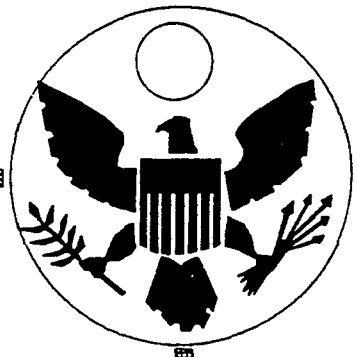
SPECIAL ACCESS PROGRAM SUPPLEMENT TO THE NATIONAL INDUSTRIAL SECURITY PROGRAM MANUAL



D R A F T
29 MAY 1992

FOR OFFICIAL USE ONLY

SPECIAL ACCESS PROGRAM SUPPLEMENT

TO THE

NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING MANUAL (NISPOM)

(Note: Since the content of the base line is not known as of 1 June 1992, this supplement will be redrafted during the later part of 1992 to remove items that subsequently appear in the baseline document)

****
**** Questions concerning the content of ****
**** the SAP Supplement may be directed ****
**** to Mr. Richard F. Williams, Office ****
**** of the Deputy Under Secretary of ****
**** Defense for Security Policy, ****
**** (703) 614-0578/9. ****
****

Revision: 29 MAY 92/JMB

FOREWORD

The National Industrial Security Program Operating Manual (NISPOM) Special Access Program supplement provides the allowable specific security requirements and procedures to the baseline NISP requirements in accordance with pertinent instructions and directives for the administration of Special Access Programs. It prescribes requirements and provides instructions to all references listed in Chapter I of this supplement. Security guidance in the baseline NISPOM shall be applicable to all SAPs. In cases where there is conflict between the supplement and other security directives, the supplement shall take precedence. In cases of doubt, the Facility Program Manager (FPM) or the Facility Control Officer (FCO) should consult the Program Security Officer (PSO) prior to taking any action. In cases of extreme emergency requiring immediate attention, the action taken should be such that the government's interest and the security of the program are protected from compromise.

This supplement establishes the SAP security policies newly issued by all agencies/departments of the Executive Branch of the U. S. Government. Existing provisions will be reviewed within two years of the implementation date of this supplement.

(SCIFs)), September 1987;

(9) NTISSI 300 (National Telecommunications and Information Systems Security Instruction) (National Policy on Control of Compromising Emanations);

(10) NTISSI 7000 (National Telecommunications and Information System Security Instruction (NTISSI) TEMPEST Countermeasures for Facilities), 17 October 1988; and,

(11) National Computer Security Center "Rainbow Series" (Computer Security).

(12) Additional references will be added to reflect superseded regulatory instruments.

1-101. Scope.

With regard to industrial security measures, the guidance contained herein is binding upon all persons (military, Executive Branch, civilian, contractor, and consultants) who are granted access to SAP information. The policies and procedures listed herein are a condition precedent to any negotiations leading to Program participation and establishment of a Program facility at a particular organization.

1-102. General Indoctrination and Guidance.

a. **Existence of SAP.** Government Agency SAPs are either **ACKNOWLEDGED** or **UNACKNOWLEDGED** programs. AN UNACKNOWLEDGED SPECIAL ACCESS PROGRAM WILL NOT BE MADE KNOWN TO ANY PERSON NOT AUTHORIZED FOR SUCH INFORMATION.

b. **Need-to-know.** Classified SAP program information may be discussed with or disseminated only to those persons specifically indoctrinated and then only after a determination of the required level of access.

c. **GPM.** The Government Program Manager is responsible for implementation and maintenance of the "program".

d. **SAP Access Authorization.** The GPM or designated "Approving Official" shall authorize all SAP briefings and will make all "need-to-know" access determinations.

SAP = Special Access Program

CHAPTER 2

DEFINITIONS AND RESPONSIBILITIES

2-100. General.

a. **Existence.** Special Access Programs are very sensitive in nature, and as such, fall into the two major categories: **ACKNOWLEDGED SAPs** and **UNACKNOWLEDGED SAPs.**

b. **Waiver.** Any security waivers require the express written approval of the Program Security Officer (PSO).

c. **Right of Appeal by Contractor.** Any requirement necessitated by a threat/cost/sensitivity/risk analysis shall be imposed by contract. The contractor has the responsibility to comply with additional contractually imposed requirements. The contractor has the right to appeal within government SAP channels any requirement in excess of this supplement or the contract, and may do so without fear of prejudice or penalty.

d. Executive Agency SAP Policy Council. **To be determined.**

2-101. Definitions. For purposes of SAP activities, the following definitions apply:

a. **Access Approval Authority.** Person or individual (by title or position) authorized to grant program access as identified in the Access Baseline or other program compartmented documentation.

b. **Billets.** A determination that in order to meet need-to-know protection, certain SAP programs may elect to limit access to a pre-determined number of properly cleared employees.

safeguarding, handling and discussing CLASSIFIED and/or UNCLASSIFIED program information, hardware and materials.

k. **Program Material.** Program material and information directly describing the service(s) provided, the capabilities developed, or the item(s) produced under the SAP.

l. **Program Security Manual (PSM).** A security manual which utilizes the menu of protective controls of this supplement. It describes based on threat/sensitivity/cost, those provisions of the NISP which apply to the individual special access program.

m. **Program Security Officer (PSO).** The government official who administers the security policies for the SAP. The PSO will be designated by the Agency SAP Director of Security and will be responsible for all aspects of SAP security.

n. **Special Access Program.**

A program approved by an agency head by Executive Order 12356.

o. **UNACKNOWLEDGED Special Access Program.** A SAP with protective controls which ensures the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information. All aspects (e.g., technical, operational, financial, logistical, etc.) are handled in an UNACKNOWLEDGED manner.

p. **ACKNOWLEDGED.** A SAP with established access controls relative to the distribution and protection of particularly sensitive classified information; however, the existence of the program has been publicly acknowledged

the relationship between the contract sponsoring agency and the contractor. To obviate the need for granting program access, the contractor shall establish internal procedures and sanitized control numbers as necessary for cost accumulation and other administration by non-program personnel. When costs are accumulated under internal sanitized numbers, program accessed personnel will prepare invoices/vouchers within program spaces and then classify them accordingly unless otherwise directed in the contract. Provisional payment invoices/vouchers will be forwarded directly to the PCO via program channels in accordance with the procedures and outlines for transmission of program classified material. In the instances where the contract number can not be cited on unclassified subcontracts or purchase orders, the contractor shall comply with Chapter 10, Subcontracting, of this supplement. The Government will furnish contract numbers or designator to the FCO to facilitate requests for clearances, periodic reinvestigations, etc., by e.g. DISCO.

i. **Correspondence (UNACKNOWLEDGED Programs).** Correspondence relating to UNACKNOWLEDGED programs will be marked, handled and classified according to the Program Security Guide. The PSO may direct that certain unclassified program documentation be prepared on non-letterhead, plain bond paper. Copies of reports, such as those required by the Reports Section of this chapter or the NISPOM will be classified accordingly.

j. **Non-Attributable Post Office Boxes.** Each UNACKNOWLEDGED program facility may be required to establish a separate non-attributable U.S. Postal Service box for each SAP or SAP related

material. Non-attributable post office boxes shall be for the exclusive use of the SAP facility and limited to persons with current SAP access. Payment for the post office box must be made from a non-attributable fund so that the identity of the facility and company will not be associated with the box. When a non-attributable post office box is changed as a result of compromise, the new box should be at a different U.S. Post Office whenever practical. In all cases, where an individual(s) is no longer accessed to the program, the post office box access list or the box will be changed within ONE business day.

k. **Non-Attributable Telephones.** Non-attributable telephones lines for UNACKNOWLEDGED programs shall not be identifiable in any manner with the facility or the SAP. Non-attributable telephone numbers shall be unlisted, unpublished and when possible a secured unit. A guide for the use of such telephones within a program facility is provided in Chapter 11, Communications, of this supplement.

l. **Program Access List.** All facilities are responsible for maintaining a current access roster of individuals program briefed at their facility. The facilities program access list should be periodically reconciled for any discrepancies against an access list provided by the PSO.

m. **Program Channels (UNACKNOWLEDGED Program).** Each UNACKNOWLEDGED SAP facility may be required to establish non-attributable SAP channels to ensure that all program related material is properly and securely transmitted. The establishment of program channels protects the relationship of all contracting

parties involved. Program channels may consist of non-attributable addresses, non-attributable telephone numbers, and other mechanisms for the transmission of classified and/or sensitive information outside of normal company methods. Non-attributable addresses and telephone numbers must not be connected in any way to the contractor or the contract sponsoring agency. Revelation or compromise of these program channels constitutes a security violation. An integral part of the program channel is the Document Control Center located within the secured perimeter of.the program facility or a SAP approved program facility where all classified program/program-related material created, received, dispatched or destroyed will be recorded and accounted for.

n. **Program Cover Stories (UNACKNOWLEDGED Programs).** Cover stories may be established for unacknowledged programs in order to protect the integrity of the program from individuals who do not have a need to know. Cover stories must be believable and cannot reveal any information regarding the true nature of the contract. Cover stories for Special Access Programs must have the approval of the PSO prior to dissemination.

PSO = Program Security Officer

o. **Program Visits (UNACKNOWLEDGED Programs).** All visits by program accessed government or contractor employees will be conducted in a manner for the protection of sensitive contract relationships as specified in the program security manual.

p. **Prohibited Items.** Items that constitute a threat to the security integrity of the facility e.g. radios, cameras, are prohibited in SAP controlled areas unless authorized by the PSO. All categories of storage media entering and leaving the SAP

WARNING

THIS PACKAGE CONTAINS CLASSIFIED U.S. GOVERNMENT INFORMATION. TRANSMISSION OR REVELATION OF THIS INFORMATION IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY TITLE 18, U.S. CODE, SECTION 798. IF FOUND, PLEASE DO NOT OPEN. "CALL COLLECT" AT THE FOLLOWING NUMBERS: (area code)(number) (PSO/APSO/FCO work number) **DURING WORKING HOURS** OR (area code)(number)(PSO/APSO/FCO home number) **AFTER WORKING HOURS.**

a. In the case of an UNACKNOWLEDGED SAP, a contractor's firm or business name, address, logo, watermark or the identity of Government organizations will not appear on the inner or outer containers. Do not use company postage meter cachet. The materials will be transmitted by the baseline security measures or as otherwise identified in the SAP SPP. A non-attributable return address will be used on UNACKNOWLEDGED SAPs. On acknowledged programs where association is unclassified, company identification may be used.

b. **Requirements for Hand-carrying.** The PSO through the FCO will provide detailed provisions if hand-carrying of SAP materials is permitted. Unless specifically authorized, hand-carrying of SAP material may be prohibited.

c. **ELECTRONIC TRANSMISSION NETWORKS.** Secure facsimile/electronic transmission (encrypted secure) equipment may be required to be used for the transmission of program classified

should be conducted on Class 4 instruments in the secure mode. Maximum utilization of Type 4 instruments should be emphasized on a continuing basis and as an integral part of Security Education and Awareness Programs. The use of specialized equipment, such as answering devices or speaker phones with Class 4 telephones must be authorized by the customer.

(1) **Non-Attributable telephones** are not readily identified in any manner with the facility, company, government agency or SAP. The procurement, billings and payments for the instruments are made in the name of an individual using a home or non-attributable post office box address (see non-attributable mailing procedures below). Controlling the telephone bill precludes analysis which can be particularly revealing in identifying program participants. Another advantage is it bypasses the activity's switchboard operators. In order to make Foreign Intelligence Service (FIS) monitoring of telephone conversations more difficult, the following must be strictly adhered to:

(a) Non-attributable telephone numbers will be unlisted and unpublished. At the time of procurement, the telephone company should be informed that the telephones are private, that billings will not be made through the activity's channels, and that no information will be released concerning the telephone number or its physical location. All non-attributable telephone numbers will have a different exchange prefix than that of the existing facility. However, it is permissible to utilize a system whereby fiber-optic lines with disassociated numbers enter a trunk network to a building switch and are then re-routed to

another number within the SAPF.

(b) The non-attributable telephone is not secure; classified information will not be discussed or "talked around" over the non-attributable telephone. Use of military ranks, rates, industrial titles and geographical locations shall not be disclosed on the telephone.

(c) Non-attributable telephones for program use will be answered only by program briefed personnel, with instructions to never divulge any revealing information relative to the location of the telephone or to respond to any other classified inquiries by a caller.

(d) When answering a non-attributable telephone, program personnel will state the proper salutation, e.g. "Good morning" or "Hello". Do not use the company name or the telephone number when answering these telephones, however, company program identifiers may be used.

(e) Non-attributable telephone numbers will be changed when compromised or when OPSEC considerations warrant. New numbers will be transmitted/distributed only via secure telephone (STU-III), secure facsimile, or US Postal Service Registered Mail or in person. Postal Service Express Mail or commercial express mail services are not authorized for this purpose.

(f) Payment for the installation services and monthly billings will be made from a petty cash fund or some other method that avoids company affiliation.

(g) Calls placed on non-attributable telephones will be non-attributable number to non-attributable number unless