[redacted]

Headquarters
Department of the Army
Washington, DC
1 June 1986

[redacted]*Army Regulation 380-381

Effective 1 June 1986

Security

Special Access Programs (SAPs)

(U) Summary. This regulation establishes policies and prescribes procedures for establishing, administratively controlling, and supporting Special Access Programs (SAPs) and SAPs with "carve-out" contracts.

(U) Applicability. This regulation applies to the Active Army. It does not apply to the Army National Guard (ARNG) or U.S. Army Reserve (USAR).

(U) Impact on New Manning System. This regulation does not contain information that affects the New Manning System.

(U) Internal control systems. This regulation is not subject to the requirements of AR 11-2. It does not contain internal control provisions.

(U) Committee continuance approval. The DA Committee Management Officer concurs in the continuance of the Special Access Programs Oversight Committee (SAPOC) which was established by AR 380-381 (C), 15 August 1983.

(U) Supplementation. Supplementation of this regulation and establishment of forms other than DA Forms are prohibited, unless prior approval is obtained from HQDA(DACS-DMP), WASH DC 20310-0200.

(U) Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

(U) Suggested improvements. The proponent agency of this regulation is the Office of the Chief of Staff, Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA(DACS-DMP), WASH DC 20310-0200.

(U) Distribution restriction. This publication contains operational information that is for official use only. Distribution is limited to U.S. Army agencies. Requests from outside the U.S. Army for release of this publication must be made to HQDA(DACS-DMP), WASH DC 20310-0200.

*This regulation supersedes AR 380-381 (S), 1 March 1985, and rescinds DA Form 5400, March 1985.

Contents (U)

	Paragraph	Page
Purpose	1	3
References	2	3
Explanation of abbreviations and terms	3	3
Policy	4	3
Responsibilities	5	5
Procedures	6	7

Appendix

A. References	A-1
B. Format for Reporting Special Access Programs	B-1
C. Special Access Program Oversight Committee Charter	C-1
D. Special Access Program Determination Criteria	D-1
E. Technology Management Office Responsibilities	E-1
F. Limited Special Access Program	F-1
G. Format for Annual SAPOC Revalidation	G-1
H. Special Access Program Disestablishment	H-1
I. Information Systems Requirements Package	I-1

Glossary ..... Glossary 1

1. (U) Purpose

a. (U) This regulation establishes policies and prescribes procedures for establishing, administratively controlling, and supporting Special Access Programs (SAPs) and SAPs with "carve-out" contracting. The following terms apply:

(1) (U) *Special Access Program (SAP).* Any program imposing a must "need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information under provisions of AR 380–5. Such a program may include, but is not limited to, access clearance, adjudication or investigative requirements, special designation of officials authorized to determine a must "need-to-know," or special lists of persons determined to have a must "need-to-know." The justification for a SAP must establish that:

(a) (U) Normal management and safeguarding procedures are not sufficient to limit access; and

(b) (U) The number of persons who need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved.

(2) (U) *Carve-Out.* A classified contract issued in connection with an approved SAP in which the Defense Investigative Service (DIS) has been relieved of contractor security inspection responsibility in whole or in part under the Defense Industrial Security Program (DOD 5220.22–M).

b. (U) The types of activities which may be governed by this regulation include:

(1) (U) Research, development, and acquisition of systems, items or services.

(2) (U) Modifications to existing systems in which a significant vulnerability has been discovered.

(3) (U) Intelligence collection and exploitation.

(4) (U) Foreign materiel procurement and exploitation.

(5) (U) Strategic and tactical operational concepts and plans.

(6) (U) Activities and organizations involved in the conduct of covert or clandestine operations.

2. (U) References

(U) Required and related publications and prescribed forms are listed at appendix A.

3. (U) Explanation of abbreviations and terms

(U) Unless explained in the text of this regulation or cited references, abbreviations and special terms are defined in the glossary.

4. (U) Policy

a. (U) The creation of SAPs and the utilization of "carve-out" contracts dictate that extraordinary management measures be applied to ensure:

(1) (U) Strict compliance with the provisions of law and applicable regulations.

(2) (U) Propriety in solicitation and awarding of contracts and purchase requests.

(3) (U) Financial accountability.

(4) (U) Involvement of appropriate authorities in the decisionmaking process.

(5) (U) Security controls are established and enforced.

b. (U) It is the policy of the Department of the Army to use the security classification categories and the applicable sections of E.O. 12356, DOD Directive 5200.1–R and AR Regulation 380–5 to limit access to classified information. The "need-to-know" principle in the regular classification system will normally apply, so there will be no need to resort

to formal SAP provisions. The granting of SAP status, therefore, will not be a routine action. It must be specifically demonstrated that:

(1) (U) The proposed activity could not be accomplished or would incur unacceptable security risks unless granted SAP status.

(2) (U) The proposed activity is so sensitive that the cost, loss of advantage, or damage to national defense which would result from compromise is unacceptable.

(3) (U) The provisions of the Army Information Security Program (AR 380-5) are not sufficient to ensure the necessary limitations on access to program information.

(4) (U) The proponent is prepared to incur the additional restrictions and costs inherent in a SAP.

c. (U) While not all inclusive, the following conditions provide guidelines for determining what type activity or program should be considered for SAP approval.

[redacted]

through the appropriate Army Staff element to HQDA(DACS-DMP), WASH, DC 20310-0200, in accordance with appendix B. Requests will be:

(1) (U) Accompanied by a security plan, classification guide, billet structure and information systems requirements package (app I).

(2) (U) Coordinated by the requestor with the Army Staff and appropriate MACOMs.

[redacted]

(4) (U) Forwarded by the TMO for Secretary of the Army approval and necessary reporting to the Deputy Under Secretary of Defense (Policy) [DUSD(P)].

e. (U) The use of a "carve-out" contract is prohibited unless such contract supports an approved SAP. The fact that a classified contract is a part of an approved SAP is not, of itself, sufficient justification for a "carve-out" contract.

(1) (U) Requests for approval of a SAP with a "carve-out" contract must include rationale for use of "carve-out" contracting and proposed "carve-out" contracting procedures. These procedures must comply with DOD 5220.22-M, AR 380-49, appendix B, and with Federal, Defense, and Army acquisition regulations. Program managers and proponents for SAPs must specify what organization is assuming the security responsibilities which are "carved-out" of DIS.

(2) (U) Commanders or heads of DA activities sponsoring a SAP supported by a contractor will use DD Form 254 (Contract Security Classification Specification) when establishing a "carve-out" contract.

[redacted]

[redacted]

[redacted]

g. (U) The range of extraordinary security protections and access controls afforded to approved SAPs may not be applied to other programs, even though such programs otherwise meet the definition of a SAP in paragraph 1 of this regulation. Specifically, no collaterally classified programs other than an approved SAP may control access through signed nondisclosure statements or use "carve-out" contracting.

h. (U) Requests for waivers to policy as set forth in this regulation may be submitted to HQDA(DACS-DMP).

5. (U) Responsibilities

a. (U) *The Secretary of the Army (SA)* is responsible for all matters related to compartmented activities within the Department of the Army. The Secretary may delegate portions of those responsibilities to the Under Secretary of the Army, Assistant Secretaries of the Army, General Counsel, or others.

b. (U) *The Assistant Secretary of the Army (Research, Development, and Acquisition) [ASA(RDA)]* is designated as the principal assistant to the Secretary and Under Secretary of the army for matters related to RDA compartmented activities, including those funded by RDTE or procurement appropriation funds. The Assistant Secretary shall assist in policy direction and oversight, unless specifically exempted by the Secretary of the Army or Under Secretary of the Army and be responsible for:

(1) (U) Oversight of research and development, the technology base, and hardware systems issues, specifically including examination of technology feasibility, related to compartmented programs.

(2) (U) Oversight of compartmented systems acquisition and related procurement procedures.

(3) (U) Acquisition of systems, components, and modifications developed under a Special Access Program which must be protected by SAP procedures during procurement and fielding.

(4) (U) Coordination with OACSI to ensure that technology transfer issues are addressed during development of technical programs.

c. (U) *The General Counsel (GC)*, will provide legal and policy advice on SAP matters.

d. (U) *The Chief of Staff, Army (CSA)* will be responsible for the development, coordination, review, and execution of all compartmented activities within the Army.

e. (U) *The Vice Chief of Staff, Army (VCSA)* will be responsible for the management of compartmented programs and the implementation, through the SAPOC, of policies assigned in paragraph 4. The Vice Chief of Staff of the Army responsibilities include:

[redacted]

(2) (U) Ensuring that the TMO:

[redacted]

(*b*) (U) Institutes procedures to coordinate all actions related to SAPs.

(3) (U) Serving as the chairman of the SAPOC (app C).

f. (U) *The Deputy Chief of Staff for Personnel (DCSPER)* will provide the necessary personnel management system for classified/compartmented programs and activities.

g. (U) *The Deputy Chief of Staff for Operations and Plans (DCSOPS)* will—

(1) (U) Coordinate user review and analysis of candidate SAPs, unless this responsibility is specifically assigned to another agency.

(2) (U) Provide policy guidance and standards for operations security (OPSEC) measures appropriate for SAPs.

h. (U) *The Deputy Chief of Staff for Research, Development, and Acquisition (DCSRDA)* will:

(1) (U) Provide SAP life cycle management policy and support.

(2) (U) Coordinate with other DOD components/departments to ensure no duplication of efforts or differences in security protection for multi-service programs.

(3) (U) Coordinate a technical review of candidate SAPs, unless this responsibility is specifically assigned to another agency.

i. (U) *The Deputy Chief of Staff for Logistics (DCSLOG)* will:

(1) (U) Provide SAP contracting and procurement policy and support.

(2) (U) Ensure that appropriate Army management of the contracting function is in place and operative for all contracts in support of SAPs.

(3) (U) Ensure the concept of Integrated Logistics Support is included in all materiel development or materiel acquisition SAPs.

[redacted]

j. (U) *The Assistant Chief of Staff for Intelligence (ACSI)* will—

(1) (U) Provide policy for intelligence and counterintelligence support to SAPs, to include enemy threat and countermeasures, assessment of the foreign intelligence threat, assessments of the net security risk to SAPs, and counterintelligence support to the OPSEC process.

(2) (U) Provide preliminary intelligence assessments of candidate SAPs to support the decisionmaking process of the SAPOC.

(3) (U) Maintain the capability to analyze and evaluate potential adversaries' technologies.

k. (U) *The Assistant Chief of Staff for Information Management (ACSIM).* The ACSIM will coordinate information systems aspects of SAP support.

l. (U) *Chief of Engineers (COE).* In discharging responsibilities for military construction, the COE will provide reimbursable construction support for secure facilities when requested by commanders of host commands having responsibility for providing those facilities.

m. (U) *Comptroller of the Army (COA).* The COA will—

(1) (U) Develop a system and implement procedures to provide financial and budgeting guidance, Army Staff support and execution review for SAPs at an appropriation program level.

(2) (U) Monitor Congressional reprogramming of SAP funds and ensure these actions receive review at the appropriate levels.

(3) (U) Provide cost analysis/pricing support for selected SAPs.

n. (U) *The Inspector General (TIG).* TIG will provide inspector general oversight of SAPs.

o. (U) *The Judge Advocate General (TJAG).* TJAG will provide legal and policy advice on SAP matters.

p. (U) *Chief of Legislative Liaison (CLL).* The CLL will coordinate Congressional interest in and briefings on Army SAPs and ensure that appropriate committees are kept informed of SAP status.

q. (U) *Director, Program Analysis and Evaluation Directorate (PAED).* The Director, PAED, will—

(1) (U) Ensure that SAPs compete with other Army programs for resourcing in the POM development process.

(2) (U) Notify the TMO of all approved SAP program and funding profiles.

r. (U) *Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC).* The CG, TRADOC will—

(1) (U) Institute procedures to ensure early identification and protection of combat developments, concepts, and systems with SAP potential.

(2) (U) Support user review and analysis of candidate SAPs, unless this responsibility is specifically assigned to another agency.

s. (U) *Commanding General, U.S. Army Materiel Command (CG, AMC).* The CG, AMC will—

(1) (U) Institute procedures to ensure early identification and protection of any potential R&D breakthrough or significant vulnerability of an existing or proposed U.S. Army system with SAP potential.

(2) (U) Support a technical review of candidate SAPs, unless this responsibility is specifically assigned to another agency.

t. (U) *Commanding General, U.S. Army Forces Command (CG, FORSCOM).* The CG, FORSCOM will institute procedures to ensure early identification and protection of activities, operational concepts, and combat developments requiring SAP status.

u. (U) *Commanding General, U.S. Army Information Systems Command (CG, USAISC).* The CG, USAISC will coordinate information systems aspects of SAP support and provide technical support, as required, for SAPs that require secure information systems. The Commanding General, 7th Signal Command is designated as the executive agent responsible to the CG, USAISC.

v. (U) *Commanding General, U.S. Army Strategic Defense Command (CG, USASDC).* The CG, USASDC, will institute procedures to ensure early identification and protection of any R&D breakthrough of significant vulnerability of an existing or proposed U.S. Army effort within the Strategic Defense Initiative Program with SAP potential.

w. (U) *Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM).* The CG, INSCOM will—

(1) (U) Institute procedures to ensure early identification and protection of sensitive intelligence activities and capabilities.

[redacted]

(3) (U) Provide counterintelligence and security support to commanders or heads of DA activities having proponency for approved SAPs.

[redacted]

(5) (U) Assist proponent agencies in preparing security classification guides and prescribe cover and passive counter-measures for approved SAPs and LSAPs.

(6) (U) Maintain the capability to collect information relevant to potential adversaries' technologies.

(7) (U) Provide, in coordination with OACSI, HOIS

[redacted]

threat information to organizations and installations supporting SAPs.

(8) (U) Provide comments in each case on the feasibility of using "carve-out" contracts for specific SAPs.

x. (U) *All Department of Army Staff elements, MACOM commanders, and Special Access Program proponents* will, for the SAPs for which they have proponency:

(1) (U) Designate a single point of contact for SAPs. This POC will serve as the central point for initial inquiries and responses on SAPs.

(2) (U) Manage the planning, programming, budgeting, accountability, and execution of SAPs.

(3) (U) Coordinate with OACSI for intelligence and counterintelligence support to OPSEC and threat support necessary for execution of SAPs.

(4) (U) Coordinate with ODCSRDA and AMC for RDA SAPs.

[redacted]

(6) (U) Maintain a file of security plans, classification guides and billet structures on SAPs for which they have the lead.

(7) (U) Assist in the discharge of responsibilities for SAPs and adherence to the policies stated in this regulation.

(8) (U) Coordinate with USAISC for secure communications advice and support.

(9) (U) Nominate activities, systems, concepts, or operations, as described in paragraphs 1 and 4 of this regulation, for SAP approval.

(10) (U) Notify the TMO and all effected agencies upon program termination. Insure no funds are expended on programs after their termination.

6. (U) Procedures

(U) It is essential that candidate Special Access Programs be identified as early as possible and that they be given special protection from concept through a point where a determination is consciously made that special protection is no longer warranted. Special protective procedures include:

a. (U) *Security.* Security is the responsibility of the program manager or proponent, who must provide the required personnel and financial resources to support the security plan for the SAP. Sound and continuous security planning is essential to successful execution of a SAP. Program managers and proponents should recognize that special security provisions generally have resource implications for their program and should plan accordingly. Program managers or proponents are encouraged to request CG, INSCOM to provide advice and assistance in planning for these special provisions. The SAPOC will evaluate special security provisions and overall security planning in conjunction with the processes of initial approval and annual revalidation of SAPs. Enhanced security measures incorporated into security planning and procedures for a SAP include:

(1) (U) Only those persons essential to the conduct of the program to include those involved in management and oversight will be granted access to program information. That information will be segregated by levels with individuals read-on to the level justified by a must need-to-know criteria only.

(2) (U) As a minimum a SECRET clearance with a favorable National Agency Check is required for access to Army SAP information. This may be supplemented with local agency checks, credit checks, and letters to past and present employers.

[redacted]

(4) (U) A billet structure for each Army SAP will be established by the proponent or program manager and approved by the SAPOC. SAP proponents or program managers will manage access to their SAPs within the approved billet constraints. The billet structure will identify the access control authorities and access approval authorities necessary for the accomplishment of required SAP briefings and debriefings. The billet structure will be briefed in the annual SAP revalidation and may be adjusted at that time, as necessary. Based on urgent need, requests to grant additional access beyond the number authorized for a SAP will be submitted to HQDA(DACS-DMP) for approval by the SAPOC or by the Vice Chief of Staff, Army. The billet structure will consist of those positions identified by the program manager/proponent necessary for the successful execution of the SAP and those identified in the Army SAP baseline. The Army SAP baseline includes those positions at all command levels necessary to manage and oversee SAPs. The Army SAP baseline will be provided to program managers/proponents by HQDA(DACS-DMP) and the personnel on this baseline will be briefed on the SAP when it

[redacted]

is approved. The program manager/proponent will determine when other personnel in the SAP billet structure will be briefed and provide access approval authorities with SAP briefing materials.

(5) (U) Voluntary acceptance in writing of specific administrative restrictions and liability for unauthorized disclosure is required as a prerequisite for receiving access. DA Form Form 5399-R (Special Access Program Initial Security Briefing) will be used for SAP indoctrinations. DA Form 5399-R will be reproduced locally on 8½ × 11 inch paper. A copy for reproduction purposes is located at the back of this regulation.

(6) (U) Operations security (OPSEC) constitutes a key factor in management of SAPs and is the responsibility of the program manager or proponent of a SAP. Security procedures established for each program in a security plan and classification guide will be followed. One copy of the plan and guide will be provided to the TMO with the initial request for SAP approval and will be evaluated by the TMO and staffed to ACSI and INSCOM for review and comment. Individuals approving classification guides must have original TOP SECRET classification authority. Program security provisions to include proposed billet structure will be briefed to and approved by the SAPOC. Security classification guides for programs where DIS has contractor security inspection responsibility will be provided to appropriately accessed DIS personnel. AR 380-5, appendix E, contains guidance on the preparation of a security classification guide.

(7) (U) Information systems security is a critical consideration. Provisions and requirements for secure information systems will be identified and described in each SAP request (app I). Acquisition of secure information systems equipment is a program manager or proponent responsibility. The ACSIM and CG, USAISC will provide advice and assistance, as necessary, to meet this requirement.

(8) (U) An aggressive program will be maintained to terminate accesses upon completing the work for which those accesses were originally granted using DA Form 5401-R (Special Access Program Security Termination Guide). Generally, the larger the number of persons with access, the greater the risk of program compromise. The number of persons with access will be one of the principal program issues reviewed in the annual SAP revalidation process. DA Form 5401-R will be reproduced locally on 8½ × 11 inch paper. A copy for reproduction purposes is located at the back of this regulation.

(9) (U) SAP proponents or program managers are responsible for ensuring that all prime contractor and subcontractor facilities are inspected by U.S. Army or Defense Investigative Service personnel at least twice a year. Prime contractor inspections of their subcontractors for compliance with SAP security requirements are not authorized.

(10) (U) Security violations, compromises, vulnerabilities, and weaknesses detected by whomever will be reported to the SAP program manager or proponent and the SAP security manager. The report will include recommended corrective action. The program manager and SAP security manager will evaluate the recommendation and take prompt action to resolve the reported security problem per AR 380-5 or DOD 5220.22-M. Significant security violations or compromises will be expeditiously reported by the program manager or proponent through appropriately accessed personnel in the chain of command to HQDA(DAMI-CI), WASH DC 20310-1054, who will notify the TMO. The initial report will include all known details of the violation or compromise, to include investigative or corrective action taken to date. An interim damage assessment will be expeditiously forwarded. Failure to resolve the security problem will be reported through the SAP proponent's chain of command to the TMO by the supporting INSCOM element. Significant or recurring security problems which result in a SAP security compromise will be an issue for SAPOC review.

(11) (U) DA Pamphlet 380-381, Security for Special Access Programs, provides additional guidance and information on the security provisions appropriate for SAPs.

b. (U) *Information.* Dissemination of information pertaining to specific SAPs will be handled case-by-case. The originating control specified in paragraph 6*a*(3) retains authority for approving access to SAPs.

(1) (U) No SAP may be openly identified in DA press releases or Congressional budget data or reports. However, appropriate authorities will be briefed in sufficient detail to satisfy all legal and program review requirements. These authorities will be added to access control rosters. Information (vocal or written) concerning specific SAPs will be provided to the Congress through the Chief, Legislative Liaison (CLL). Congressional staff members will be given a program security briefing, execute an initial security briefing statement, and be added to the program billet structure and access roster. All briefings of Members of Congress or their staffs on SAPs will be reported to the TMO for inclusion in the Congressional data book.

(2) (U) Strict security requirements of SAPs and "carve-out" contracts will be written into standard procedures for Army agencies, contractors, and test ranges engaged in these programs.

(3) (U) SAP information shall be stored, as a minimum, in a GSA approved safe-type steel file container having a built-in, three position, dial-type, GSA approved combination lock or a Class A vault or vault type room that meets the standards established by the head of the DOD Component concerned. See AR 380-5 for the standards applied to DA agencies and DOD 5220.22-M, Industrial Security Manual, for contractor requirements.

c. (U) *Limited Special Access Program.* The nature of certain projects, programs, and activities requires special protection be established expeditiously to avoid compromise. This means that these programs require SAP security controls before they are actually approved as SAPs. In these instances MACOM commanders and Department of the Army Deputy and Assistant Chiefs of Staff are authorized to apply for a Limited Special Access Program (LSAP) for a period not to exceed 6 months. The procedures governing LSAPs are discussed in appendix F.

d. (U) *SAP Approval Process.* The processing of SAP approval requests will be expedited to the greatest degree possible. Figure 1 depicts the approval process flow.

(1) (U) In general, the steps in the approval process are:

[redacted]

(d.) (U) *Brief to SAPOC.* The proposed SAP and the results of the detailed evaluation will be briefed to the working SAPOC, which will make an interim recommendation on SAP approval. The SAPOC will be briefed and will make the final recommendation on SAP approval. The functions and members of the SAPOC and working SAPOC are at appendix C.

(e.) (U) *Routing and Review.* The SAPOC recommendation and SAP request package are routed to the Under Secretary of the Army and the Chief of Staff of the Army, in turn. Questions that arise will be staffed by the TMO for resolution. The Secretary of the Army will then consider the request and approve or disapprove the action.

(f.) (U) *Official Notification.* If the Secretary of the Army approves the request, the TMO registers the SAP with ODUSD(P) and notifies the submitting agency, OACSI, and INSCOM.

(2) (U) *Administration*

(a.) [redacted]

(b. [redacted]

(c [redacted]

(3) (U) *Disestablishment.* A SAP may be recommended for disestablishment by the proponent or program manager when SAP security controls are no longer required. The SAPOC may also recommend a SAP be disestablished at the annual revalidation or at other times. Disestablishment does not mean the program will be cancelled. It only means that the program will be transitioned to the security controls of AR 380-5 and SAP security controls will no longer be applied. Guidance on SAP disestablishment is found at appendix H.

[redacted]

[redacted]

e. (U) *Nicknames and codewords.* All LSAPs and approved SAPs will be assigned an unclassified nickname. The request for a nickname will be forwarded to HQDA(DACS-DMP), WASH DC 20310-0200. When OPSEC requires the use of a codeword, the request procedure is the same as for a nickname.

f. (U) *Funding.* Funds associated with the execution of SAPs are to be managed and accounted for by the Army Staff proponent, MACOM commander, or program manager for the respective SAP and monitored by the TMO, unless exempted by the Secretary of the Army. The sponsoring agency will provide appropriate program and budgetary input to COA and PAED dedicated POCs to assure that funds are programmed and budgeted each FY. Funds will be accounted for in accordance with established finance and accounting procedures or as determined by the COA. Each Army Staff proponent, MACOM commander, or program manager will establish an internal review and inspection plan, submit the proposed plan with the request for SAP approval and provide the TMO a copy of the work plan with the annual revalidation.

g. (U) *Contracting.*

(1) (U) Contracting in a secure environment will require special procedures. The requirements of the Federal, Defense, and Army acquisition regulations cannot be waived in some cases and in other cases may be waived with the specific approval of authorized contracting officials and with substitution of adequate safeguards.

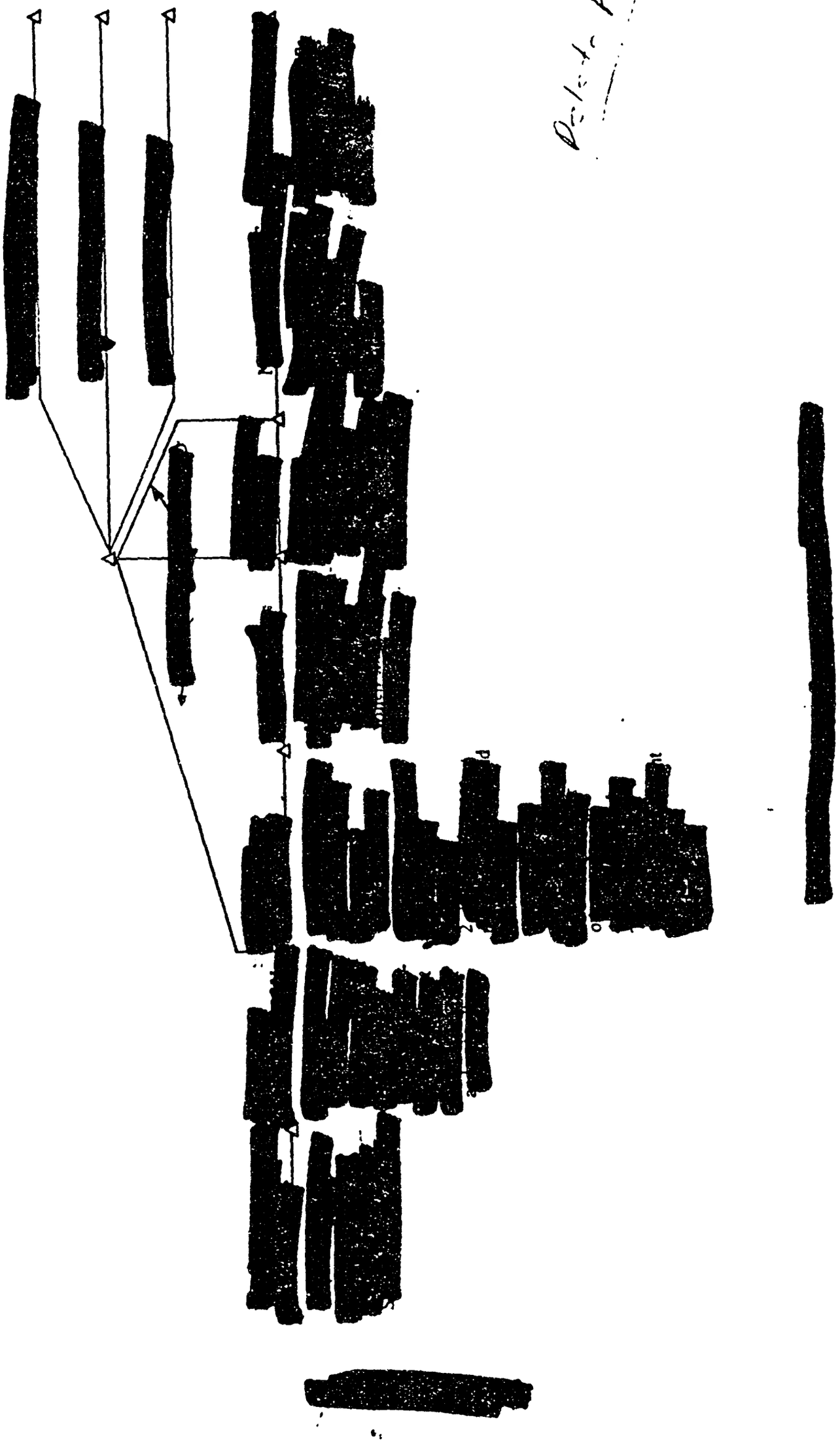
(2) [redacted]

(3) (U) Contract planning will be included in the request for SAP approval and subsequent approval briefing.

h. (U) *Special Security Provisions.* Special Access Programs are individually unique and may require special security provisions. The use of the Special Finance and Accounting Office, the requirement for a secure facility/vault, the application of a two-man control rule, and project information access procedures are examples of special provisions. Each of these has resource implications for the program manager or proponent and for other agencies within the Department of the Army. Program managers or proponents must determine whether these special provisions have applicability. The CG, INSCOM may be requested to provide advice and assistance in making this determination. Special provisions for the protection of program information will be evaluated in the SAP approval process and will be briefed to the SAPOC. The SAPOC may recommend these special provisions in part or in total to the Secretary of the Army.

[redacted]

[redacted]



By Order of the Secretary of the Army:

JOHN A. WICKHAM, JR.
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION: To be distributed in accordance with DA Form 12-9B, requirements for AR, Security. Active Army—B; ARNG and USAR—None.

SPECIAL ACCESS PROGRAM INITIAL SECURITY BRIEFING
For use of this form, see AR 380-381; the proponent agency is OCSA.

I, the undersigned, certify that I have received a security briefing concerning the below listed Special Access Program(s). I am aware that willfull disclosure of classified Government information to any unauthorized person may be punishable under Federal Criminal Statutes. I realize that the safeguarding of classified information or material is of the utmost importance and that loss or compromise of this information or material could be detrimental to the interests or national security.

Program (s) _____
(Nickname/or code word)

I understand that specific classification guidance exists for this project and is available for reference. I have been instructed in the nature of this classified information and the procedures governing its safeguarding. I understand that willfull violation or disregard of security regulations may cause the loss of my access authorization and security clearance.

I agree that I will never divulge, publish, or reveal (either by word, conduct, or other means) any classified Government information or knowledge concerning the above Special Access Program(s) except in the performance of my official duties in accordance with the laws of the United States.

I understand that no change in my relationship and/or my organization's relationship will relieve me of my obligation under this agreement.

I take this obligation freely, without any mental reservation or purpose of evasion. I understand that signing this document constitutes agreement to undergo a counterintelligence polygraph examination, if requested by proper authority, to determine my suitability for receiving and/or maintaining access to program information.

WITNESS:

_____ _____
(signature) (date) (signature) (date)

_____ _____
(signature) (date) (printed name)

_____ _____
(printed name) (SSN)

_____ _____
(position and organization) (organization, telephone #, position)

PRIVACY ACT STATEMENT
The authority for obtaining the personal information is Title 10, USC 3012. The principal use of this information is for identification for granting access to this project's information. No other use of this information will be made. Disclosure of the information is voluntary; however, failure to provide the data may delay or preclude access to this project's information.

CLASSIFY WHEN COMPLETED (If required)

SPECIAL ACCESS PROGRAM SECURITY TERMINATION GUIDE

For use of this form, see AR 380-381; the proponent agency is OCSA.

I, the undersigned, fully realize the importance to the National Security of the requirement for the safeguarding of classified defense information. In the fulfillment of this obligation, I certify that:

a. I understand the appropriate provisions of the espionage laws and Federal criminal statutes applicable to the safeguarding of classified defense information or material.

b. I have been advised that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of the designated _____ information by me could cause irreparable injury to the United States and be used to advantage for a foreign nation.

c. I have surrendered and no longer have in my possession, custody, or control any information or material concerning _____

d. I shall not communicate or transmit any classified defense information concerning _____, orally or in writing, to any unauthorized person or in writing, to any unauthorized person or agency.

e. I shall report to my Program Security (OPSEC) Manager, his authorized representative, a local Federal Bureau of Investigation office, or an authorized official as delineated in the _____ LOI, without delay, any incident wherein an attempt is made by an unauthorized person to solicit information concerning this subject.

f. I have received an oral debriefing.

WITNESS:

_____	_____
(signature) (date)	(signature) (date)
_____	_____
(printed name)	(printed name)
_____	_____
(position/organization)	(organization/telephone #/position)
	_____
	(SSN)

PRIVACY ACT STATEMENT.
The authority for obtaining the personal information is Title 10 USC 3012. The principal use of this information is for identification in connection with limited access program information. No other use of this information will be made.

DA FORM 5401-R, JUN 86 EDITION OF MAR 85 IS OBSOLETE.

CLASSIFY WHEN COMPLETED (If required)

Appendix A

References (U)

Section I
Required Publications

(U) AR 70-9 (Army Research Information Systems and Reports). Cited in appendix H, paragraph H-3*d*(3).

(U) AR 380-5 (Information Security Program). Cited in paragraphs 1a(1), 4*b*, 6*a*(6), 6*a*(10), 6*b*(3), and 6*d*(3).

(U) AR 380-49 (Industrial Security Program). Cited in paragraphs 4*e*, and 6*a*(10).

(C) AR 715-30 (Secure Environment Contracting (U)). Cited in paragraph 6*g*(2).

(U) DA Pam 380-381 (Security for Special Access Programs). Cited in paragraph 6*a*(11).

(U) DOD 5200.1-R (Information Security Program). Cited in paragraphs 4*b* and 6*f*(2)(*a*).

(U) DOD 5220.22-M (Industrial Security Program). Cited in paragraphs 1*a*(2), 4*e*, 6*a*(10), and 6*b*(3).

Section II
Related Publications

(U) AR 37-64 (Special Mission Funds (U)).

(U) AR 70-1 (Systems Acquisition Policy and Procedure).

(U) AR 70-10 (Test and Evaluation During Development and Acquisition of Materiel).

(U) AR 71-3 (User Testing).

(U) AR 71-9 (Materiel Objectives and Requirements).

(U) AR 381-10 (Intelligence Activities).

(U) AR 381-11 (Threat Support).

(S) AR 381-102 (Intelligence Operational Support Activities (U)).

(C) AR 381-141 (Intelligence Contingency Funds (U)).

(U) AR 530-1 (Operations Security).

(U) AR 604-5 (Personnel Security Program).

(U) AR 1000-1 (Basic Policies for Systems Acquisition).

(U) DOD 5200.2-R (Personnel Security Program).

Section III
Prescribed Forms

(U) DA Form 5399-R (Special Access Program Initial Security Briefing).

(U) DA Form 5401-R (Special Access Program Security Termination Guide).

Section IV
Referenced Form

(U) DD Form 254 (Department of Defense Contract Security Classification Specification).

Appendix B

Format for Reporting Special Access Programs (U)

(U) Requests for establishing SAPs will be submitted through appropriate Army Staff elements to HQDA(DACS-DMP), WASH DC 20310-0200 in the suggested format shown below.

a. (U) Agency.

b. (U) Unclassified name or short title of program.

c. (U) Date established as a Limited Special Access Program.

d. (U) Relationship, if any, to other programs in DOD or other Government agency.

e. (U) Rationale for establishment of the SAP. (Why normal management and safeguarding procedures for classified information are inadequate must be explained.) Include a brief description of project and the specific requirement for the project with known or anticipated threat.

f. (U) Detailed draft billet structure which incorporates the Army baseline billet structure for SAPs, identifies billets by position, and estimates the number of persons to be granted access. Access control authorities and access approval authorities will be identified.

g. (U) Draft program security plan, classification guide and information systems requirements package (app I).

h. (U) Identify the program security manager, access control authority, and total resources dedicated to OPSEC.

i. (U) Proposed contracting/acquisition plan including recommended contracting office and location. Format in accordance with Federal Acquisition Regulation and Supplements, subpart 7.1. If "carve-out" contracting is proposed, provide rationale.

j. (U) Anticipated cost and proposed funding profile. Include internal audit controls which will be established.

k. (U) Agency POC (position or title, address, and telephone number).

Appendix C

Special Access Programs Oversight Committee (SAPOC) (U)

C-1. (U) Purpose

(U) The SAPOC will provide oversight for the establishment, management, and support of SAPs within DA and maintain an awareness of all sensitive compartmented activities within DA.

C-2. (U) Composition

a. (U) The SAPOC will be chaired by the Vice Chief of Staff, Army (VCSA). In the absence of the VCSA, the Director of the Army Staff will chair the SAPOC. Standing members of the SAPOC will be the GC, ACSI, and TJAG. The remaining members of the SAPOC will be determined on a must "need-to-know" basis from the agenda for each specific meeting and may include:

(1) (U) The ASA (RDA).
(2) (U) The DCSLOG.
(3) (U) The DCSOPS.
(4) (U) The DCSPER.
(5) (U) The DCSRDA.
(6) (U) The ACSIM.
(7) (U) The COA.
(8) (U) The COE.
(9) (U) The Dir, PAED, OCSA.
(10) (U) The CLL.
(11) (U) Representative from TIG.
(12) (U) Others as needed and appropriate.

b. (U) Army Staff principals will ordinarily attend SAPOC meetings unless the principal has delegated SAP matters to an assistant or deputy. In this case the assistant or deputy will be considered the principal for SAPs and the SAPOC Executive Secretary notified accordingly. Only the Army Staff principal or the designated principal for SAPs may attend SAPOC meetings.

c. (U) The Chief, Technology Management Office, will be the Executive Secretary of the Committee.

C-3. (U) Functions

a. (U) *The SAPOC will—*

(1) (U) Review requests for the establishment of SAPs and forward these requests with appropriate recommendations through the Under Secretary of the Army and Chief of Staff, Army to the Secretary of the Army for approval.

(2) (U) Review, assess, and revalidate existing programs annually to determine effectiveness and need for continuation.

(3) (U) Review and recommend policy for management of SAPs.

b. (U) *The committee* is authorized to request information from HQDA agencies and MACOMS in connection with its functions.

C-4. (U) Direction and control

The committee will meet at the call of the chairperson, who will determine the frequency of meetings. After each meeting, minutes will be prepared and submitted to all members of the committee.

C-5. (U) Administrative support

a. (U) The Office of the Chief of Staff, Army is responsible for administrative support of the SAPOC.

b. (U) Funds for travel, per diem, and overtime of members, if required, will be provided by the organization to which the committee member is assigned.

C-6. (U) Correspondence

All communication to the SAPOC will be addressed to HQDA(DACS-DMP), WASH DC 20310-0200.

C-7. (U) Working SAPOC

a. (U) The working SAPOC will be composed on a must "need-to-know" basis from those staff agencies identified in paragraph C-2. The Chief, Technology Management Office, will serve as the chairman of the working SAPOC. Members will be those staff agency representatives who have working knowledge of SAPs and are the dedicated SAP POC within their respective agency. These representatives must possess a final TOP SECRET clearance with current Special Background Investigation.

b. (U) The purpose, functions, direction,and control for the working SAPOC will be the same as for the SAPOC. However, in those instances where the working SAPOC has convened and recommended action, the action will be briefed to the VCSA or the full SAPOC for final approval.

Appendix D

Special Access Program Determination Criteria (U)

D-1. (U) Criteria for Special Access Program Status

(U) The criteria discussed below will be used to screen candidates for special access program status. Following each criterion, a series of questions relevant to that criterion is listed to aid in reaching a decision.

D-2. (U) Criteria

a. (U) Normal management and safeguarding procedures could be insufficient to protect information from compromise.

(1) (U) Would transmission of program documents through normal administrative channels adequately restrict the numbers of people gaining access to the information?

(2) (U) Is the sensitivity of the program such that inadvertent disclosure would endanger a major strategic, tactical, or technological advantage?

(3) (U) Would inadvertent disclosure permit a potential adversary to develop a countermeasure or countercountermeasure so quickly as to negate operational benefit?

(4) (U) Is the proposed activity or program politically sensitive due to foreign policy considerations?

(5) (U) Will the disclosure of our knowledge of a foreign technology compromise sources?

(6) (U) Will the disclosure of information on a specific program have an adverse effect on other SAP protected programs?

(7) (U) Is there an existing vulnerability in the U.S. system the disclosure of which would give an adversary a significant advantage?

(8) (U) Would acquisition of the technology, system, or information by hostile elements endanger the military capability of U.S. forces or create a threat to national security?

b. (U) The numbers of persons requiring access must be reasonably small and commensurate with the objective of providing extra protection for the information involved.

(1) (U) Is it feasible to limit the number of people both within any one organization and in total who have access to the information?

(2) (U) Is the potential loss in efficiency caused by compartmentation acceptable?

(3) (U) Has the proposed activity already received a degree of public or internal military exposure that would be infeasible to overcome?

(4) (U) Is it possible to develop, produce, or field the system without a large number of people gaining access?

c. (U) Special access controls must be needed to protect the information when balanced against the requirement to disseminate for use that same information and the additional cost of special access controls.

(1) (U) Would the proposed activity conceal technology or only a discrete application?

(2) (U) How would the proposed activity interface with related developments?

(3) (U) Is the proposed activity of multi-service interest? If so, how are similar projects in those services being handled?

D-3. (U) Impact of Special Access Program Status

(U) A decision to make an activity a special access program will result in some combination of the following actions, which will be restrictive as well as protective in nature.

a. (U) Central control will be exercised over access to information. Generally, more stringent security clearance requirements will be imposed on participants.

b. (U) The following information will be concealed from those not authorized access:

(1) (U) The fact and purpose of the undertaking;

(2) (U) The resources allocated to, and the organizations involved in, the undertaking; and

(3) (U) The characteristics, capabilities, and effectiveness of the product developed by the undertaking.

c. (U) Operations security measures will be applied.

[redacted]

Appendix E

Technology Management Office (U)

(U) The Technology Management Office (TMO) has been established within the Office of the Chief of Staff, Army and reports directly to the Vice Chief of Staff, Army. The TMO charter includes the following responsibilities:

a. (U) Serve as the central point of contact for all initial inquiries and correspondence concerning Army sponsored or supported Special Access Programs (SAP).

[redacted]

c. [redacted]

d. (U) Provide Executive Secretary of Special Access Program Oversight Committee (Chief, TMO).

e. (U) Monitor audit review, analysis, and oversight of planning, programming, budgeting, and execution of SAPs.

f. (U) Coordinate requirements for and monitor all Congressional SAP briefings.

g. (U) Coordinate and assist in the development of models for resourcing and financing SAPs.

h. (U) Monitor all program and budget elements and financing associated with SAPs, unless exempted by the Under Secretary of the Army.

[redacted]

j. [redacted]

k. (U) Serve as POC to DUSD(P) for all Army initiated and supported SAPs and "carve-out" contracts.

l. (U) Serve as proponent for AR 380-381(C).

[redacted]

Appendix F

Limited Special Access Program (U)

F-1. (U) Limited Special Access Programs (LSAP) may be applied for by a MACOM commander or Department of the Army Deputy or Assistant Chief of Staff for a period not to exceed 6 months. Application is made to the Technology Management Office (TMO). The TMO will notify the SAPOC at the first meeting after an LSAP is registered for SAPOC approval to continue as an LSAP and to begin SAP evaluations.

a. (U) The LSAP request consists of no more than a two-page description outlining the proposed program, estimated schedule, estimated funding, reason for compartmentation, and any other relevant issues.

b. (U) Until the LSAP is approved, funds may be expended just as for any other non-compartmented program. Funds may not be expended for a program operated in accordance with compartmented procedures in this regulation unless approved as an LSAP or SAP.

c. (U) If the SAPOC approves continuation of an LSAP, the TMO will notify the Under Secretary of the Army. The LSAP proponent will then prepare SAP evaluation documents required by appendix B.

F-2. (U) The criteria for an LSAP are the same as for a SAP and are discussed in paragraphs 1 and 4 and appendix D of this regulation. The key factor in determining whether or not to establish an LSAP is the potential for and damage resulting from compromise.

F-3. (U) During the 6-month period authorized for an LSAP, the program should be evaluated for approval as a SAP. If at the end of 6 months the program has not been formally submitted, the LSAP will be terminated, and no further resources will be committed to or used for wo related to making that program a SAP.

F-4. (U) MACOM commanders and Department of t Army Deputy and Assistant Chiefs of Staff must publish pr gram management guidance, security plans and classific tion guides, and initial billet structures for the establishme of LSAPs, and this guidance must be filed with th Technology Management Office.

F-5. (U) Authorities granted in approval of an LSA include:

a. (U) Appointment of access approval authorities.

b. (U) Access limitation based on a must need-to-know

c. (U) Maintenance of knowledgeability lists.

d. (U) Preparation of draft security plan, classificatio guide, and billet structure with identified access contro authorities and access approval authorities.

e. (U) Use of approved special markings along with nor mal security classification.

f. (U) Initial coordination with INSCOM for counter intelligence support and cover support.

g. (U) Use of a DA approved nickname.

F-6. (U) The following authorities are withheld pending final approval of an LSAP as a SAP.

a. (U) Use of signed initial security briefing statements.

b. (U) The use of "carve-out" contracts.

F-7. (U) Request for waivers on LSAP requirements will be submitted to HQDA (DACS-DMP).

Appendix G

Format for Annual SAPOC Revalidation (U)

(Classify when completed)

G-1. (U) Codeword (S) and nickname (U).

G-2. (U) State of threat and enemy technology.

G-3. (U) Access and security status.
a. (U) Total number with access.
b. (U) Compromises (actual/potential) to date.
c. (U) HOIS threat.
d. (U) OPSEC support to date (description and cost).
e. (U) Special security provisions.
f. (U) "Carve-out" contract provisions and an alternate security inspection plan.

G-4. (U) Description of Program.
a. (U) Requirement.
b. (U) How it works.
c. (U) Potential value (tactical and technical lead).

G-5. (U) Program schedule with key milestones.
a. (U) Status at last review.
b. (U) Response to actions directed by SAPOC.
c. (U) Status now.

G-6. (U) Funding Profile.
a. (U) Indicate what is already programmed (amount and how funded—by PE, through lab, reprogramming, etc.).
b. (U) Show requirements, if different from programmed funding.
c. (U) SMF status.

G-7. (U) Contracting Procedures.
a. (U) Contracting officer and location.
b. (U) "Carve-out" contracting procedures.
c. (U) Contract and its schedule and performance.

G-8. (U) Issues/Problems.
a. (U) Technical.
b. (U) Programmatic.
c. (U) Funding.
d. (U) Legal.
e. (U) Contracting.

G-9. (U) Required Decisions.
a. (U) Options.
b. (U) Recommendations.

Appendix H

Special Access Program Disestablishment (U)

H-1. (U) General

(U) This appendix provides policy and procedures for planning and implementing disestablishment of Special Access Programs (SAP).

H-2. (C) Rationale

a.

b. (U) The tactical or strategic impact or value of the system, operation, or activity has significantly lessened.

c.

d. (U) The resources required for continued enhanced security procedures are excessive compared to the benefits achieved by the SAP process.

e. (U) Similar technology and application is being developed openly by other services or foreign nations or being developed without equivalent levels of protection.

f. (U) A compromise has occurred that obviates the protection achieved by continued enhanced security.

g. (U) The tactical or strategic mission of the system, operation or activity has been accomplished and there is no further mission requirement.

h. (U) The system has been fielded and operational use at the tactical or strategic levels precludes compartmentation.

H-3. (U) Procedures

a.

b.

c.

(1) (U) Basis/rationale for disestablishment.

(2) (U) Control of information relating to disestablishment.

(3) (U) Fiscal controls.

(4) (U) Recommended disposition of information and access knowledgeability lists or rosters.

(5) (U) Disposition of hardware resulting from RDT&E to date.

(6) (U) Recommendation whether the program should continue as a classified program, be downgraded to an unclassified program, cease entirely or be held in abeyance pending future technological advances.

(7) (U) Legal considerations.

(8) (U) Verification that similar technology, development or application is not underway elsewhere within DOD and receiving special access security protection.

(9) (U) Review of all contracts and recommendations made regarding termination, transfer or continuation.

d.

[redacted]

(1) (U) A letter of instruction (LOI) must be prepared which:

(*a*) (U) Establishes administrative and operational criteria to be effected during disestablishment.

(*b*) (U) Establishes new criteria for administrative and operational protection of the program or activity.

(2) (U) A new classification guide must be prepared.

(3) (U) Proponents must consider the inclusion of program technical data in Army research information systems and reports in accordance with AR 70-9 (1 May 81).

(4) [redacted]

[redacted]

(5) (U) Contractual documents may require modification or renegotiation. Modification must include the applicable DD Form 254 for revised security requirements. Integral to this consideration are the return or reallocation of government furnished equipment (GFE), (e.g., secure communications equipment) and the cancellation of the requirement for a closed work area.

(6) (U) Reprogramming of project funds and the cancellation of letters of authorization (LOA) and expenditure authorization documents (EAD) pertaining to special mission funds (SMF).

e. (U) Once disestablishment has been effected, the TMO will be notified by record correspondence.

[redacted]

Appendix I

Information Systems Requirements Package (U)

(U) Early identification of secure information requirements is essential to provide adequate and reliable point to point secure voice line, data and facsimile transmission. Inclusion of the data outlined in the Information Systems Requirements Package, will assist in providing these services in a secure and timely manner. The format and information to be included in an Information Systems Requirements Package is shown at figure I-1.

Format for an Information Systems Requirements Package (U)

1. (U) General.
   a. (U) Name of project proponent.
   b. (U) Project participants (agency name, address, point of contact and secure/nonsecure telephone numbers).
   c. (U) Unclassified name or short title of program.

2. (U) Scope of Requirement.

3. (U) Urgency.
   a. (U) Priority of need.
   b. (U) Implementation:
      (1) (U) Date of initial operational capability required.
      (2) (U) Date final operational capability required.
      (3) (U) Impact if service is not provided.

4. (U) Capability.
   a. (U) Show the common user or dedicated communication electronic capabilities that presently exist or are available to proponent and participants.
   b. (U) Indicate how these capabilities satisfy any portion of this requirement in their present or modified state.

5. (U) Security Management.
   a. (U) Name of security manager.
   b. (U) Provide a copy of the program security plan and classification guide.

6. (U) Financial.

(U) Identify funding type, source, and control for information systems.

7. (U) Procurement.

(U) Identify unique security or OPSEC requirements.

8. (U) Accountability.

(U) Describe the desired or planned concept for property accountability.

9. (U) Technical.
   a. (U) Show type of service required (Secure and/or nonsecure data, voice, facsimile, radio, satellite, AUTOVON, or AUTODIN).
   b. (U) Describe type of traffic to be transported. (Text or narrative, magnetic tape, punched card, graphic, maps, imagery, drawings, photographic).
   c. (U) Identify interfaces with existing systems, networks, or equipment.
   d. (U) Describe any different capabilities required for different phases of the project.

Figure I-1. (U)

10. (U) Operations and Security.
   a. (U) Operational concept (fixed, transportable, or mobile).
   b. (U) Identify service points or end user locations (covert, clandestine or classified).
   c. (U) Determine if there is a requirement for a Sensitive Compartmented Information Facility (SCIF).
   d. (U) Identify the program security and OPSEC parameters or restrictions.
   e. (U) Classification level of information to be passed.
   f. (U) Operating hours.
   g. (U) Operators.
   h. (U) Determine if redundant systems are required.
   i. (U) Identify the network control facility (if needed).

11. (U) Maintenance.
   a. (U) Identify unique security or OPSEC requirements for maintenance.
   b. (U) Identify organic maintenance support capability.
   c. (U) Determine the response time needed to restore telecommunications and meet mission requirements.

Figure I-1 (Continued) (U)

[redacted]

(U) Covert operations

(U) Operations that are so planned and executed as to conceal the identify of or permit plausible denial by the sponsor. They differ from clandestine operations in that the emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation.

(U) Intelligence

(U) The product resulting from collection, processing, intergration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas, particularly its technology and weapon systems.

(U) Operations security (OPSEC)

(U) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

(U) Threat

(U) Capability of a potential enemy to limit or negate mission accomplishment, or to neutralize or reduce the effectiveness of a current or projected organization or material item. Two types of threat information are required, as shown below.

a. (U) Intelligence collection threat (efforts by HOIS to gain information on U.S weapon systems).

b. (U) Combat capability threat (hostile forces' weapon systems the U.S. Army will face on the battlefield).

Glossary 2

[redacted]