access Control System. Compartmentation within the system will be denoted by the use of terms identifying categories of product information (e.g., COMINT, HUMINT, IMAGERY, TECHNICAL) and by project codewords which refer to collection activities. (U)

Description of System

General

10. 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. (U)

Access to APEX Special Access Control System

11. There are three basic requirements for individual access to the APEX Special Access Control System:

A. 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.

B. Favorable adjudication by the SIO of the appropriate Government Sponsor that the nominee meets uniform personnel security criteria and investigative requirements set forth in this manual and DCID 1/14.

C. 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 US Government Sponsor. (U)

Revalidation of Access

12. It is the responsibility of each US Government Sponsor to maintain a continuous review of access approvals to ensure that only those contractor 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. (U)

Termination of Access

13. 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. At that time, each individual will be required to account for and surrender all APEX materials. The responsible SIO will be notified of all terminations of access. (U)

14. When an individual leaves one firm to join another, he/she will be debriefed from all APEX accesses. (U)

Access Approvals

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

Responsibilities of Contractor APEX Control and Security Officers

Basic Duties/ Responsibilities of Contractor APEX Control Officers

16. Contractor APEX Control Officers are to administer the APEX Special Access Control System within their firms and will:

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

B. 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.

C. 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.

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

E. Provide advice and guidance on the proper classification levels, codewords, and caveats within the APEX Special Access Control System.

F. Perform such other duties as might be required. (U)

Basic Duties/ Responsibilities of Contractor APEX Security Officers

17. Contractor APEX Security Officers are responsible for all security aspects of the APEX Access Control System within their firms and will:

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

B. Maintain current listings of all APEX-accessed individuals within their jurisdiction, and which APEX contract(s) they support.

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

D. When authorized conduct required security indoctrinations and debriefings of personnel approved for APEX access and obtain signed Nondisclosure and Termination Secrecy Reminders as necessary.

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

F. 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.

G. 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.

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

I. Perform such other duties as might be required. (U)

Security Standards for Access Approval

Need-to-Know Policy

18. Access to the APEX Special Access 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 approving 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. (U)

Personnel Security Standards

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

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

B. 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:

(1) 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.

(2) 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. (U)

20. Prior to security approval and indoctrination of an individual into the APEX Special Access Control System, the nominee must have a complete background investigation and meet the additional provisions of DCID 1/14 which specifies the investigative and personnel security criteria for access to sensitive compartmented information. (U)

Reinvestigations

21. Programs will be instituted requiring the periodic reinvestigation of personnel provided access to APEX information in accordance with DCID 1/14. 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. (U)

Changes in Personal Status

22. Responsible officials must take into consideration any change in personal status that may have a bearing on the continuing eligibility of individuals approved for access to APEX material. Name changes (resulting from marriage, divorce, or court decree) must be reported to the appropriate US Government ACO/ASO. (U)

Contacts or Associations With and Marriages To Foreign Nationals

23. 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 US Government Sponsor through the Contractor APEX Security Officers:

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

    B. Close and continuing or any regular, frequent nonofficial contact with any other foreign national. (U)

24. 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 US Government Sponsor through the Contractor APEX Security Officer. Failure to report such contact may result in withdrawal of access to APEX material. (U)

25. 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 in accord with DCID 1/14 before there is any determination that a waiver of standards might be made to continue the approved person in APEX-indoctrinated status. (U)

Travel Restrictions

26. ***Unofficial Travel.*** Persons granted authorization for access to certain categories of extremely sensitive information on foreign intelligence sources and methods protected by the APEX Special Access 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 (DCID 1/20). 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 extremely sensitive information on foreign intelligence sources and methods. (U)

27. The CACO/CASO shall advise all persons having access to APEX information who plan unofficial travel to or through designated countries that they 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 US Government Sponsor through their Contractor APEX Security Officer, any incidents of potential security concern that occurred during the trip. (U)

28. ***Official Assignment/Travel.*** No person with access to APEX information will be assigned to or directed to participate in hazardous activities (as defined in DCID 1/20) until he/she has been afforded a defensive security briefing and/or risk-of-capture briefing as applicable. (U)

29. ***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. (U)

Factors Governing Contractor Access

Factors Considered in Selection of Contractor Firms

30. 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 and inspect 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. (U)

Restrictions on Access

31. 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. (U)

Types of Access

32. Within the APEX Special Access 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). (U)

33. 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 DCID 1/14 and must withstand strict need-to-know tests. (U)

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

A. ***Administrative Access Approval.*** Personnel who do not require substantive access to individual APEX compartments, but who require physical access to APEX-accredited areas or who administratively process APEX materials, will be given an administrative access called APEX-GENERAL. The APEX-GENERAL access may be given in two phases:

(1) Phase I accesses will accommodate those personnel who must have physical access to APEX areas but who do not need to see or process clear text APEX materials. Guards, couriers carrying APEX materials in sealed pouches, technical personnel such as switching center and computer technicians, are examples of types of personnel who might require Phase I access.

(2) Phase II accesses will accommodate those personnel who process substantive clear text APEX materials in an administrative capacity. Examples of such personnel include secretaries, distribution personnel, communications center and ADP output device operators, and document control personnel. (U)

35. 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. (U)

36. 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. (U)

37. ***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. (U)

38. ***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. (U)

39. ***APEX (Operational Subcompartment) - ALPHA.*** In addition to the above-cited phases of access, it is envisioned 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. (U)

40. ***APEX (Generic Product).*** The product resulting from operational collection projects will be identified within the APEX Special Access Control System by its generic term. Specific access approval will be required for each of the four generic categories of APEX products. 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. (U)

Physical Security

Construction and Protection Standards

41. All APEX materials held by contractors must be stored in Contractor APEX Control Facilities. These standards for construction and protection of CACFs will be as prescribed in Physical Security Standards for Sensitive Compartmented Information Facilities, dated 30 April 1973 or other such guidelines that may supersede it. (U)

Accreditation of CACFs

42. Before an industrial facility is authorized to handle APEX material, it must be inspected and certified by the appropriate US Government Sponsor as having met the aforementioned construction and protection standards. Actions concerning accreditation of CACFs will be reported to the APEX Control Staff by the US Government Sponsor. (U)

Inspections

43. Periodic inspection of CACFs is mandatory and must be done at least annually. Inspections are to be performed by designated government APEX security officers experienced in conducting security inspections for the control and storage of APEX materials and will assure that procedures and physical 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 inventory of APEX documents of such scope to ensure that accountability and control are being maintained. Failure to locate any such documents will be reported on a priority basis. (U)

Colocation Within Facilities

44. 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 among 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. (U)

Emergency Destruction and Evacuation Planning

45. Each CACF must maintain an emergency plan approved by the responsible government APEX security officer. 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. (U)

Personnel Access Controls

46. 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 Government APEX security officer who has original cognizance over the facility. Access to CACFs by uncleared visitors must be approved in advance by the cognizant US Government Sponsor 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. A visitor control log including the visitor's name and affiliation; date and time of entry/exit; purpose of visit; and point of contact will be maintained and retained by each CACO/CASO. (U)

Two-Person Rule

47. To provide security and safety protection to APEX materials, all CACFs will be occupied by at least two APEX indoctrinated persons when in use. Persons selected to work in such areas will be chosen on the basis of proven reliability and maturity. (U)

Technical Security *

Technical Security Countermeasures Inspections

48. Technical Security Countermeasures Inspections will be conducted as part of the accreditation process of a CACF and following major physical renovations. Reinspections will be scheduled by the cognizant SIO who will also ensure that personnel assigned to CACFs are briefed concerning the threat of technical penetration. (U)

Computer Security

49. All automatic data-processing equipment used in CACFs will be operated in compliance with DCID 1/16 (Security of Foreign Intelligence in Automated Data-Processing Systems and Networks). No APEX or APEX-related information is to be processed before approval by the responsible SIO. (U)

Compromising Emanations Control (TEMPEST Security)

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

Access Approval Certifications

General Guidelines

51. The responsible SIO, normally acting through the ASO, is the 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 neccessity of visit requirements have been established. (U)

Visits to/by Contractors

52. APEX-related visits will not be undertaken to/by the contractor without the approval of the cognizant government APEX contract authority. 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 not exceeding one year may be authorized. Visit certifications are to be made in writing, either by

* All requirements for technical security approvals are in addition to physical security approvals outlined in this manual. (U)

letter or secure communications circuits, or otherwise as directed by the program manager. (U)

Information Updates

53. A critical need of the APEX Special Access 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 CACO/CASOs must provide timely information on changes in the status of their personnel to the US Government Sponsor. These updates will also ensure that all briefing or debriefing actions are recorded as soon as possible. (U)

Security Classification and Control Guidelines

Basic Guidance

54. 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. (U)

Decompartmentation Sanitization

55. Contractors are not authorized to decompartment or sanitize APEX materials. CACO/CASOs may request or make recommendations for decompartmentation or sanitization of specific materials if essential to contract performance. (U)

Control Standards and Procedures

Classification Levels

56. Information in the APEX Special Access Control System will be classified and use of derivative classification will be 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. The following terms used in this system are unclassified when standing alone or not connected to the intelligence activities or intelligence information they designate: APEX; the APEX Special Access Control System; the codewords which identify the categories or intelligence product within the system (i.e., COMINT, HUMINT, IMAGERY, TECHNICAL). Project identifiers may be used outside the APEX control system, but must be protected by the standard classification level of CONFIDENTIAL or SECRET. 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. (U)

Classification Guides

57. 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. (U)

Labeling

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

A. ***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.

B. ***Control System Caveats.*** All documents controlled within the system will be marked "HANDLE VIA APEX 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.

C. ***Codewords and Indicators.*** Codewords for operational projects and product indicators will be placed following or below the classification marking on the front and back covers (if any), top and bottom of the title page (if any), first page, and each page which contains information requiring specific codeword/indicator protection.

D. ***Control Numbers.*** APEX control numbers for hard copy documents generated by contractors will be directed by the US Government Sponsor. They will consist of the letter "A", a three-digit number identifying the contractor, a dash, a five-digit assigned number, a slant or oblique stroke, and the last two digits of the current year; e.g., A123-12345/80. A sequential ("one up") system, beginning with 00001 each year for each contractor, will be used as the assigned number. The control number 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 the document. Copy numbers of individual documents will be reflected as Copy __ of __ on the cover and first page of the document. Copy numbers of finished publications may be shown as Copy __ on the cover sheet, cover (if any), and first page. Electrical messages will be excluded from the requirement for APEX Control Numbers.

E. ***Classification Review Notice.*** APEX materials are classified for a period of 20 years (except for foreign government information which will remain protected for 30 years). The following Classification 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 government authority)
REVIEW ON: (indicate date, 20 or 30 years from date of issuance)
REASON FOR EXTENDED CLASSIFICATION: APEX 59E
The abbreviation "REVW (date 20/30 yrs)" may be substituted in electrically transmitted messages.
If derivative classification, use the following format:
DERIVATIVE CL BY _____
REVIEW ON _____
DERIVED FROM (source document or classification guide citation)

F. ***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. The classification and handling controls for 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. (U)

Pouching and Transmittal Requirements

59. 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 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. Special contracting relationships with unique security requirements may be arranged by US Government Sponsors or program managers. Such arrangements must be approved by the appropriate SIO and coordinated with the APEX Steering Group. (U)

60. 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. (U)

61. 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. This container will be marked:

* Does not apply to ARFCOS. (U)

PROPERTY OF THE US GOVERNMENT

DO NOT OPEN

If found call: (insert Phone No.) Collect

(city/state)

62. 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. (U)

Electrical Transmissions

63. 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. (U)

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

65. 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. (U)

66. 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. (U)

Cover Sheets

67. An APEX 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.

A. TOP SECRET APEX hard copy material will be covered with unique cover sheets. There are cover sheets for TOP SECRET APEX *publications* which incorporate on the reverse side a dissemination control log and a certification of destruction. There are cover sheets for TOP SECRET APEX *documents* (less formal issuance than publications) which incorporate on the front of the cover sheet a dissemination control log and a certificate of destruction.

B. There are separate cover sheets for TOP SECRET documents and publications.
Operational compartments (Yellow)
Operational subcompartments (Brown)
Product compartments (Red)

C. SECRET and CONFIDENTIAL level APEX material will be covered with a Gray cover sheet.

D. Cover sheets need not be used on electrical transmissions or on hard copy material that does not leave an APEX facility.

E. Samples of the cover sheets are at Enclosure I. Cover sheets are available through the US Government Sponsor. (U)

Destruction

68. As soon as possible after its purpose has been served, all APEX 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 degaussed or destroyed only by equipment specifically approved by the contracting authority. (U)

Reproduction

69. Reproduction of APEX material will be subject to the restrictions and procedures established by the responsible SIO. 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. (U)

70. Reproduction of all hard copy APEX materials within the APEX Special Access Control System requires the consent of the originator, and shall be accomplished by the CASO or ACASO following procedures approved by the US Government Sponsor. (U)

Accountability

71. 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. (U)

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

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

74. Reports of discrepancies will be provided immediately to the responsible US Government Sponsor. The CASO will initiate a search for all of the missing documents and the Sponsor will conduct an investigation. (U)

75. CACOs will keep a record of all APEX-numbered material received by or dispatched from 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 or dispatched APEX materials will be retained for two years. Records of incoming or dispatched TOP SECRET APEX documents will be detroyed five years after the documents are transferred, downgraded, or destroyed. (U)

76. Working materials containing APEX-controlled information that are used and retained exclusively within a CACF—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. If they are to be removed from the CACF they will be controlled as regular APEX materials. (U)

77. Contractors or consultants will not distribute APEX materials outside a CACF without the permission of the contract monitor or the responsible SIO. (U)

Procedures for Control of Specialized Hard Copy Documents

Automatic Data Processing:

78. 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 Special Access Control System markings, and other required APEX caveat designators. To the extent possible, other ADP-related media will be similarly marked. (U)

Film/Photographic Materials

79. Roll film, flats, slides, or other forms of photographic negatives or positives used for photographic interpretation are considered raw intelligence data and need not be subject to individual accountability controls, but must be labeled as to security classification and controlled under APEX control procedures. (U)

80. Labels on roll film placed in opaque containers will be located as follows:

    A. One on end of spool flange.

    B. One on side of spool container.

    C. One on container cover. (U)

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

82. The film itself will include all APEX control system markings on the heading and tail identification. (U)

Microfiche

83. Each microfiche will have a heading whose elements are readable without magnification. The heading elements will specify: the long and short titles of the documents; security classification and codewords, which will not be abbreviated; and standard abbreviations or codes for handling caveats, APEX control numbers, copy numbers, dissemination control marking, 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. (U)

Microfilm

84. Each role of microfilm, whether mounted on an open reel or in a cartridge, will contain security information which is readable without magnification. 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. (U)

Raw Data

85. Bulk receipts will be used on raw data that is dispatched to or from any ACF or CACF via the APEX CONTROL SYSTEM. (U)

Security Violations/Compromises

Responsibility to Report

86. 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 primary focus is to determine the damage to the nation's security and secondly to ascertain management or individual actions to minimize recurrence. The cognizant government ASO is to be notified in a timely fashion of both the incident and the results of the investigation of it. (U)

Investigative Responsibility

87. 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. (U)

88. 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. (U)

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

90. 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. (U)

Corrective Action

91. 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. (U)

Security Education

General

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

Initial Indoctrination

93. Personnel are to be indoctrinated by a designated ASO. The indoctrination will cover:

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

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

C. The administrative, physical, and other procedural security requirements of the APEX Special Access Control System.

D. Individual classification management responsibilities of personnel in the APEX system, including classification guidelines and marking requirements.

E. The criminal penalties for espionage and unauthorized disclosure.

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

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

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

(1) The prohibition against disclosing any classified information to unauthorized persons, with special emphasis upon nonsecure telephones and nonsecure places.

(2) Procedures to determine that prospective recipients are approved for access.

(3) 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.

(4) The requirement for prior review of public speeches or writings related to work done or in progress involving APEX compartmented materials or materials from predecessor programs.

I. Execution of a Nondisclosure Secrecy Agreement. (U)

Continuing Security Programs

94. Security education programs will be established as directed by the US Government Sponsor to ensure that persons granted access to APEX material are periodically instructed as to its unique sensitivity and their personal responsibility for protection of APEX materials. (U)

Termination of Access

95. 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:

A. 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.

B. 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.

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

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

E. A reminder of the risks associated with hazardous activities.

F. Execution of a Termination of Access/Security Reminder. (U)

Glossary

APEX Control Facility (ACF)
A formally accredited area, room, group of rooms, or installation where APEX material may be stored, used, discussed, and/or electrically processed. Procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular APEX material authorized for use or storage within the ACF.

APEX Control Officer (ACO)
The US Government–designated individual charged with responsibility for administration of the APEX Special Access Control System. SIOs will appoint or cause to be appointed ACOs and alternates to administer the system within their organizations and jurisdictions.

APEX Control Staff
A staff of professionals supporting the APEX Steering Group and the DCI in establishing and operating a single Community special access system for national foreign intelligence (APEX).

APEX Security Officer (ASO)
The US Government–designated individual charged with responsibilty for all security aspects of the APEX Special Access Control System. SIOs will appoint or cause to be appointed ASOs and alternates to enforce APEX security within their organizations and jurisdictions.

APEX Special Access Control System
A system which provides for the security control of Special Access Programs within the category of national security information called National Foreign Intelligence. It includes collection programs, its product categories of COMINT, HUMINT, IMAGERY, and TECHNICAL Intelligence, and especially sensitive material in the ROYAL category.

Codeword
Generally a word or term which conveys a prearranged meaning other than the conventional one.

Compartmentation
Formal systems of restricted access established and/or managed by the Director of Central Intelligence (DCI) to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs.

Contractor APEX Control Officer (CACO)
The contractor-employed individual charged with responsibility for administration of the APEX Special Access Control System within his firm. Appointments of CACOs will be approved by the cognizant US Government Sponsor.

Contractor APEX Security Officer (CASO)
The contractor-employed individual charged with responsibilty for all security aspects of the APEX Special Access Control System within his firm. Appointment of CASOs will be approved by the cognizant US Government Sponsor.

Decompartmentation
The removal of information from a compartmentation system without attempting to conceal the generic source.

Defensive Security Briefing
Formal advisories which alert personnel to the potential for harassment, provocation, or entrapment while traveling within hazardous areas. They should be based on actual experience when available, and include information on courses of action helpful in minimizing adverse security and personal consequences.

Document
Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data-processing cards and tapes, maps, charts, paintings, drawings, photos, engraving, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form. In the context of this manual, publications are documents which have been produced by a printing plant.

Executive Agent
Within the meaning of this manual, that person, organization, or entity which functions on behalf of another in the accomplishment of specific intelligence tasks mandated by higher government authority.

Executive Agent Program
A program wherein a single department, agency, or organization collects or processes foreign intelligence for the Intelligence Community at the direction of the DCI or higher national authority.

Foreign Government Information
Information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement

requiring confidentiality with, a foreign government or international organization of governments. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record.

Hard Copy Document
Any document that is initially published and distributed by the originating component in paper form and that is not stored or transmitted by electrical means.

Hazardous Activities
Hazardous activities include assignments or visits to, and travel through, countries listed in DCID 1/20. Hazardous activities also include assignment or travel in combat zones or other areas where hostilities are taking place, duties behind hostile lines, and duties or travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action.

Intelligence Sources and Methods
A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support US intelligence activities.

National Collection Program
A program wherein a single department, agency or organization collects or processes foreign intelligence for the Intelligence Community at the direction of the Director of Central Intelligence (DCI) or higher national authority.

National Foreign Intelligence
Information collected about foreign entities collected by or in the name of the DCI to satisfy national level policymakers. It includes the means and sources through which this information is collected. It does not include departmental efforts to collect information to satisfy needs unique to their mission. It recognizes a difference between classified defense materials and classified national level information.

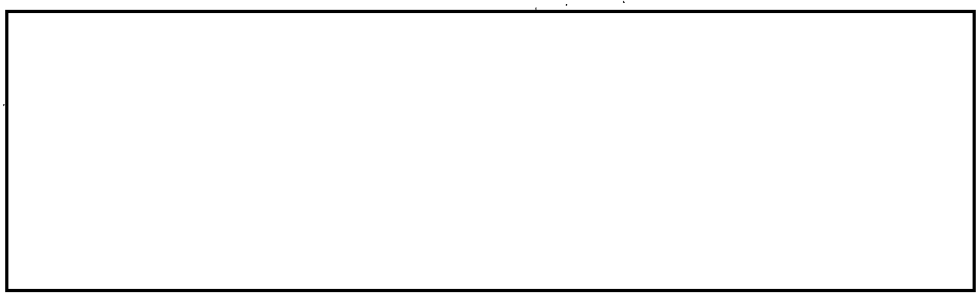
Operational Compartments
Within the APEX Security Control System, those collection activities which deal with proposed, developing, or functional foreign intelligence collection operations. Included within the definition are all policy, planning, research development contracting, systems operations, budgeting, and mission-related data.

Operational Subcompartments
A special category created to give analysts, processors, tasking officers, and resource managers access to specified operational project data needed to perform their jobs.

Product Compartments
Intelligence resulting from APEX-controlled collection activities which is segregated into generic categories of information. Product includes some raw data and intelligence information as well as finished intelligence such as estimates, reports, and other written matter.

Program Manager/Director
The head of an operational activity which collects or processes foreign intelligence for the Intelligence Community at the direction of the Director of Central Intelligence (DCI) or higher national authority.

Release of Classified Intelligence
For the purpose of this directive, release is the authorized visual, oral, or physical disclosure of classified intelligence.



25X

Sanitization
The concealment of sensitive intelligence sources, methods, and analytical procedures to permit dissemination of information outside of compartmentation systems.

Sensitive Compartmented Information (SCI)
The term SCI means all information and material bearing special controls for restricted handling within compartmented foreign intelligence systems. The term does not include Restricted Data as defined in the Atomic Energy Act of 1954, as amended.

Sensitive Sources, Methods, and Analytical Procedures
Those aspects of foreign intelligence collection, processing, or exploitation activities which are vulnerable to hostile actions that nullify or curtail their effectiveness or continuing productivity.

Senior Intelligence Officer (SIO)
For purposes of implementing the APEX Special Access Control System, the SIOs are defined as those senior principals and observers to the NFIB who head intelligence organizations or intelligence producing agencies within the Intelligence Community. For purposes of expediency and workability, the principals may delegate this authority to other persons within their organization.

Technical Surveillance Countermeasures (TSCM) Inspections
A thorough physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and physical security weaknesses. TSCM inspections differ from TEMPEST surveys in that the latter are limited to investigation and studies of compromising emanations whereas the TSCM inspections are basically designed to prevent or discover the technical penetration efforts of hostile intelligence services.

TEMPEST Security Inspections
A thorough technical investigation and study of compromising electromagnetic emanations through the use of sensitive electronic listening devices and recorders.

US Government Sponsor
In the context of this manual, that US Government office which has designated responsibility for the contract.

This glossary is Unclassified

Enclosure I-A

Controlled Publication

APEX operational publication cover sheet (front). Cover sheet for use with APEX operational publications. Project name(s)/ codeword(s)/product indicator(s) will be placed as shown. Cover sheet stock is unclassified. Cover sheets are classified when classified project name(s), codeword(s), and/or titles are affixed.

APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX

(Publication Title Goes in this Position)

Top Secret

Control Number A-00000000/80

This is an APEX publication Restricted to those approved for access to:

_____ _____ _____

[*Project Name(s) / Codeword(s) / Product Indicator(s)*]

Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign on the reverse side and maintain a record of its internal dissemination. Each indviidual who sees this document will also sign and indicate the date of handling.

Handle via APEX Control System

Top Secret

Pub. No. 00-00000
Day Month Year
Copy

See overleaf for opposite side of this sheet.

Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination.
Each individual who sees this document will also sign and indicate the date of handling.

Unit	Signature	Date Rec'd	Released

Certification of Destruction
When document is destroyed, this control sheet may be kept or returned to the originator and be destroyed when five years old.

Destroyed by (Signature) Witnessed By (Signature)

Unit Date

APEX operational publication cover sheet (rear) with integral dissemination control log and certificate of destruction.

Enclosure I-B

APEX operational document cover sheet (front). Cover sheet for use with APEX operational documents. Project name(s)/ codeword(s)/product indicator(s) will be placed as shown. Cover sheet stock is unclassified. Cover sheets are classified when classified project name(s) or codeword(s) is/(are) affixed.

Controlled Document

APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX

Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination

Each individual who sees this document will also sign and indicate the date of handling

To: Name and Location Date

From:

Top Secret

Control Number

Copy **of**

Date

This is an APEX document Restricted to those approved for access to:

[*Project Name(s) / Codeword(s) / Product Indicator(s)*]

Certification of Destruction
When document is destroyed, this control sheet may be kept or returned to the originator and be destroyed when five years old.

Destroyed By (Signature) Witnessed By (Signature)

Unit Date

Handle via APEX Control System

Top Secret

See overleaf for opposite side of this sheet.

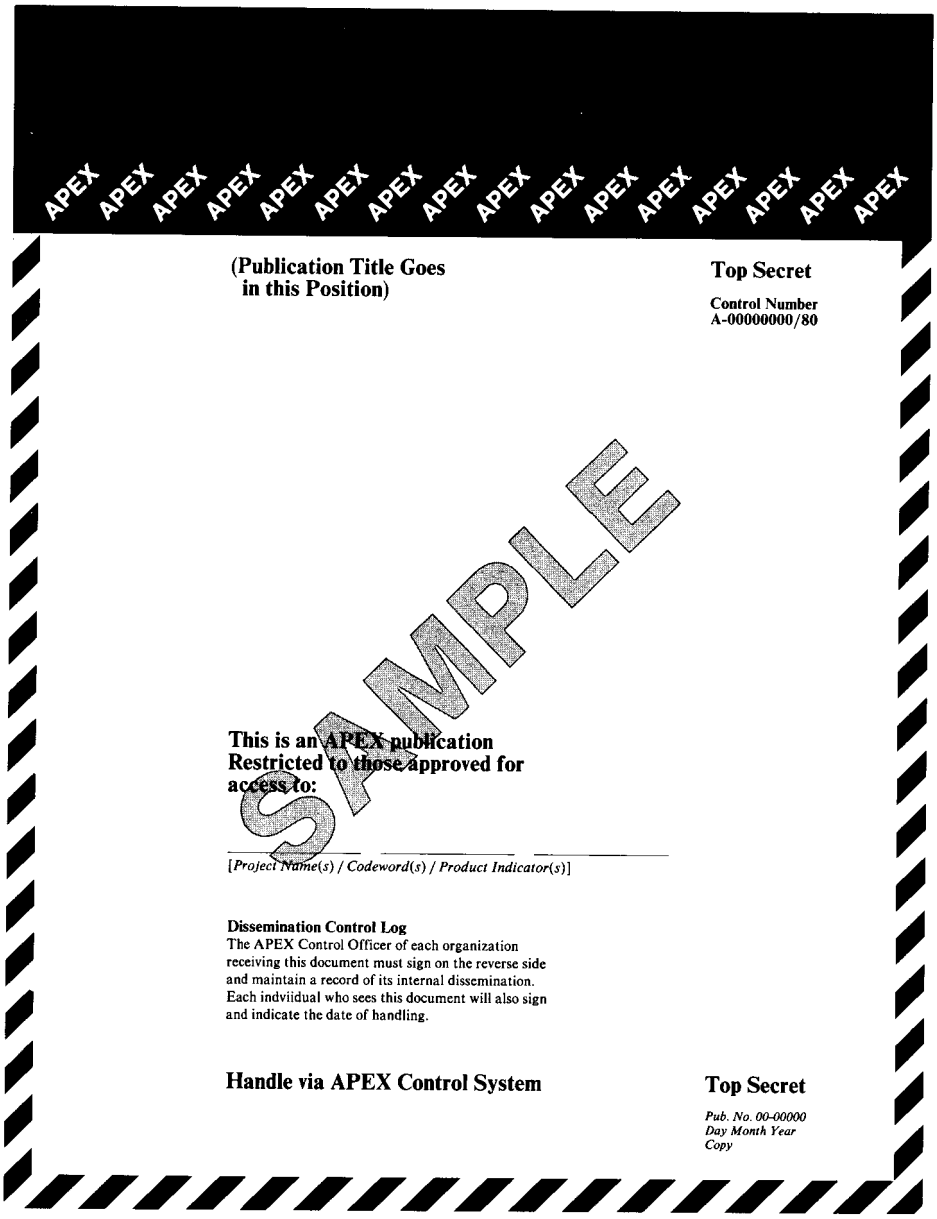
Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination.
Each individual who sees this document will also sign and indicate the date of handling.

Unit	Signature	Date Rec'd	Released

APEX operational document cover sheet (rear). Continuation of the dissemination control Log.

Enclosure I-C

Cover sheet for operational subcompartment publication (front). Operational project name(s) with the suffix ALPHA, other operational subcompartment name(s), codeword(s), and product indicator(s), if appropriate, will be placed as shown. Cover stock is unclassified. Cover sheets are classified when classified project name(s) with ALPHA suffix, codeword(s), and/or titles are affixed.



See overleaf for opposite side of this sheet.

Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination.
Each individual who sees this document will also sign and indicate the date of handling.

Unit	Signature	Date Rec'd	Released

Certification of Destruction
When document is destroyed, this control sheet may be kept or returned to the originator and be destroyed when five years old.

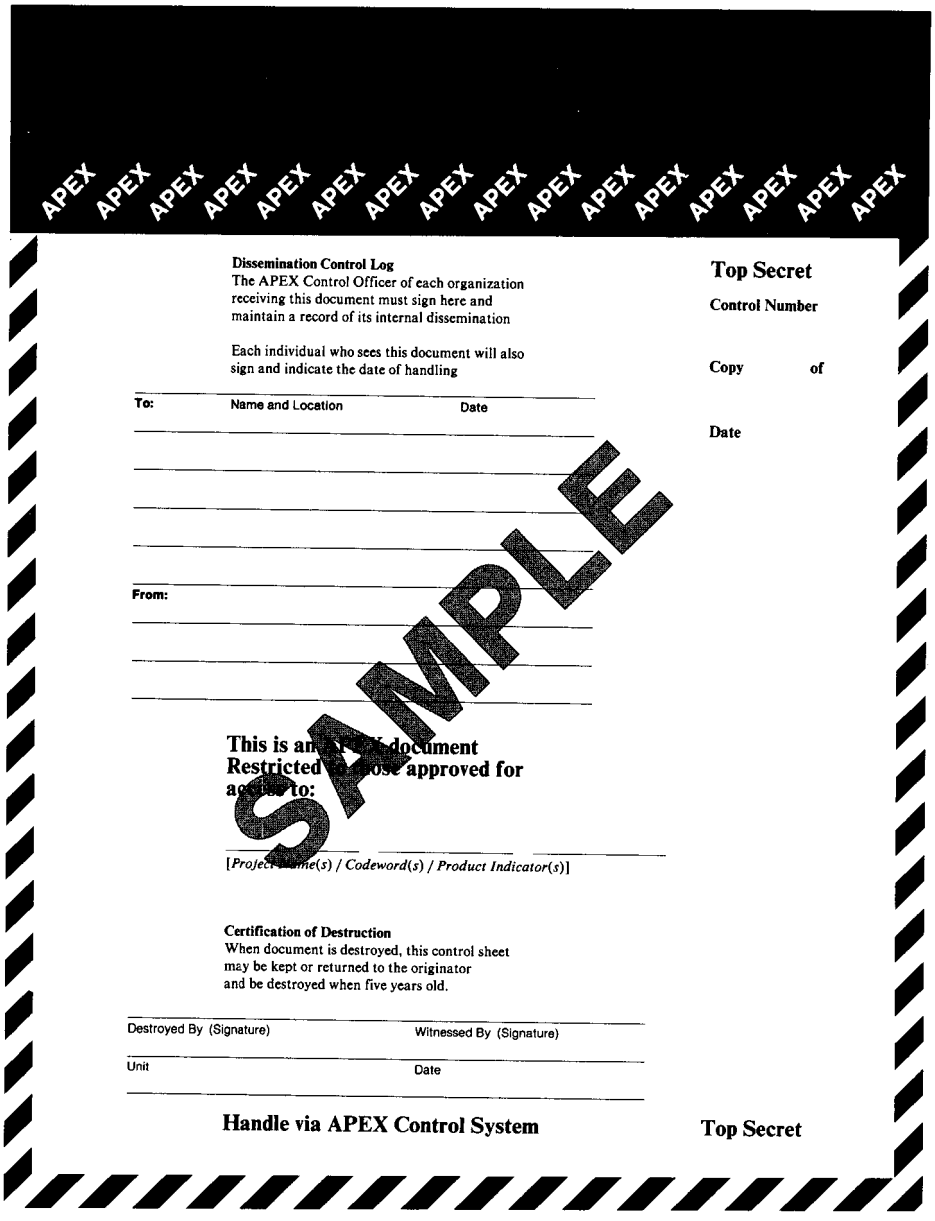
Destroyed by (Signature) Witnessed By (Signature)

Unit Date

Cover sheet for operational subcompartment publication (rear) with integral dissemination control log and certificate of destruction.

Enclosure I-D

Cover sheet for use with operational subcompartment document (front). Operational project name(s) with the suffix ALPHA, other operational subcompartment name(s), codeword(s), and product indicator(s), if appropriate, will be placed as shown. Cover sheet stock is unclassified. Cover sheets are classified when classified project name(s) with ALPHA suffix, and/or codeword(s) is/(are) affixed.



See overleaf for opposite side of this sheet.

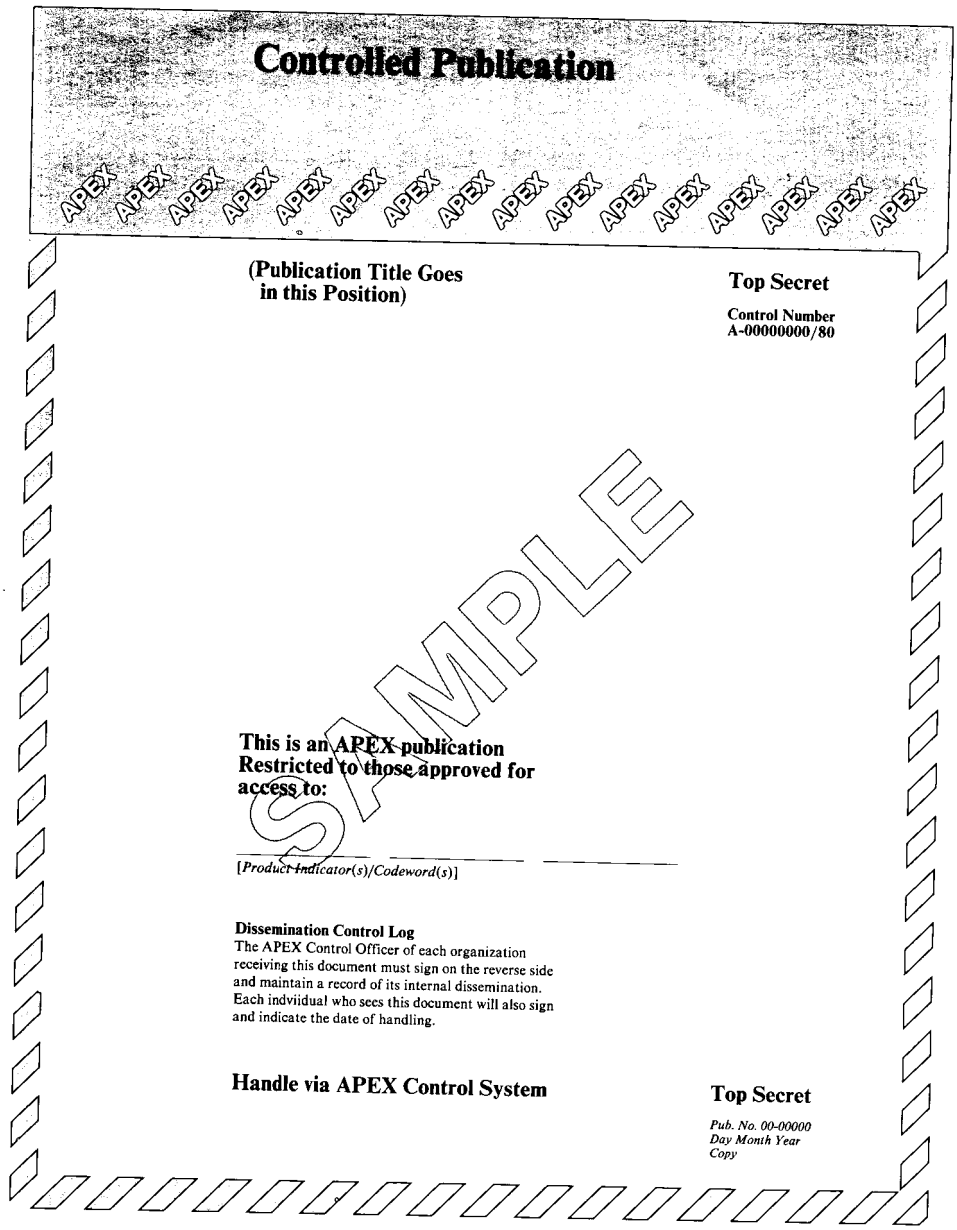
Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination.
Each individual who sees this document will also sign and indicate the date of handling.

Unit	Signature	Date Rec'd	Released

Cover sheet for use with operational subcompartment document (rear). Continuation of the dissemination control log.

Enclosure I-E

Cover sheet for product publications (front). Product generic source indicator(s) and/or codeword(s), as appropriate, will be placed as shown. Cover sheet stock is unclassified. Cover sheets are classified when classified codeword(s) and/or titles are affixed.



See overleaf for opposite side of this sheet.

Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination.
Each individual who sees this document will also sign and indicate the date of handling.

Unit	Signature	Date Rec'd	Released

Certification of Destruction
When document is destroyed, this control sheet may be kept or returned to the originator and be destroyed when five years old.

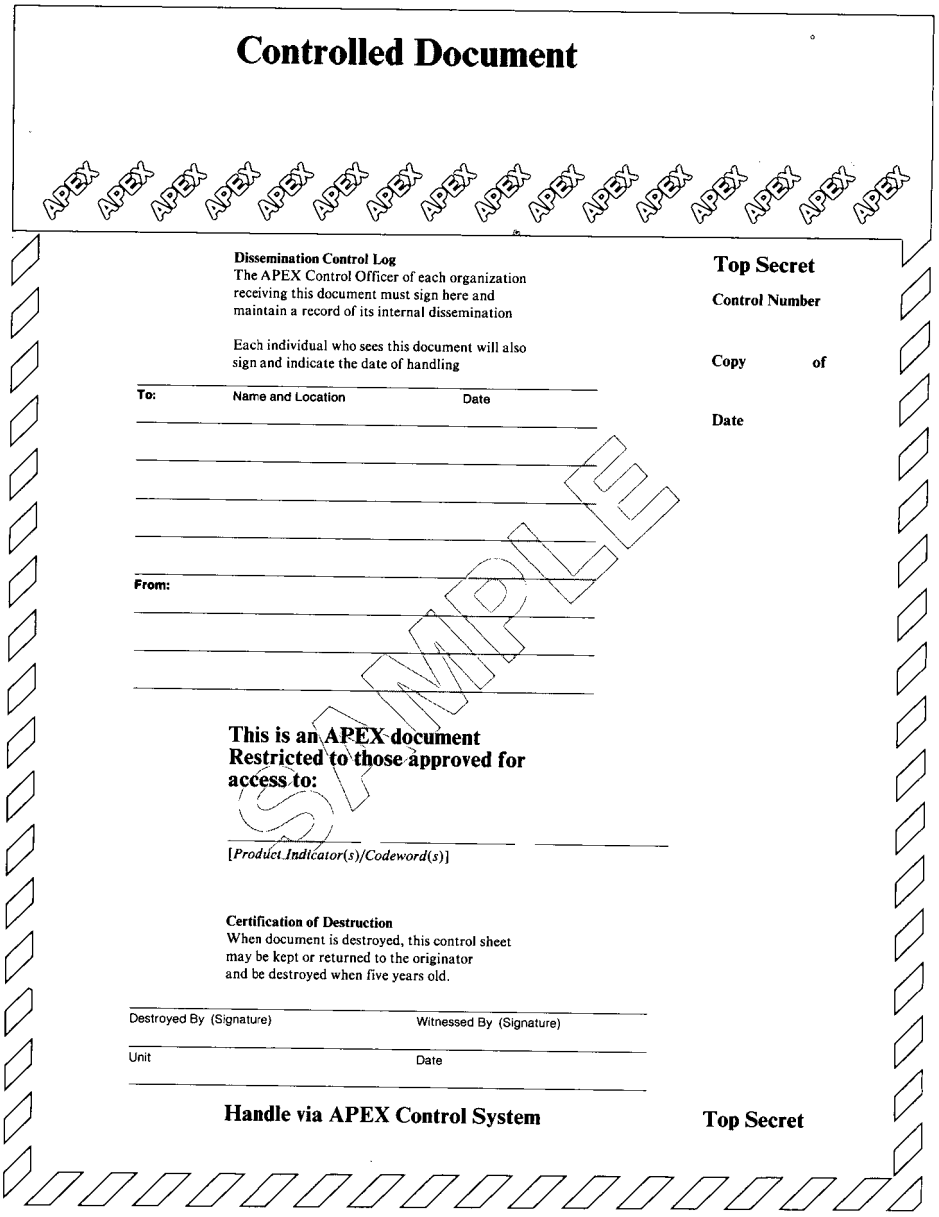
Destroyed by (Signature) _____ Witnessed By (Signature) _____

Unit _____ Date _____

Cover sheet for product publications (rear) with integral dissemination control log and certificate of destruction.

Enclosure I-F

Cover sheet for product documents (front). Product generic source indicator(s) and/or codeword(s), as appropriate, will be placed as shown. Cover sheet stock is unclassified. Cover sheets are classified when classified codeword(s) is/(are) affixed.



Controlled Document

APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX APEX

Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination

Each individual who sees this document will also sign and indicate the date of handling

Top Secret

Control Number

Copy **of**

Date

To: Name and Location Date

From:

SAMPLE

This is an APEX document Restricted to those approved for access to:

[*Product Indicator(s)/Codeword(s)*]

Certification of Destruction
When document is destroyed, this control sheet may be kept or returned to the originator and be destroyed when five years old.

Destroyed By (Signature) Witnessed By (Signature)

Unit Date

Handle via APEX Control System

Top Secret

See overleaf for opposite side of this sheet.

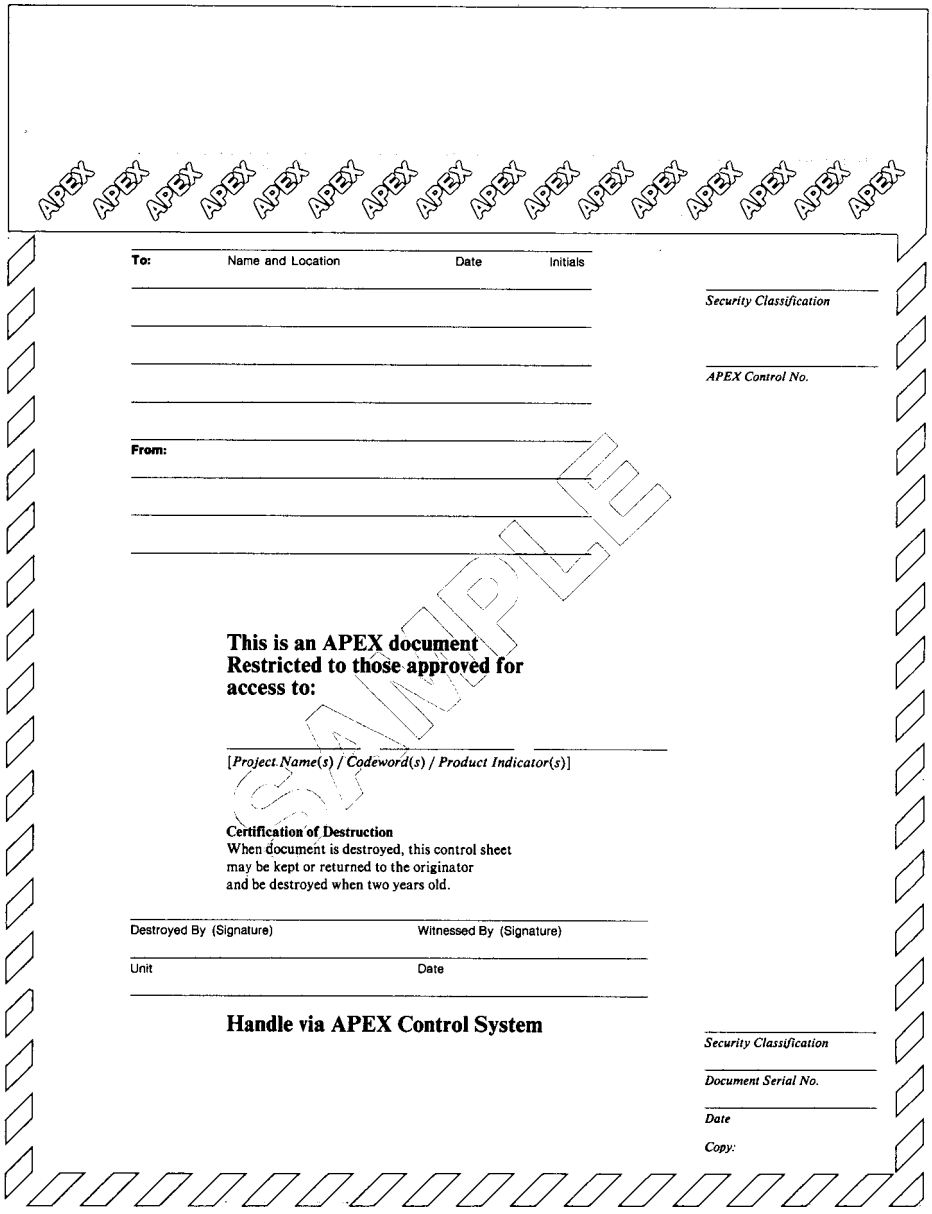
Dissemination Control Log
The APEX Control Officer of each organization receiving this document must sign here and maintain a record of its internal dissemination.
Each individual who sees this document will also sign and indicate the date of handling.

Unit	Signature	Date Rec'd	Released

Cover sheet for product documents (rear). Continuation of dissemination control log.

Enclosure I-G

Cover sheet for all CONFIDENTIAL and SECRET documents in the APEX Control System. Project name(s)/codeword(s)/product indicator(s) will be placed as shown. Cover sheet stock is unclassified. Cover sheets are classified when classified project name(s) and/or codeword(s) is (are) affixed.



See overleaf for opposite side of this sheet.