

Security

Special Access Programs (SAPs)

Headquarters
Department of the Army
Washington, DC
12 October 1998

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-381

Special Access Programs (SAPs)

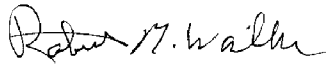
This regulation--

- o Contains extensive new and updated information on establishing, maintaining, supporting, and disestablishing Special Access Programs (SAPs).
- o Implements applicable portions of Department of Defense Directive 5205.7.

Effective 13 November 1998

Security

Special Access Programs (SAPs)



Robert M. Walker
Acting Secretary of the Army

History. This publication is a revision of AR 380–381, dated 4 December 1992.

Summary. This regulation sets forth the implementing instructions and procedures for establishing, maintaining, supporting, and disestablishing Special Access Programs

(SAPs). This regulation implements applicable parts of Department of Defense Directive 5205.7.

Applicability. This regulation applies to units and activities of the Active Army, Army National Guard of the United States, and the U.S. Army Reserve. It also applies to Army or joint program contractors and consultants when contract performance depends on access to a SAP.

Proponent and exception authority. The proponent of this regulation is the Chief of Staff, Army (CSA). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponents may delegate the approval authority, in writing, to a division chief within the proponent agency in the grade of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated.

Supplementation. Supplementation of this

regulation and establishment of command and local forms are prohibited without prior approval of the Secretary of the Army.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Chief, Technology Management Office (DACS–DMP), 200 Army Pentagon, Washington, DC 20310–0200.

Committee Continuance Approval. The DA Committee Management Officer concurs in the continuance of the Special Access Program Oversight Committee, the Fix-It Committee, and the SAP Program Performance and Budget Execution Review System Committee established by AR 380–381.

Distribution. Distribution of this publication is made in accordance with Initial Distribution Number (IDN) 091030 for command levels D and E, for the Active Army, Army National Guard of the U.S., and U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1–1, page 1

References • 1–2, page 1

Explanation of abbreviations and terms • 1–3, page 1

Restrictions on using Special Access Programs • 1–4, page 1

Chapter 2

Responsibilities, page 1

The Secretary of the Army • 2–1, page 1

The Under Secretary of the Army • 2–2, page 1

The Assistant Secretary of the Army (Research, Development, and Acquisition) • 2–3, page 1

The Assistant Secretary of the Army (Manpower and Reserve Affairs) • 2–4, page 1

The Assistant Secretary of the Army (Financial Management and Comptroller) • 2–5, page 1

The Director of Information Systems for Command, Control, Communications, and Computers • 2–6, page 1

The General Counsel • 2–7, page 2

The Inspector General • 2–8, page 2

The Auditor General • 2–9, page 2

Chief of Public Affairs • 2–10, page 2

The Chief of Staff, Army • 2–11, page 2

The Vice Chief of Staff, Army • 2–12, page 2

The Deputy Chief of Staff for Personnel • 2–13, page 2

The Deputy Chief of Staff for Intelligence • 2–14, page 2

The Deputy Chief of Staff for Operations and Plans • 2–15, page 2

The Deputy Chief of Staff for Logistics • 2–16, page 2

Chief of Engineers • 2–17, page 2

The Judge Advocate General • 2–18, page 2

Chief of Legislative Liaison • 2–19, page 2

Director, Program Analysis and Evaluation Directorate • 2–20, page 2

Chief, Technology Management Office • 2–21, page 3

Commanding General, U.S. Army Training and Doctrine Command • 2–22, page 3

Commanding General, U.S. Army Materiel Command • 2–23, page 3

Commanding General, Forces Command • 2–24, page 3

Commanding General, U.S. Army Space and Missile Defense Command • 2–25, page 3

Commanding General, U.S. Army Intelligence and Security Command • 2–26, page 3

Commanding General, U.S. Army Criminal Investigation Command • 2–27, page 3

Department of the Army Staff • 2–28, page 3

Major Army Commands and program executive officers • 2–29, page 3

*This regulation supersedes AR 380–381, dated 4 December 1992.

Contents—Continued

Program/Project/Product Managers of SAPs • 2–30, *page 4*
Sensitive Records and Information Agency • 2–31, *page 4*
Defense Security Service • 2–32, *page 4*

Chapter 3

Special Access Program Design, *page 4*

Purpose • 3–1, *page 4*
SAP types • 3–2, *page 4*
SAP categories • 3–3, *page 4*

Chapter 4

SAP Life Cycle, *page 4*

Establishment phase • 4–1, *page 5*
Maintenance Phase • 4–2, *page 5*
Disestablishment • 4–3, *page 7*
Joint SAP Management • 4–4, *page 8*

Chapter 5

SAP Security, *page 8*

Programs ineligible for SAP security • 5–1, *page 8*
Physical security • 5–2, *page 8*
Document/information security • 5–3, *page 9*
Personnel security • 5–4, *page 10*
Technical security • 5–5, *page 10*
Treaties • 5–6, *page 10*
Technology Transfer/Foreign Disclosure • 5–7, *page 11*
Program security plan • 5–8, *page 11*
Security incidents involving SAP information • 5–9, *page 12*

Chapter 6

Access Control, *page 13*

Validation of access requirements • 6–1, *page 13*
Access levels • 6–2, *page 13*
Billet structure • 6–3, *page 14*
Rosters • 6–4, *page 14*
Request for access • 6–5, *page 14*
Indoctrination • 6–6, *page 14*
Termination • 6–7, *page 15*
Billet structure management system • 6–8, *page 15*

Chapter 7

Industrial Security, *page 15*

Defense contractors • 7–1, *page 15*
National Industrial Security Program • 7–2, *page 15*
Contractor Personnel Security • 7–3, *page 15*
Physical Security • 7–4, *page 15*
Industrial Security Inspections • 7–5, *page 15*
Contract Management • 7–6, *page 16*
Security infractions, violations, and compromises at contractor facilities • 7–7, *page 16*
Contract security requirements • 7–8, *page 16*

Chapter 8

Information Mission Area, *page 16*

General • 8–1, *page 16*
Information Systems Requirements Package • 8–2, *page 17*
Information Management Support Plan • 8–3, *page 17*
Accreditation • 8–4, *page 17*
System Maintenance • 8–5, *page 17*
Information Management support • 8–6, *page 17*
Records management • 8–7, *page 17*

Chapter 9

Funding, *page 18*

SAP funding • 9–1, *page 18*
Establishment phase • 9–2, *page 18*
Maintenance phase • 9–3, *page 18*
Disestablishment • 9–4, *page 18*

Annual SAP reports • 9–5, *page 18*

Appendixes

- A. References, *page 19*
- B. Establishment, *page 20*
- C. Management Control Evaluation Checklist, *page 21*
- D. Format for SAPOC Briefing, *page 22*
- E. Guidance on Preparing the Standard SAPOC Slide (QUAD Chart), *page 29*
- F. Disestablishment Concept Plan, *page 30*
- G. Disestablishment Certification Checklist, *page 30*
- H. Program Performance and Budget Execution Review System Charts, *page 31*
- I. Reprogramming Request Format, *page 34*
- J. Fix-It Status Sheets, *page 35*
- K. Format for Information Systems Requirements Package, *page 36*
- L. Format for Information Management Support Plan, *page 36*

Table List

Table 5–1: SAP security matrix, *page 12*
Table B–1: SAP establishment timeline, *page 20*

Figure List

Figure D–1: Program description, *page 22*
Figure D–2: Justification for SAP category, *page 23*
Figure D–3: Relationship to other programs, *page 23*
Figure D–4: Foreign targets and technology, *page 24*
Figure D–5: External threat assessment, *page 24*
Figure D–6: Security assessment, *page 25*
Figure D–7: Access status, *page 25*
Figure D–8: Milestone chart, *page 26*
Figure D–9: Funding profile, *page 26*
Figure D–10: Manpower profile, *page 27*
Figure D–11: Contracting, *page 27*
Figure D–12: SAP inspections and audits, *page 28*
Figure D–13: Issues/problems, *page 28*
Figure D–14: Decision sought, *page 29*
Figure E–1: Quad chart, *page 30*
Figure H–1: RDTE PPBERS chart (example), *page 32*
Figure H–2: OMA PPBERS chart (example), *page 33*
Figure I–1: Sample reprogramming request, *page 34*
Figure J–1: Sample Fix-It Status Sheet, *page 35*

Glossary

Index

Chapter 1 Introduction

1-1. Purpose

This regulation sets forth the implementing instructions and procedures for establishing, maintaining, supporting, and disestablishing Army Special Access Programs (SAPs).

1-2. References

Required and related publications and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the Glossary.

1-4. Restrictions on using Special Access Programs

a. Only approved Prospective Special Access Programs (PSAPs) and SAPs may use the extraordinary security measures outlined in this regulation.

b. Proponents of acquisition, intelligence, or operations and support activities who identify a particularly sensitive piece of information that they believe merits SAP protection should report this information through the chain of command for a security policy review. If a determination is made that the information warrants SAP controls, the Major Army Command (MACOM)/Program Executive Office (PEO) reports this to Chief, Technology Management Office (TMO), who coordinates a security review at HQDA. Some examples of potential SAPs are—

(1) A specific technology with potential for weaponization that gives the United States a significant technical lead or tactical advantage over potential adversaries.

(2) Sensitive technology that is especially vulnerable to foreign intelligence exploitation without special protection.

(3) An emerging technology, proposed operation, or intelligence activity risking the compromise of other SAPs.

(4) Exposure of sensitive activities that could jeopardize the lives of U.S. citizens.

(5) A capability that is so unique or sensitive that it requires protection beyond normal procedures.

(6) An extremely sensitive activity requiring special protection from disclosure to prevent significant damage to national security or the reputation or interests of the United States.

(7) Methods used to acquire foreign technology or equipment.

(8) Sensitive support to DOD and non-DOD agencies.

c. In compliance with DOD policy, HQDA and its subordinate units and activities will not establish, disestablish, implement, fund, categorize, create carve-out status, or change the mission or scope of a SAP without written approval of the Deputy Secretary of Defense (DEPSECDEF).

Chapter 2 Responsibilities

2-1. The Secretary of the Army

The Secretary of the Army (SA) has overall responsibility for SAPs within the Department of the Army. The SA will—

a. Make recommendations to the DEPSECDEF concerning the establishment, disestablishment, categorization, carve-out status, and changes of mission and scope of Army SAPs.

b. Ensure adequate oversight of Army SAPs.

c. Delegate, at SA discretion, management of Army SAPs.

2-2. The Under Secretary of the Army

The Under Secretary of the Army (USA) will—

a. Approve SAP reprogramming actions.

b. Serve as co-chairman of the SAP Program Performance and Budget Execution Review System (PPBERS).

2-3. The Assistant Secretary of the Army (Research, Development, and Acquisition)

The Assistant Secretary of the Army (Research, Development, and Acquisition (ASA(RDA))) will—

a. Serve as the Army Acquisition Executive for all Army programs, including SAPs, and as the principal assistant to the SA for matters relating to Acquisition SAPs (AQ-SAP).

b. Ensure a single subordinate commander of a major Army command (MACOM) or program executive officer (PEO) is responsible for each AQ-SAP throughout its life cycle.

c. Conduct periodic reviews of secure environment contracting conducted in support of SAPs.

d. Ensure SAP protection and procedures for procurement and fielding of systems, components, and modifications are developed and acquired under SAP provisions.

e. Coordinate with the Office of the Deputy Chief of Staff for Intelligence (ODCSINT) on issues concerning technology transfer.

f. Coordinate within Army and other DOD components to eliminate duplication of effort and ensure consistent security classification for similar technologies.

g. Coordinate technical review of PSAPs.

h. Evaluate proposed acquisition strategies and plans for Army SAPs.

i. Coordinate with Office of the Deputy Chief of Staff for Logistics (ODCSLOG) to integrate logistics support and property accountability considerations into AQ-SAP efforts and products.

2-4. The Assistant Secretary of the Army (Manpower and Reserve Affairs)

The Assistant Secretary of the Army (Manpower and Reserve Affairs) (ASA(M&RA)) will—

a. Review and assist in developing policy regarding personnel and personnel security support to SAPs.

b. Provide guidance concerning the documentation process to ensure that Tables of Distribution of Allowances accurately reflect Army requirements consistent with approved SAP missions and the Army Authorization Document.

c. Evaluate and approve requests for special pays, as appropriate, in support of SAP missions.

d. In coordination with the ASA(FM&C), assist in establishing guidance to ensure proper control and accountability of financial data pertaining to Army personnel assigned to SAPs.

2-5. The Assistant Secretary of the Army (Financial Management and Comptroller)

The Assistant Secretary of the Army (Financial Management and Comptroller) (ASA(FM&C)) will—

a. Provide financial and budget policy and guidance for SAPs.

b. Provide liaison with Congress for SAP budgets.

c. Coordinate with Defense Finance and Accounting (DFAS) to ensure DFAS provides a secure finance and accounting network to process sensitive financial transactions.

d. Provide financial quality assurance oversight through the Special Review Office (SRO).

e. Coordinate the Army's Budget Estimate Submission for SAPs with OSD.

2-6. The Director of Information Systems for Command, Control, Communications, and Computers

The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) will—

a. Coordinate information systems support for SAPs.

b. Assist TMO in developing information systems policy for SAPs.

c. Validate and approve Information System Support Plans (ISSPs).

d. Through USACECOM Technology Applications Office (TAO):

(1) Provide information management support in preparing Information Systems Requirements Packages (ISRPs) and Information Management Support Plans (IMSPs).

(2) Provide technical advice and support in preparing ISRPs and IMSPs.

2-7. The General Counsel

The General Counsel (GC) will—

- a. Review Army SAPs and prospective Army SAPs for legality and propriety before submission to OSD.
- b. Advise the SA on legal and policy issues.
- c. Conduct policy reviews.

2-8. The Inspector General

The Inspector General (TIG) will—

- a. Evaluate managerial procedures and practices pertaining to operations, personnel, materiel, funding, secure environment, contracting, and security of SAPs.
- b. Identify issues, situations, or circumstances that affect SAP mission performance.
- c. Provide a secure system for program personnel to report fraud, waste, and abuse without fear of reprisal or unnecessary disclosure of information.
- d. Conduct non-criminal investigations as directed by the Vice Chief of Staff, Army.
- e. Inspect Army SAPs and Army involvement in non-Army SAPs.
- f. Develop and coordinate an annual inspection plan with TMO, other inspection/audit agencies, MACOMs, and PEOs.

2-9. The Auditor General

The Auditor General (TAG) will—

- a. Maintain auditors with appropriate clearance and access to perform audits of SAPs.
- b. Coordinate with TMO when performing audits of SAPs.

2-10. Chief of Public Affairs

The Chief of Public Affairs (PA) will—

- a. Staff media queries on SAPs and provide releasable information.
- b. Provide public affairs guidance on SAP matters.

2-11. The Chief of Staff, Army

The Chief of Staff, Army (CSA) will develop, coordinate, review, and conduct oversight of all Army SAPs.

2-12. The Vice Chief of Staff, Army

The Vice Chief of Staff, Army (VCSA) will—

- a. Review SAPs through the Special Access Program Oversight Committee (SAPOC) and serve as chairman of the SAPOC.
- b. Serve as the chairman of the Executive Fix-It Committee.
- c. Serve as the co-chairman of the SAP PPBERS.
- d. Provide guidance and direction to Chief, TMO.

2-13. The Deputy Chief of Staff for Personnel

The Deputy Chief of Staff for Personnel (DCSPER) will—

- a. Provide policy on SAP personnel matters.
- b. Coordinate with ODCSOPS to establish procedures ensuring MACOM SAPs properly use allocated personnel spaces to resource the SAPs.
- c. Ensure that the U.S. Army Total Personnel Command (PERSCOM) coordinates designated DA approved personnel assignment actions for SAPs.

2-14. The Deputy Chief of Staff for Intelligence

The Deputy Chief of Staff for Intelligence (DCSINT) will—

- a. Oversee Army Intelligence SAPs (IN-SAPs) and serve as IN-SAP Army Staff (ARSTAF) proponent.
- b. Establish security, counterintelligence, and intelligence policy for SAPs.
- c. Coordinate necessary counterintelligence support for the execution of Army SAPs.
- d. Provide OPSEC and threat assessments for responsible

MACOMs and program managers to SAPs and present these to the Working SAPOC for inclusion in the SAPOC revalidation briefing.

- e. Advise the SAPOC on whether a program or activity warrants SAP protection.
- f. Review SAP security plans and guides for accuracy and completeness.
- g. Provide input as requested to Office of the Deputy Under Secretary of Defense for Policy (Policy Support) (ODUSD(P)(PS)) concerning Army SAP security classification guides.
- h. Coordinate intelligence property issues for Army SAPs with DCSLOG.
- i. Coordinate policy for polygraph support to Army SAPs.
- j. Review and approve disclosure of official Army information (classified and unclassified) for release to foreign governments and international agencies. Coordinate with TMO and Director for Special Programs, Office of the Under Secretary of Defense for Policy (Policy Support)(OTUSD(P)(PS)) for release of information and technology identified by SAP proponents for release to foreign governments and international agencies.

2-15. The Deputy Chief of Staff for Operations and Plans

The Deputy Chief of Staff for Operations and Plans (DSCOPS) will—

- a. Oversee Operations and Support SAPs (OS-SAPs) and serve as the ARSTAF proponent.
- b. Provide policy guidance and standards for operations security (OPSEC) measures appropriate for Army SAPs.
- c. Develop Army policy and guidance for materiel requirements for SAPs.
- d. Establish and validate Army acquisition priorities for SAPs.
- e. Coordinate and approve manpower requirements, allocate manpower resources, and prepare tables of distribution and allowances (TDA) documents for SAPs.
- f. Conduct manpower and workload validations of SAPs to support HQDA and PEO/PMs.
- g. Task U.S. Army Force Management Support Agency (USAFMSA) to provide necessary support and analysis of SAP manpower requirements.

2-16. The Deputy Chief of Staff for Logistics

The Deputy Chief of Staff for Logistics (DCSLOG) will—

- a. Integrate logistics support for all Army materiel development or acquisition for SAPs.
- b. Provide policy guidance on property accountability and logistics support for SAPs.

2-17. Chief of Engineers

The Chief of Engineers (COE) will provide secure architectural-engineering, construction, real estate, and contracting support to SAPs as required.

2-18. The Judge Advocate General

The Judge Advocate General (TJAG) will provide legal and policy advice on SAP matters to CSA and the ARSTAF.

2-19. Chief of Legislative Liaison

The Chief of Legislative Liaison (CLL) will—

- a. Coordinate congressional briefings on Army SAPs.
- b. Provide required reports to selected congressional committees on Army SAPs.
- c. Assist TMO in updating clearance information for individuals in Congress accessed to Army SAPs.
- d. Assist TMO in verifying access of individuals in Congress.

2-20. Director, Program Analysis and Evaluation Directorate

The Director, Program Analysis and Evaluation Directorate (PAED), will—

- a. Ensure that SAPs compete with other Army programs for resources in the Program Objective Memorandum (POM) development process.

- b. Coordinate with the ARSTAF and TMO to develop SAP program funding profiles and provide copies of approved profiles to TMO.
- c. Provide program analyses for reprogramming actions.
- d. Coordinate SAP POM during the program review process with OSD.

2-21. Chief, Technology Management Office

The Chief, Technology Management Office (TMO), will—

- a. Serve as the Army primary point of contact for the management and oversight of Army and Army-supported SAPs.
- b. Establish policy for the management of SAPs.
- c. Coordinate establishment, maintenance, and disestablishment of SAPs.
- d. Act as the approval authority for establishment and disestablishment of Army PSAPs.
- e. Approve the creation or closure of SAP subcompartments when there is no change to the categorization, carve-out status, mission, or scope of the parent SAP. In cases where creation or closure of a subcompartment will change the mission or scope of the parent SAP, Chief, TMO will submit the action through SA to the Deputy Secretary of Defense for approval.
- f. Serve as the Executive Secretary for the SAPOC, SAP PPBERS, and Fix-It committees.
- g. Provide quarterly update reviews to the senior Army leadership.
- h. Assist CLL in coordinating congressional SAP access briefings and congressional notifications.
- i. Monitor budget and financing associated with SAPs.
- j. Review SAPs for compliance with authorizations, legal constraints, funding, and continued enhanced security measures.
- k. Serve as the POC for Army sensitive support to DOD and non-DOD agencies.
- l. Maintain a registry of Army involvement in SAPs and sensitive activities.
- m. Maintain the Army baseline billet roster.
- n. Coordinate indoctrination of ARSTAF principals to Army SAPs.
- o. Direct the Sensitive Records and Information Agency (SRIA).

2-22. Commanding General, U.S. Army Training and Doctrine Command

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

- a. Institute procedures to ensure early identification and protection of combat developments, concepts, and systems with SAP potential.
- b. Identify support requirements for SAP-developed products deployed to the field.

2-23. Commanding General, U.S. Army Materiel Command

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

- a. Institute procedures to ensure early identification and protection of potential research and development (R&D) breakthroughs that may warrant SAP protection.
- b. Conduct appropriate technology feasibility reviews of AMC SAPs.
- c. Provide support and oversight for AMC SAPs.

2-24. Commanding General, Forces Command

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

2-25. Commanding General, U.S. Army Space and Missile Defense Command

The Commanding General, U.S. Army Space and Missile Defense Command (USASMDC), will institute procedures to ensure early

identification and protection of potential R&D breakthroughs within the USASMDC that may warrant SAP protection and coordinate potential release of SAR information through DA DCSINT to SARD-SO and TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. DA DCSINT will coordinate, as required, with Director for Special Programs, OTUSD(P)(PS), prior to any release.

2-26. Commanding General, U.S. Army Intelligence and Security Command

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

- a. Institute procedures to ensure early identification and protection of sensitive intelligence activities that may warrant SAP protection.
- b. Provide dedicated counterintelligence, security, and OPSEC support to commanders, program managers, or heads of DA activities having proponentcy for Army SAPs or Army supported SAPs. This support includes counterintelligence (CI) assessments of Army SAPs, PSAPs and contractor facilities involved in Army SAP contracts.
- c. Provide DCSINT with counterintelligence assessments of the threat posed to SAPs by Foreign Intelligence Services (FIS) and technology assessments of foreign research and development efforts related to SAP technologies. Coordinate with DCSINT to provide this information to organizations and installations supporting SAPs.
- d. Provide to DCSINT an annual counterintelligence (CI) evaluation of the OPSEC and security posture of Army SAPs and Army-supported SAPs.
- e. Manage and execute the Army polygraph program in support of SAPs.
- f. Provide technical surveillance countermeasures (TSCM), TEMPEST, ADP security and counter-SIGINT support to SAPs.
- g. Conduct security reviews of SAP disestablishment actions, security plans, and CI support plans.

2-27. Commanding General, U.S. Army Criminal Investigation Command

The Commanding General, U.S. Army Criminal Investigation Command (CG, USACIC), will—

- a. Maintain criminal investigators with appropriate clearances and access to conduct investigations of criminal activity in or directed against SAPs.
- b. Maintain effective liaison, through individuals well acquainted with special access procedures, with TMO to ensure quick response to investigative requirements.
- c. Conduct criminal investigations in all instances of suspected criminal activity in or directed against Army SAPs in accordance with applicable Federal statutes, DOD Directive 5205.7, DOD Instruction 5505.2 and AR 195-2.
- d. Conduct periodic economic crime threat assessments.
- e. Coordinate with TMO to conduct crime prevention surveys on SAPs.

2-28. Department of the Army Staff

The ARSTAF sections having SAP proponentcy or support requirements for SAPs will—

- a. Designate a central point of contact for SAPs.
- b. Provide appropriate staff oversight for the planning, programming, budgeting, and execution of SAPs.
- c. Act as SAP managers when appointed to do so.

2-29. Major Army Commands and program executive officers

The MACOMS and program executive officers (PEOs) who supervise managers of SAPs will—

- a. Assist program managers in managing their programs.
- b. Establish internal inspection programs for SAPs.
- c. Conduct periodic property reviews to validate new requirements and document materiel assets in support of SAPs.

d. Coordinate with ARSTAF proponents and DCSINT for SAP intelligence, counterintelligence, and threat assessments.

e. Ensure that all SAPs are incorporated into the Internal Review and Audit Compliance (IRAC) program as described in chapter 4.

f. Coordinate potential release of SAR information through DA DCSINT to SARD-SO and TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. DA DCSINT will coordinate with Director for Special Programs, OTUSD(P)(PS), prior to any release.

g. Coordinate with USAFMSA for manpower support for TDA documentation.

2-30. Program/Project/Product Managers of SAPs

In addition to the duties and responsibilities normally incumbent on managers and those delineated by law and regulation, Program/Project/Product Managers (PMs) of SAPs will—

a. Maintain essential SAP information including establishment, documentation, security plans, access rosters, and security inspection records.

b. Plan, prepare, and implement security and OPSEC programs designed to protect critical program information.

c. Coordinate with TMO for information systems advice and support.

d. Establish and maintain a viable records management program.

e. Coordinate with SRIA for records management assistance.

f. Coordinate with the Defense Security Service (DSS) for industrial facility reviews.

g. Identify, establish, maintain, and forward to the SAP Archive, SRIA, appropriate historical record files pertaining to the program and its operations.

h. Coordinate potential release of SAR information through DA DCSINT to SARD-SO and TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. DA DCSINT will coordinate with Director for Special Programs, OTUSD(P)(PS), prior to any release.

2-31. Sensitive Records and Information Agency

The SRIA will—

a. Operate the Army Records Center for Sensitive Records and Information. Accept, review, process, archive, and destroy Army sensitive records in accordance with DOD Directive 5205.7, AR 380-381, and AR 25-400-2. Respond to requests for information. Conduct records review and disposition.

b. Conduct Army-wide document searches for sensitive information. Compile and prepare document indexes and responsive documents for forwarding to requesting agencies. Coordinate declassification reviews.

c. Maintain the Billet Structure Management System (BSMS) for the Army. Develop, maintain and distribute the BSMS system software. Identify BSMS hardware and software system requirements for Army SAPs. Maintain a consolidated BSMS database for Army SAPs. Ensure consistency between program office databases and SRIA master database through regular periodic updates and data transfers.

2-32. Defense Security Service

The DSS will—

a. Maintain industrial security inspectors with appropriate clearances and access to perform facility clearance inspections and industrial security reviews of contractor facilities supporting Army SAPs.

b. Coordinate with TMO in the conduct of industrial security reviews.

Chapter 3 Special Access Program Design

3-1. Purpose

a. *Special Access Program.* A SAP is a security program established under the provisions of Executive Order (EO) 12958 and approved by the DEPSECDEF to apply extraordinary security measures to protect extremely sensitive information. SAP status is defined by DOD Directive 5200.1R.

b. *Prospective Special Access Program.* A PSAP is an interim security program to apply extraordinary security measures to protect extremely sensitive information pending approval of SAP status by the DEPSECDEF. Chief, TMO approves PSAP status for Army programs.

3-2. SAP types

DOD recognizes three types of SAPs: Acquisition (AQ-SAP), Intelligence (IN-SAP) and Operations and Support (OS-SAP). Within the Army, ASA(RDA) is the proponent for AQ-SAPs, DCSINT for IN-SAPs, and DCSOPS for OS-SAPs.

a. AQ-SAPs protect sensitive research, development, test, and evaluation (RDT&E), modification or procurement efforts.

b. IN-SAPs protect the planning and execution of especially sensitive intelligence or counterintelligence units or operations, including the collection, analysis, and exploitation of intelligence. IN-SAPs also protect especially sensitive programs to procure and exploit foreign materiel.

c. OS-SAPs protect the planning, execution, and support to especially sensitive military operations. This type of SAP may protect organizations, property, operational concepts, plans, or activities.

3-3. SAP categories

a. *Army SAPs.* SAP categories reflect the sensitivity of protected material and the degree of protection needed beyond collateral security management. Categories I through III delineate programs requiring varying degrees of protection with CAT I being the most sensitive and CAT III being the least sensitive. The Army SAPOC determines the category designation for each SAP. SAP categories may change as a program matures based on changing needs for protection or the sensitivity of the information being protected. The categories are—

(1) Category I (CAT I): Army SAPs that are extremely sensitive and include only the most critical technical developments and the most sensitive intelligence and operational activities. Compromise would cause exceptionally grave damage to national security. Only Army CAT I SAPs are eligible for consideration for waived SAP status.

(2) Category II (CAT II): Army SAPs that include critical acquisition, intelligence and operational activities that do not meet the criteria for CAT I. Compromise would cause serious damage to national security.

(3) Category III (CAT III): Army SAPs usually having significant non-Army participation, relatively short duration or are not suitable for a billet structure.

(4) Unless waived by the SAPOC or the DEPSECDEF, if necessary, CAT I, II and III SAPs follow security procedures listed in figure 5-1.

b. *Non-Army SAPs.*

(1) Category N (CAT-N) is the category designation for SAPs or sensitive activities where the Army is the executive agent but not the sponsor. Security measures for CAT-N SAPs are in accordance with this regulation as amended by memoranda of agreement (MOAs) between Army and the program sponsor. CAT-N programs have the same management oversight as Army SAPs unless otherwise directed by the VCSA.

(2) Army elements may also participate in SAPs that are neither sponsored nor executed (primarily) by Army. Approval for, and

management of, Army participation in SAPs executed by other organizations are governed by paragraph 4–4 of this regulation. Security measures for these SAPs are in accordance with the executing organization's security procedures.

Chapter 4 SAP Life Cycle

4–1. Establishment phase

a. As soon as an organization determines that an activity needs SAP protection, it should request approval to establish a PSAP. MACOM/PEO proponents route PSAP requests through their MACOM commander (if applicable) and ARSTAF principal to TMO using the format at appendix B. TMO reviews the request and staffs it with the ARSTAF. If the review is favorable, TMO notifies the proponent in writing of the PSAP approval. This notification includes PSAP nickname and registration date, critical program elements, PSAP security level and category, funding guidance, and date to present the PSAP to the SAPOC. The ARSTAF proponent informs appropriate activities and organizations of the requirement for increased security procedures. Once the MACOM/PEO receives PSAP approval, the program applies selected SAP security controls to the program.

b. PSAP status is valid for 6 months from the date it is approved by TMO. During that period, the MACOM/PEO proponent, the ARSTAF proponent, the SA (through the SAPOC) and the DEPSECDEF (through the OSD SAPOC) must determine whether to grant SAP status. If the DEPSECDEF does not approve SAP status within this 6-month period, authority to use SAP security controls terminates unless OSD has granted an extension in writing.

c. PSAPs will not receive obligated funds without written TMO approval. PSAPs will receive only those minimum obligated funds necessary for program security and administration until the DEPSECDEF grants SAP approval.

d. Proponents of an approved PSAP apply SAP security controls to the prospective program with one exception: they do not execute indoctrination statements until the SAP is formally approved. However, to keep track of who knows of the PSAP, the program office, the MACOM/PEO and TMO keep knowledgeability rosters so that indoctrination statements can be executed if SAP status is approved.

e. The SAP Approval Process follows.

(1) TMO authorizes the PSAP in writing and advises the VCSA.

(2) The TMO furnishes written notification of the approval of PSAP status to the ARSTAF and MACOM/PEO proponent and other appropriate Army organizations.

(3) The PSAP program office, MACOM/PEO proponent and TMO initiate knowledgeability rosters to maintain record of all personnel knowledgeable of the PSAP.

(4) The program prepares the necessary supporting documentation to request creation of a SAP and submits it to TMO within 60 days of being granted PSAP status (see paras 5–8, 6–4, and app B). The MACOM/PEO assists the PSAP program office in coordinating with the working SAPOC members as indicated below.

(5) The ASA(RDA) evaluates the proposed acquisition strategy and acquisition plan for AQ–SAPs.

(6) The ASA(RDA) conducts a technology feasibility review for AQ–SAPs. This may be done through the appropriate MACOM or directly with the PEO.

(7) The ASA(RDA), DCSOPS, and DCSINT evaluate the availability of funds, manpower, and reprogramming actions for AQ–SAPs, OS–SAPS, and IN–SAPs respectively.

(8) The DISC4 validates information management and secure communications requirements.

(9) DCSINT ensures INSCOM conducts a CI assessment of the program's security and OPSEC posture and a multidiscipline counterintelligence assessment of the threat. DCSINT coordinates the foreign technology threat assessment with the National Ground Intelligence Center.

(10) The DCSPER evaluates the personnel assets required and conducts a personnel affordability and supportability assessment.

(11) TJAG and GC provide legal and policy evaluations.

(12) If applicable, the DCSLOG evaluates the proposed SAP materiel development or acquisition plan in light of Integrated Logistics Support (ILS).

(13) The Program Analysis and Evaluation Directorate (PAED) of OCSA and ASA(FM) evaluate the proposed funding profile required and conduct an affordability assessment.

(14) TMO schedules the working SAPOC to meet within 90 days of granting a program PSAP status. The MACOM/PEO proponent briefs the PSAP to the working SAPOC and the appropriate ARSTAF elements brief the results of their detailed evaluations.

(15) TMO schedules the SAPOC to meet at a date between 10 and 30 days after the working SAPOC. The MACOM/PEO briefs the SAPOC. If the SAPOC approves the program for SAP status, TMO prepares a memorandum to SA recommending submission of the PSAP through the OSD-level SAP central office to the OSD SAPOC for SAP approval. This memorandum sets forth the enhanced security measures intended for the SAP, any upgrade of adjudicative requirements that may be intended, the SAPOC minutes, the Report of Establishment of the SAP, and the congressional notification letters. If the prospective SAP deals with Special Operations/Low Intensity Conflict (SO/LIC) activities, the SA memorandum must be coordinated with ASD (SO/LIC) before submission to the respective OSD level SAP central office.

(16) If the OSD SAPOC approves the SAP, the DEPSECDEF notifies Congress. The PSAP becomes a SAP 30 days after congressional notification unless Congress raises an objection.

4–2. Maintenance Phase

a. *Maintenance of Army-executed SAPs.* Maintenance of Army-executed SAPs includes periodic reviews by senior leaders at HQDA; audits, inspections and investigations by DOD and Army agencies; the management control program (UP AR 11–2 as modified by this regulation); and the internal review and audit control program (UP AR 11–7 as modified by this regulation).

b. *Reviews.*

(1) *Special Access Program Oversight Committee.* The DA SAPOC oversees the establishment, management, support and disestablishment of SAPs.

(a) *Composition.* The SAPOC is a general officer-level forum chaired by the VCSA. In the VCSA's absence, the senior standing member of the SAPOC serves as chairman. The standing members of the SAPOC are ASA(RDA), GC, DCSINT, DCSOPS, and TJAG. Other members are invited to attend meetings of interest to them. Frequently invited members include ASA(FM&C), DISC4, DCSLOG, DCSPER, COE, PAE, CLL, TIG, AG (Auditor General), AMC and INSCOM.

(b) *Executive secretary.* Chief, TMO is the Executive Secretary of the SAPOC.

(c) *SAPOC reviews.* The SAPOC—

1. Reviews requests for the establishment of SAPs and forwards these requests with appropriate recommendations to SA.

2. Reviews existing programs annually to determine whether to revalidate them as SAPs.

3. Reviews and recommends policy for management of SAPs.

(d) *Meetings.* The committee meets at the call of the chairman. Generally, the SAPOC meets monthly to review selected programs so that all Army programs receive an annual review. TMO prepares minutes after each meeting, submits the minutes to VCSA for approval, and furnishes copies of the minutes to all standing and invited members of the committee.

(e) *Costs.* Costs of travel, per diem and overtime related to the SAPOC are the responsibilities of individual attendees and their organizations.

(f) *Working SAPOC.* Chief, TMO, chairs the working SAPOC. Standing members include points of contact from ODCSINT, ODCSOPS, ASA (RDA), TJAG, and OGC. Other attendees include points of contact from each of the major ARSTAF elements and HQ INSCOM/902d MI Group, AMC, and the AAA. The working

SAPOC reviews each program prior to its presentation to the SAPOC (format for the SAPOC briefing is at app D). During its review, the working SAPOC identifies issues and formulates recommendations to present to the SAPOC.

(2) *The SAP PPBERS Committee.*

(a) *Purpose.* The SAP PPBERS committee provides oversight of SAP program and budget accomplishments. It convenes at the call of the chairperson when special SAP budgetary or funding issues arise.

(b) *Composition.* The USA and the VCSA jointly chair the SAP PPBERS committee. Standing members of the committee are the GC, ASA(FM&C), ASA(RDA), DCSINT, DCSOPS, Director of PAED, and TJAG. Additional members may include DISC4, DCSLOG, DCSPER, COE, CLL, AAA, and TIG, depending on the agenda. The committee's Executive Secretary is the Chief, TMO.

(c) *PPBERS review.* The PPBERS reviews—

1. Overall program performance objectives.
2. Obligation and disbursement data.
3. Budget year (BY) issues or problems.
4. Deviations from planned performance and HQDA goals.
5. Recommended corrective actions.

(d) *Administrative support.* TMO provides administrative support to the SAP PPBERS committee.

(e) *Working PPBERS committee.* Chief, TMO chairs the Working PPBERS committee. It consists of representatives from those staff agencies identified for the Executive PPBERS committee and other activities and organizations invited by Chief, TMO. The Working PPBERS committee has the same general purpose as the Executive PPBERS committee. However, the Working PPBERS committee is a recurring forum, meeting quarterly to compare actual program performance with HQDA goals. Two weeks prior to meetings of the working PPBERS committee, the SAP proponent submits data to TMO in the format given in appendix H.

(3) *Fix-It Committee.*

(a) *Purpose.* The Fix-It committee provides oversight of SAP audits and inspections. It convenes annually to brief the VCSA (or Director of the Army Staff (DAS)) on progress made during the year to resolve issues and correct deficiencies identified in audits and inspections.

(b) *Composition.* The Fix-It Committee is a general officer forum chaired by the VCSA. In the VCSA's absence, the DAS chairs the committee. Standing members are the ASA(RDA), ASA(FM&C), GC, DCSINT, DCSOPS, TJAG, AAA, TIG, Director of PAED, and USACIC. The VCSA or DAS designates other members of the Fix-It Committee based on the agenda for a specific meeting. Additional attendees may include representatives of DISC4, DCSLOG, and DCSPER and CG INSCOM, CG AMC, CG MDW, and COE. The Chief of TMO is the Executive Secretary of the Fix-It Committee.

(c) *Support.* TMO provides administrative support to the Fix-It Committee.

(d) *Working Fix-It Committee.* The Chief, TMO co-chairs the Working Fix-It with either the Chief, SAIG-IO (for findings related to inspections) or the Chief, SAAG-AFI (for findings related to audits). The Working Fix-It committee is comprised of action officers from TMO, SAIG-IO, ODCSINT, SAAG-AFI, a technical representative from the Field Investigation Unit (FIU) of USACIDC, and the command or staff element responding to the findings. It meets quarterly to review actions taken to resolve findings from audits and inspections. Respondents brief their open findings and the committee decides whether actions taken by the respondents are adequate to close the finding. One week prior to a meeting of the working Fix-It committee, respondents provide TMO with Fix-It Status Sheets (see app J). If a respondent is recommending that a finding be closed, he or she must coordinate that recommendation with the issuing audit or inspection organization prior to the meeting of the working committee. Additionally, if the respondent is recommending closure of an audit finding, the respondent must provide the results of the follow-up IRAC review(UP AR 11-7).

(c) *Audits.* Audits are detailed examinations of any sensitive activity following generally accepted auditing standards issued by the

General Accounting Office (GAO). Audits include financial audits, economy and efficiency audits, program audits, and SA Special Area of Interest.

(1) *Internal audits.* Internal audits include those performed by the U.S. Army Audit Agency (AAA) as well as those done by IRACs. All Army SAPs are subject to internal audit. TMO integrates the AAA audit plan with the SAIG-IO inspection schedule, the SAPOC schedule, and external audit and inspection requirements to minimize duplication of effort. In developing their audit plans, IRAC organizations with SAP responsibilities should contact TMO to gain an appreciation of recent and planned audits and inspections of their program.

(2) *External audits.* Organizations outside the Army conduct external audits. These include GAO, the Department of Defense Inspector General (IG, DOD), and the Defense Contract Audit Agency (DCAA). TMO functions as the entry point for all SAP-related external audits entering Army channels except standard DCAA contract support audits. TMO notifies the cognizant MACOM SAP central office or IRAC after being notified of an external audit. TMO also ensures the Army provides written response to draft external audit reports in a timely manner.

(3) *Coordination.* SAP proponents and program offices coordinate directly with Defense Contract Management Command (DCMC) and DCAA for contract audits as well as accounting and financial advisory services regarding contracts for Army SAPs.

(4) *Findings.* Findings from AAA audits of SAPs and all non-Army (for example, DOD IG, GAO, and so forth) audits of SAPs are addressed in the Fix-It process.

d. *Inspections.*

(1) The SAIG conducts inspections of SAPs and sensitive activities under the authority of AR 20-1. These inspections include an assessment of command and control, financial management, security, contract management, intelligence oversight and SA special areas of interest.

(2) The IG, DOD, conducts audits and inspections of SAPS or sensitive activities on the basis of special concerns or unusual events. Programs should coordinate with TMO before contacting the IG, DOD concerning inspections.

(3) The ASA(RDA), U.S. Army Contracting Agency, conducts Procurement Management Reviews (PMRs) of Secure Environment Contracting (SEC) in support of SAPs.

(4) USAFMSA conducts annual manpower management reviews when necessary. No later than 120 days prior to their annual SAPOC, SAP PMs coordinate a manpower and workload validation with the USAFMSA SAP representative to accommodate an on-site visit if USAFMSA deems it necessary. The PM reports findings of the USAFMSA annual validation at the SAPOC.

(5) The Special Review Office (SRO), U.S. Army Finance Command, ASA(FM&C), conducts quality assurance reviews of financial activity under the authority of AR 11-37. SRO refers any serious deficiency or repeat deficiency to the Fix-It Committee for resolution. SRO reviews the Finance and Accounting Offices that have sensitive support missions annually and semiannually reviews those that have special mission funds.

(6) DSS conducts industrial security reviews of contractors having SAP-related contracts. These DSS inspections cover security vulnerabilities, compliance with security plans and contracts, security violations, and security compromises.

(7) Army organizations responsible for SAPs include SAPs in their organizational inspection programs as commanders deem necessary.

e. *Investigations.*

(1) Each program manager and commander or director of a SAP or sensitive activity must develop and publicize procedures for reporting fraud, waste, and abuse without compromising sensitive information. This can be a hotline notification procedure, or it may be addressed during the program indoctrination briefing.

(2) When audits or inspections uncover criminal wrongdoing or suspected wrongdoing, the lead inspector or auditors must notify TMO and the FIU, USACIDC, immediately.

(3) The IG, DOD and GAO also have investigative branches.

Before an IG, DOD or GAO investigation, the TMO must be notified. TMO will facilitate the granting of the necessary SAP accesses for these investigations.

(4) Security related incidents involving SAPs will be investigated and reported in accordance with AR 380-5 and SAP security guidelines. Items of counterintelligence interest will be investigated by INSCOM in accordance with AR 381-12 and SAP security procedures.

(5) Program Managers, Commanders, or Directors of Army SAPs will immediately report all instances of suspected criminal activity in or against a SAP through appropriately cleared channels to the FIU, USACIDC.

f. Management Control Program.

(1) SAPs are subject to the requirements of AR 11-2 (Management Control) as modified herein. Commanders, PEOs or PMs of assessable units will use the Management Control Evaluation checklist at appendix C in assessing Army SAPs under their control. If assessable units identify material weaknesses in their SAPs, they report these to the TMO where they are addressed through the Fix-It process. The assessable unit also sends an unclassified version of the material weakness through command channels.

(2) If Army participation in a non-Army SAP requires a deviation from the participating Army unit's Management Control Plan, the SAP sponsor will address the deviation in an MOA between the unit and the SAP sponsor.

g. Internal Review and Audit Compliance Program.

(1) The IRAC program (UP AR 11-7) applies to SAPs with the modification that MACOMs that have established SAP central offices are authorized to designate these offices as the focal point for SAP audits. In this capacity, SAP central offices—

(a) Serve as the POC for SAP audits by agencies external to the MACOM.

(b) Secure support from MACOM IRAC offices to assist during audits by agencies external to the MACOM. This assistance may include liaison with external auditors, negotiating audit results and audit follow on.

(c) Ensure that SAPs are included in the audible entity files of the responsible IRAC office.

(2) MACOMs/PEOs or ARSTAF POCs responsible for a SAP will—

(a) Ensure that the SAP has adequate IRAC support, including accessed auditors at supporting IRAC offices, to meet command and program audit needs. The MACOM/PEO/ARSTAF can arrange this support from internal assets or from other DOD organizations capable of providing audit support at SAP locations.

(b) Coordinate IRAC coverage when multiple commands or installations have overlapping responsibility for a single SAP or sensitive activity.

h. Restructure.

(1) SAPs may require restructuring for several reasons:

(a) To create a new subcompartment.

(b) To disestablish an existing subcompartment.

(c) To alter an existing charter or create a new one.

(d) To change security requirements.

(2) A SAP PM desiring to restructure submits a memorandum through the chain of command to TMO. The memorandum includes the specifics of the restructure, the reason for the restructure, a statement of any impact on security, manpower, or funding and a point of contact for the restructure.

(3) TMO reviews and staffs the request. If TMO determines that the proposed restructure does not change the scope or mission of the SAP, the Chief, TMO, can approve the restructure. If the Chief, TMO determines that the restructure changes the scope or mission of the SAP, TMO will staff the proposed restructure through the Army leadership. If the Army leadership concurs with the proposed restructure, Chief, TMO will submit the proposed restructure to the OSD-level SAP central office for their recommendation for approval by the DEPSECDEF.

i. Training. Program Security Managers (PSMs) follow the guidance in AR 380-5, chapter 10, regarding security education requirements for personnel accessed to SAPs. Additionally, PSMs will use the guidance in AR 530-1, appendix F, regarding OPSEC training requirements.

4-3. Disestablishment

a. Procedures. The ARSTAF/MACOM/PEO proponent recommends a SAP for disestablishment when the SAP no longer requires extraordinary security controls. The SAPOC may also identify a SAP for disestablishment at the annual revalidation. Disestablishment does not equate to program cancellation. It means removal of SAP security controls from the program.

b. Rationale. Rationale for the disestablishment of a SAP include, but are not limited to—

(1) The RDT&E, procurement, training, or other requirements during a program's life cycle significantly increase the number of personnel requiring knowledgeable.

(2) The tactical or strategic impact or value of the system, operation, or activity lessens significantly.

(3) Technological advances required to develop, produce and field a system have not, or will not, reach the required levels.

(4) The resources required for continued enhanced security procedures are excessive compared to the benefits achieved by continuing to maintain SAP status.

(5) Other Services or foreign nations are developing similar technology or applications without equivalent levels of protection.

(6) A security compromise negates the protection achieved by continued enhanced security.

(7) The program has met the tactical or strategic mission of the system, operation, or activity and there is no further mission requirement.

(8) The Army has fielded the system and operational use at the tactical or strategic levels precludes continued use of extraordinary security measures.

(9) The Army established the SAP to protect an identified vulnerability but countermeasures have been developed eliminating the vulnerability.

c. Procedures.

(1) Throughout the planning for SAP disestablishment, the program limits knowledge of this considered course of action until the DEPSECDEF approves the disestablishment and notifies Congress.

(2) Prior to recommending SAP disestablishment, the MACOM/PEO conducts a risk assessment of the potential for compromise of program information and the effects of such a compromise if SAP controls are removed.

(3) The MACOM/PEO develops a disestablishment concept (app F), staffs it for ARSTAF review and concurrence, and submits it to TMO.

(4) After favorable review by the ARSTAF, TMO schedules the SAP disestablishment as a SAPOC topic. The SAPOC forwards its recommendation to the SA.

(5) If the SA recommends disestablishment, TMO will forward the SA recommendation to OSD with congressional notification letters. If Congress does not object within 14 days, TMO notifies appropriate ARSTAF, MACOM, and PEOs that disestablishment has been approved and the program commences disestablishment actions.

(6) Disestablished SAPs return to the normal oversight system within 6 months of approval to disestablish. After disestablishment, the responsible MACOM/PEO certifies to TMO that the actions specified in appendix G have been accomplished. TMO refers to the Fix-It committee for follow-up all SAPs not completing disestablishment actions and gaining certification (UP app G) as disestablished by the end of the 6-month period.

d. Non-Army SAP. Termination of Army participation in a non-Army SAP. There are occasions when the Army withdraws from SAPs but the programs continue to be managed as SAPs by other agencies. In these cases Army follows the procedures set forth by the SAP sponsor for termination. While the program is still an

approved SAP, the Army protects the special access information in accordance with the existing program security plan.

4-4. Joint SAP Management

a. Category-N SAPs.

(1) CAT-N SAPs are those executed by the Army but sponsored by others. They are managed and overseen in the same manner as Army-sponsored SAPs unless otherwise approved by the SAPOC.

(2) Before accepting execution responsibility for a CAT-N SAP, the responsible MACOM or PEO develops an MOA with the sponsoring agency. The MOA defines program relationships, responsibilities, security procedures and financial arrangements. Additionally, the MOA specifies any deviations from security and oversight requirements established in this regulation. Any security deviations from DOD 5200.1-R, 5200.2-R, 5220.22-R, and 5220.22-M, or for SAPs in which SCI material is handled, deviations from DOD S-5105.21-M-1, DOD TS-5105.21-M-2, and DOD TS-5105.21-M-3, may not be implemented without approval of the DEPSECDEF. The proposed MOA is included in the SAP justification package that is staffed during the SAP establishment process and presented to the SAPOC. The MOA conforms to the format and guidance set forth in AR 25-50 and includes the effective date and a requirement for biennial review. Army MOA signature authority is based on the level of agreement.

(3) CAT-N MOAs are reviewed every other year as a minimum. Substantive changes are staffed through TMO for SAPOC approval. If the SAP sponsor has an immediate need that requires deviation from an approved MOA, the Chief, TMO, in coordination with OTJAG and OGC, can grant interim approval. Prior to approval, a formal review of the proposed deviations must ensure they do not violate the security requirements set forth by DOD 5200.1-R, 5200.2-R, 5220.22-R, and 5220.22-M. If the proposal involves deviation from these requirements or if the SAP handles SCI material, and the proposal deviates from DOD S-5105.21-M-1, DOD TS-5105.21-M-2, and DOD TS-5105.21-M-3, DEPSECDEF approval is required before the deviation is implemented.

b. Army participation in SAPs sponsored and executed by others.

(1) Army organizations may participate in SAPs sponsored and executed by non-Army organizations without establishing a separate Army-executed CAT-N SAP. However, the Army organization and the SAP sponsor must establish, and keep current, an MOA to govern program security and minimum Army access in cases that involve—

(a) Substantial or recurring use of Army personnel or resources (over one-half man year or \$10,000 in any 12-month period), or

(b) Risk of physical harm to Army personnel, damage to Army resources, or potential embarrassment to the Army, or

(c) Questions of propriety or policy.

(2) No DA organization, command, activity, or individual will negotiate such an agreement with any non-Army activity without prior coordination with TMO. After the MOA has been drafted, it will be forwarded to TMO for review and appropriate approval (VCSA, USA, or SECARMY) before it is signed by the Army entity entering the MOA. These programs will be managed based on their individual requirements and may have more restricted access than the Army baseline billet structure.

c. *MOA content.* MOAs between SAP proponents and Army elements include consideration of each element in the SAP matrix (table 5-1), to include a billet structure. At a minimum, access is required for the following personnel:

- (1) Secretary of the Army
- (2) Under Secretary of the Army
- (3) General Counsel
- (4) Chief of Staff, Army
- (5) Vice Chief of Staff, Army
- (6) Appropriate principals of HQDA Staff (for example, DCSOPS, DCSINT, ASA (RDA))
- (7) The Inspector General
- (8) Chief, Intelligence Oversight Division

(9) The Judge Advocate General

(10) Technology Management Office: Chief, Deputy, Legal Advisor, Finance Officer, Security Officer, Appropriate Action Officers.

d. *Non-Army SAPs.* Any involvement in non-Army SAPs which does not afford at least the minimum access defined in paragraph 4-4c above is prohibited, unless the SA approves a specific exception in writing. Requests for waivers are forwarded, with the proposed MOA, through the appropriate MACOM/PEO activity to Chief, TMO, for approval by SA.

e. *Non-DOD SAPs.* Army support to non-DOD SAPs and other sensitive activities, no matter how limited, is governed by DOD Directive 5210.36. Army units and offices will not provide support to non-DOD SAPs without prior approval in accordance with Army's implementing instructions to DOD Directive 5210.36. If an Army unit or office is approached by a non-DOD agency to provide support to a restricted or limited access program, the unit or office should contact TMO as soon as possible.

f. *Non-Army agencies.* Army sensitive support to non-Army agencies, regardless of whether the support is to a SAP or not, is also governed by DOD Directive 5210.36. If an Army unit or office is asked to provide sensitive support to a non-Army agency, the unit or office should contact TMO immediately.

g. *SAP registry.* The TMO maintains a registry of SAPs (both Army and non-Army) involving Army participation. Annually, TMO validates this register via an Army-wide SAP data call. In response to this data call, all Army units and offices report any participation in or support to SAPs and other restricted access activities (no matter how limited) sponsored or executed by non-Army agencies.

Chapter 5 SAP Security

5-1. Programs ineligible for SAP security

a. The extraordinary security measures approved for use with SAPs may not be used by non-SAP programs. No collateral program, including programs with approved Limited Dissemination controls, may use program access non-disclosure agreements (read-on statements), classified code words for program identification, "Carve-out" contracting, Special Access Required markings or cover sheets, a program billet structure, or personnel security investigative or adjudicative requirements more stringent than those required for a comparable level of classified information. These measures are reserved for SAPs.

b. SAPs derive enhanced security primarily from the restricted access features of these programs. Generally, with respect to other security features (for example, physical security, technical security, and so forth), SAPs are held to the same standards as collateral programs at the same classification level.

5-2. Physical security

a. *Security level.* As a general rule, SAPs base the level of physical security on the classification level of the information processed or stored by the SAP.

(1) Category I SAPs and SAPs processing or storing Sensitive Compartmented Information (SCI) adhere to standards established by DCID 1/21 and the applicable requirements of DOD S-5105.21-M-1, DOD TS-5105.21-M-2, and DOD TS-5105.21-M-3.

(2) Category II and III SAPs that do not process or store SCI will follow AR 380-5.

b. Risk assessment.

(1) Program managers of CAT II and III SAPs conduct risk assessments during the PSAP process to determine whether they must implement physical security measures above the standards prescribed in AR 380-5.

(2) Program offices coordinate this risk assessment with supporting INSCOM CI elements and include the results in their SAP security plan.

(3) The risk assessment incorporates—

(a) *Intelligence Threat Report*. This is a multidisciplined counterintelligence report that addresses the general and specific collection threat to the program.

(b) *Counterintelligence Assessment*. This is an in-depth analysis of the counterintelligence factors affecting the program's overall security and CI/OPSEC posture. INSCOM normally supports SAPs by developing Intelligence Threat Reports and the Counterintelligence Assessments for the programs at their request.

(c) *Program Security Assessment*. Program Managers integrate information from the Intelligence Threat Report and the Counterintelligence Assessment to determine whether the program requires further technical protection. If so, the PM requests a TSCM Survey (see para 5-5).

c. *Two Person Integrity (TPI)*. TPI is required for Category I SAPs only.

d. *Entry/Exit Searches*. MACOM/PEOs and program offices establish entry/exit programs in accordance with AR 380-5, DOD 5220.22-M (the National Industrial Security Program Operating Manual (NISPOM)), and the NISPOM Supplement.

5-3. Document/information security

a. *Marking*. Authors of classified information mark documents in accordance with AR 380-5. Additionally, authors of SAP material will—

(1) Mark SAP nicknames at the top and bottom of the outside front cover, title page, all interior pages and on the outside back cover of all documents (for example, SECRET/BROKEN BRIDGE/SPECIAL ACCESS REQUIRED).

(2) Mark the subcompartment nickname in accordance with paragraph (1) above (for example, SECRET/BROKEN BRIDGE/STURDY TWIG/SPECIAL ACCESS REQUIRED). The SAP nickname and the wording "INCLUSIVE" may be used when a report contains information on all subcompartments (for example, SECRET/BROKEN BRIDGE/INCLUSIVE/SPECIAL ACCESS REQUIRED).

(3) Use the caveat "SPECIAL ACCESS REQUIRED" on the top and bottom of all pages that contain SAP information (for example, SECRET/BROKEN BRIDGE/SPECIAL ACCESS REQUIRED).

(4) Mark the beginning of each paragraph with the initial of the classification and the initials of the unclassified nickname of the SAP and subcompartment if applicable (for example, S/BB). Programs must include the parent SAP initials before the subcompartment for portions containing subcompartment information (for example, S/BB/ST). Partial paragraphs which begin a page will be marked with appropriate paragraph markings.

b. *Unauthorized caveats*. Programs will not use the unauthorized caveats PROGRAM CONTROLLED or CONTROLLED NEED-TO-KNOW. This does not preclude use of distribution statements such as Handle via Special Access Program (Nickname) Channels.

c. *Transmission*. SAP material will be transmitted in the same manner as material with collateral classification of the same level unless the program's approved security procedures guide dictates more stringent procedures. Individuals transmitting SAP material may use—

(1) Approved secure point-to-point communications systems (for example, STU-III, secure FAX) appropriate for the security classification of the material; however, the transmitting individual must ensure that access is limited to indoctrinated SAP personnel on the receiving end of the transmission. Programs request guidance regarding approved mechanisms for secure point-to-point communications from HQDA, ODISC4 (SAIS-PPP). Additionally, programs use TEMPEST countermeasures and terminal equipment as determined by INSCOM based on analysis performed in accordance with AR 380-19-1.

(2) Defense Courier Service (DCS).

(3) Indoctrinated SAP personnel as couriers (must have courier orders).

(4) Registered mail using procedures outlined in AR 380-5 for documents up to and including SECRET SAR. Top Secret material cannot be transmitted via registered mail. Programs may use dedicated post office boxes to ensure SAP security for postal mailing. The provisions of AR 381-102 apply.

(5) U.S. Postal Service Express Mail in accordance with AR 380-5 for documents up to and including SECRET SAR if within the 50 states, District of Columbia and the Commonwealth of Puerto Rico. Using Express Mail to APO/FPO addresses is prohibited. Similarly, TS material cannot be transmitted via Express Mail.

(6) Restricted use of message dissemination systems for CAT III SAPs if authorized by the VCSA.

d. *Dissemination*. Programs must not release any classified SAP information to the public or to any individual not approved for access without written approval from the SA. Additionally,

(1) DOD grants SAP access to select members of Congress and their staffs. When indoctrinating these individuals, Access Approval Authorities (AAA) use the procedures outlined in chapter 6 of this regulation with the exception that DOD Directives do not require members of Congress to execute indoctrination statements. Offices that routinely provide Congressional briefings or SAP documents to Congress (for example, ASARDA) maintain rosters of Congressional members and their staffs granted access to SAP material and ensure that SAP security managers receive the information needed to keep their access rosters current.

(2) SAP managers and their supporting contracting officers prohibit contractor release of SAP information by using contract security classification specifications issued for each SAP-related contract. Item 12 of the DD Form 254 (Contract Security Classification Specification) must state "Public release of information concerning any aspect of this contract is prohibited."

(3) Programs coordinate with MACOM/PEO and TMO for advice and assistance on all Freedom of Information Act (FOIA) requests for SAP information.

(4) Programs and contractors will not release information pertaining to an Army SAP to the Defense Technical Information Center or any other information service. Programs must include this restriction in the DD Form 254.

(5) Patent applications containing SAP information are submitted through ASARDA to the TMO for VCSA approval prior to submission to the U.S. Patent and Trademark Office. The contractor must notify the Contracting Officer 30 days in advance before filing a patent classified at the Secret or higher level. The Government cannot stop a contractor from filing a patent. However, the Government can recommend the imposition of a secrecy order to the Patent Commissioner. To seal a case, the Patent Office requires the Signature of an Assistant Secretary or higher. If a release in judicial proceedings is anticipated, Chief, TMO will notify the Director, Special Access Program Coordination Office, OSD, of the proposed release of SAP information in connection with the judicial proceedings.

e. *Storage*. Offices that store SAP material must do so in accordance with AR 380-5, the NISPOM and SAP supplement. Additionally, these offices must segregate SAP material from collateral material in a manner that ensures only program cleared individuals have access to the material.

f. *Destruction*. Responsible offices destroy SAP material in accordance with AR 380-5 and AR 25-400-2.

g. *Archiving*. SRIA has the Army charter to archive and maintain a central repository for information related to SAPs and sensitive activities. Program offices maintain files and records per AR 25-400-2 and send SAP related documents to SRIA for archiving.

h. *Accountability*.

(1) Special access status does not add additional accountability inventory requirements to those specified in AR 380-5.

(2) Contractors account for documents in accordance with the NISPOM and the SAP supplement.

(3) Program SPGs set forth the accountability procedures for each program.

i. Receipting. Use classified information receipt for all TOP SECRET documents per AR 380-5. Documents classified SECRET/SAR and below do not require a receipt unless mailed or couriered outside of the command, in which case transmitters and recipients follow the provisions of AR 380-5 and the NISPOM.

j. Reproduction. Special access status does not add additional restrictions on reproduction to those specified in AR 380-5 and the NISPOM.

5-4. Personnel security

a. Clearances. The Army grants access to SAP information based upon an individual's level of clearance for information and need to know. The Army does not conduct separate, duplicate adjudications for access to SAP information.

b. Investigative requirements.

(1) Personnel requiring access to Category I SAP information and incumbents of Army baseline billets must have TOP SECRET clearances based on a favorable single scope background investigation (SSBI), or the equivalent, conducted by an authorized agency and favorably adjudicated in accordance with AR 380-67 and the NISPOM.

(2) Personnel requiring access to Category II or Category III SAP information must have a TOP SECRET clearance based on a favorable SSBI or a SECRET clearance based on a National Agency Check (NAC) and/or a NAC with written inquiries (NACI). The NACI is acceptable if the highest level of access required is SECRET.

(3) For initial and continued access to SAP information, the investigation cited in paragraphs (1) and (2) above must be within the last 5 years. However, AAAs may grant access to an individual with an out of date investigation if the individual has submitted a periodic re-investigation through security channels and there is no indication of new derogatory information since the previous investigation.

(4) A break in military service or civilian employment of 24 months or more during the most recent 5 year period requires a new SSBI or NAC/NACI.

c. Extraordinary requirements. Requests for extraordinary investigative requirements (that is, investigations beyond those specified in paragraph *b* above) require prior approval from the Office of the Secretary of Defense. These requests are submitted through TMO to ODCSINT for staffing.

d. Reciprocity. For purposes of SAP access, Army accepts clearance determinations made by the appropriate clearance or adjudicative authority of other DOD components and agencies of the Federal Government. The office requesting access to Army SAPs agrees to abide by all other rules for access set forth in this regulation.

e. Derogatory information. Individuals with derogatory information, information that constitutes a possible basis for taking an adverse or unfavorable personnel security action, on personnel with access to Army SAPs will report this information in accordance with AR 380-67. The PM must report valid derogatory information to the 902nd MI Group/INSCOM or FIU as appropriate for an independent impartial investigation. The PM may also suspend access to the program in accordance with AR 380-67 during the conduct of the investigation until completion of final clearance adjudication.

f. Citizenship. All persons accessed to Category I and II Army SAPs must be U.S. citizens.

g. Polygraph.

(1) Personnel approved for access to Army and non-Army SAPs may be subject to random polygraphs examinations upon approval by the SA. Any adverse action, including removal of SAP access, based solely on polygraph results is prohibited.

(2) Army does not inform program managers regarding cases referred for investigation. If the investigation reveals adverse information, the Army will adjudicate the matter and notify the program manager according to existing policy.

5-5. Technical security

a. Signal security. Army SAP proponents request counter-signals intelligence support from INSCOM to assist in identifying information transmission needs and recommending appropriate signal security requirements. Programs will—

(1) When possible, use systems listed in NSA's Information Systems Security Products and Services Catalog. Refer to AR 380-19-1 for specific requirements.

(2) Limit non-secure commercial telephones to the minimum number essential for efficient operations.

(3) Utilize secure communications as much as possible.

(4) Programs using facilities to store, process or discuss SCI follow the standards specified in DCID 1/21.

b. TEMPEST. AR 380-19-1 implements national TEMPEST policies and procedures. TEMPEST Countermeasures (CM) will be applied in proportion to the threat based on a TEMPEST CM Review by a Certified TEMPEST Technical Authority (CTTA). This CM review must be performed and validated by a CTTA prior to the programming or expenditure of funds for TEMPEST. For SAPs, requests will be forwarded to TMO for coordination with ODCSINT, DAMI-CHS. To preclude unnecessary expenditures, program offices should consult with INSCOM Technical Security representatives at the earliest possible stage in the planning process regarding the application of TEMPEST CM.

c. Technical Surveillance Countermeasures. AR 381-14 (S) prescribes the physical and technical security standards for implementation in certain facilities where SAP information is electronically processed or routinely discussed aloud.

(1) Category I program management offices that discuss or process information electronically require a TSCM survey. All other SAPs request TSCM services only when the facility risk assessment indicates the threat or vulnerability of the facility requires a technical security evaluation. PMs will include the risk assessment results in the SAP establishment package.

(2) Annually, INSCOM reviews the program facility risk assessments and the TSCM schedules for each program. INSCOM provides its results and recommendations to the program manager and HQDA ODCSINT as part of the working SAPOC brief.

(3) INSCOM will only conduct TSCM surveys on finished facilities which have physical controls and access procedures already in place. TSCM survey team members may require short-term SAP access. They must submit the appropriate access paperwork and meet the personnel security requirements set forth in paragraph 5-4 above in order to have access. Upon completion of TSCM surveys, the program manager maintains the physical security integrity of the facility and limits access to authorized and properly cleared personnel (see AR 381-14).

(4) To preclude unnecessary expenditures, program offices consult with INSCOM TSCM representatives at the earliest possible stage in the planning process regarding the physical and technical security measures required for planned construction of new SAP facilities or renovations to existing facilities. TSCM personnel will conduct a preconstruction advice and assistance service to identify required measures.

5-6. Treaties

a. Treaty authority. Army SAP facilities are subject to inspection and monitoring under select arms control treaties (for example, Open Skies and the Chemical Weapons Treaties).

b. Treaty proponent. HQDA, DCSOPS is the Army staff proponent for implementation and compliance for arms control treaties. The Assistant Secretary of the Army (Installations, Logistics and Environment) serves as the Army's arms control implementation and compliance review manager.

c. Open Skies Treaty. The Open Skies treaty is a multilateral agreement designed to promote openness and transparency with respect to military activities. The treaty permits signatories to fly unrestricted, unarmed observation missions over the territory of other signatories using aircraft equipped with a variety of optical sensors and synthetic aperture radar.

(1) The entire airspace of every treaty member is open to observation flights. Consequently, every U.S. Army facility on the territory of the United States and on the territory of all other signatory nations (Germany, Italy, Korea, and others) are subject to observation flights.

(2) The treaty requires a minimum notification time of 72 hours from the time an observing party notifies the observed party of intent to conduct an overflight until the observing party touches down onto the observed party's point of entry airfield. As a consequence, PMs and PSMs must take appropriate actions prior to an inspection to safeguard their program facilities and field testing facilities.

d. Chemical weapons treaties. The United States is currently a party to three CW agreements: two bilateral agreements with Russia (Bilateral Destruction Agreement and the Wyoming MOU) and one multilateral agreement (Chemical Weapons Convention (CWC)). The CWC prohibits the development, production, stockpiling, and use of designated types and quantities of chemical weapons. One of several verification provisions of the CWC is the use of "challenge inspections" at any Government, private or commercial activity facility to demonstrate compliance with the CWC. A team of multinational inspectors employed from the CWC's implementing body, the Organization for the Prohibition of Chemical Weapons, conducts the inspections. Challenge inspections have virtually the same protocols and requirements under all three CW agreements. The only major difference in the process is the composition of the foreign inspection team.

(1) The mere suspicion that a facility is producing or stockpiling CW agents or precursor chemicals is sufficient justification for a challenge inspection. Therefore, all facilities are potential sites for challenge inspections.

(2) During a challenge inspection, the inspection team has the right to monitor all traffic exiting the facility; take soil and air samples; request to have photos taken; review records, and interview employees. The inspection team can also request an overflight of the area/facility.

(3) SAP facilities will generally have less than 48 hours from time of notice until the time inspectors arrive at their facilities.

e. Treaty security measures. Because of the short notification times, to maintain security while complying with treaties, SAPs must maintain the ability to react quickly in the event of any challenge inspection. Additionally, Army installations and contractors that support SAPs must maintain the capacity to quickly alert SAPs resident in their facilities.

(1) SAP PMs, assisted by supporting counterintelligence personnel, must evaluate the potential threat posed by treaty inspections and overflights and develop contingency plans as part of their security and OPSEC plans.

(2) PMs must educate program personnel on the potential security threat treaties pose.

(3) Army employs an installation-based approach to treaty inspection notification. DA DCSOPS alerts MACOMs and installations that they are subject to an inspection during a specified time window. The installation notifies subordinate and tenant activities. PMs ensure that their offices, contractors (if applicable) and field sites are connected with installation notification schemes. He or she validates this periodically through direct coordination with MACOM/installation treaty POCs.

(4) TMO, the 902nd MI Group, INSCOM, and the MACOMs monitor the adequacy of SAP notifications by reviewing SAP notification plans, as necessary, during staff visits and inspections. Additionally, SAP managers brief their notification plans, as required, at working SAPOCs.

5-7. Technology Transfer/Foreign Disclosure

a. The HQDA DCSINT exercises approval authority for disclosure of official Army information, both classified and controlled unclassified, to foreign governments and international organizations. This authority may be delegated in writing to DA subordinate elements (MACOMs and below).

b. Normally, Army SAP information is not releasable to non-U.S. citizens, foreign governments, or international organizations. In rare instances, Army, in coordination with OSD, approves discrete elements of SAP information for release to foreign governments usually as part of a joint or collaborative program. Release to foreign governments and international organizations will comply with the National Disclosure Policy (NDP-1), DODD 5230.11, and DODD C-5230.33 for military intelligence SAP information. Release is not authorized without an approved international agreement (MOU, Data Exchange Agreement (DEA), an Information Exchange Agreement (IEA) in accordance with DOD Directive 5530.3, a DA DCSINT approved Delegation of Disclosure Authority Letter (DDL)), and in cases of waived SAP information, DEPSECDEF approval.

c. Program managers anticipating the need for eventual release of information/technology to foreign governments and international organizations must identify this requirement as early as possible in the SAP's "life cycle," preferably before SAP establishment, and seek approval for release of program information early on. PMs must ensure the program SCG and SPG clearly identify the release authority.

d. Program managers, MACOMs, and SAP proponents that identify the need for foreign release of SAP and SAP-related information/technology must submit the required documentation to DAMI-CHS for review and approval. DAMI-CHS will coordinate with SARD-SO and TMO.

e. The program manager will not initiate or engage in preliminary discussions with a foreign government or international organization regarding the establishment of an international agreement or potential release or exchange of classified military information, controlled unclassified information (CMI/CUI), SAP or SAP-related information without the written approval of HQDA (DAMI-CHS).

f. Any person who has any indication that a foreign government has compromised SAP information, shall report the compromise immediately to the Chief, TMO, who shall report to the DCSINT, OGC, TJAG, VCSA, CSA, USA, and SA as well as the National Disclosure Policy Committee. The DCSINT shall conduct a damage assessment and provide copies of the completed case report and damage assessment to the Chair of the National Disclosure Policy Committee.

5-8. Program security plan

a. Draft plan. The program develops and submits a draft security plan to TMO within 60 days of PSAP approval. The MACOM/PEO and ARSTAF review the security plan during the SAP approval process.

b. Plan contents. At a minimum, each SAP security plan consists of a security classification guide, security procedures guide, OPSEC Annex, threat assessment, indoctrination briefing and a billet roster (if applicable).

c. Security Classification Guide. The Security Classification Guide (SCG) describes the critical elements within the SAP and explains in detail how to classify program information. Additionally—

(1) The PSM assists the program manager and program technical personnel in preparing the SCG.

(2) The original TOP SECRET classification authority (OCA) signs the SCG.

(3) TMO, ICW DCSINT, and the SAP ARSTAF proponent, approves the SCG prior to OCA signature and SAP approval.

(4) The PSM ensures everyone handling program information has access to a SCG.

(5) The DD Form 254 for contractors references applicable SCGs.

(6) Significant changes to an approved SCG or an SCG developed for a newly proposed subcompartment must be reviewed at HQDA. Revised or proposed SCGs should be submitted by the PM through the ARSTAF proponent to TMO for approval 60 days prior to implementation unless otherwise directed by the Chief, TMO. TMO will coordinate ARSTAF review and return the SCG with comments within 45 days of receipt.

d. *Security Procedures Guide.* The PM develops a SAP Security Procedures Guide (SPG) to provide indoctrinated personnel specific security procedures for protecting program information. In addition to identifying the ACA and AAAs, the SPG addresses the following security disciplines: information system security, communication security, emission security, operational security, personnel security, information security, physical security, signal security, and TSCM. The SPG also addresses treaty verification inspections and foreign travel/contact. As with the SCG, the following occurs:

- (1) The PSM prepares the SPG
- (2) TMO approves the SPG prior to PM signature and SAP approval.
- (3) PSM ensures everyone handling program information has access to a SPG.
- (4) The DD Form 254 for contractors references applicable SPGs.

e. *OPSEC Assessment.* OPSEC is the responsibility of the SAP program manager. The program manager prepares an OPSEC Annex to the security plan (in accordance with AR 530-1) with the assistance of 902nd MI Group, INSCOM. The program provides copies to TMO and the DCSINT.

(1) SAP program offices and MACOM/PEO proponents provide all activities, agencies, or organizations supporting their program copies or appropriate extracts of the OPSEC Annex.

(2) The program office reviews and updates the OPSEC annex annually. As a minimum, the OPSEC annex addresses the essential elements of friendly information, threat, travel/mail procedures, testing, media and public release, and program signatures reduction.

f. *SAP Security Manager.* The PSM is a fully qualified individual who reports to the PM for security issues. The security manager for CAT I and II programs will be a full-time position. The SAP PSM will not have additional duties related to collateral programs, but may act as the PSM for more than one SAP under the same PM. For CAT III the PSM may be a part-time position (see table 5-1). PSMs—

- (1) Advise PMs on classification, declassification, downgrading and upgrading of SAP information.
- (2) Prepare and submit program security plans to their PMs.
- (3) Maintain billet/access rosters.
- (4) Ensure through MACOM security officers that personnel with access to the program have the appropriate level of personnel security clearance.
- (5) Serve as the program focal point for all security, CI and OPSEC related issues.
- (6) Review SAP contract requirements and assist in the preparation of the security classification specifications (DD Form 254).
- (7) Review suspected and confirmed program compromises and advise their PMs on required actions.

5-9. Security incidents involving SAP information

a. *Notification.* Individuals who become aware of a security infraction or violation involving SAP information will contact the program office immediately. Upon learning of the infraction, the PM and PSM will take immediate steps aimed to minimize further damage and regain custody of the information or material. Within 24 hours of notification of the infraction, the PM will notify HQDA (DAMI-CHS) through normal SAP reporting channels. DAMI-CHS

will notify TMO and INSCOM if appropriate. DAMI-CHS and TMO will provide additional guidance as appropriate.

b. *Preliminary investigation.* If warranted, DAMI-CHS will direct a preliminary investigation in accordance with the procedures set forth in AR 380-5. Upon completion of the preliminary investigation, the SAP PM—

- (1) Forwards a report to HQDA (DAMI-CHS) within 7 days of the incident.
- (2) Determines the appropriate remedial, administrative, disciplinary, or legal action to pursue, to include completion of DA Form 5750-R (Inadvertent Disclosure Oath) (Requirements Control Symbol (RCS) exempt, AR 335-15, para 5-2b(4)). If appropriate, execute DA Form 5750-R. A copy of this form is at the back of this regulation for local reproduction on 8 1/2- by 11-inch paper. The completed form will be retained with program read-on documentation.
- (3) If applicable, forwards a report of derogatory information through chain of command in accordance with AR 380-5 to the appropriate adjudicating authority.
- (4) Considers the removal of indoctrinated persons from access to the SAP when actions by such individuals contributed to the compromise, violation, or infraction.
- (5) Considers the impact of the security violation compromise on the SAP; determines whether the damage may be “localized” and, therefore, mitigated; considers reclassifying or declassifying any compromised SAP information; and incorporates changes in security classification of program information.

c. *Update.* As long as issues related to a compromise or security infraction remain unresolved, SAP PMs will provide monthly updates to HQDA (DAMI-CHS) via normal SAP reporting channels. Additionally, the PM will render a final report within 30 days of closure.

d. *Nickname or code word compromise.* If the association of a nickname or code word with a specific classified activity is compromised, or is suspected of being compromised, the program reports the incident in the manner described above and requests a new nickname or code word. TMO takes the necessary action to cancel the compromised nickname/code word in the Global Command and Control System database.

e. *Compromise of automated information systems.* If a compromise of SAP information involves automated information systems, the PM will consult HQDA (DAMI-CHS) to determine if the incident should be brought to the attention of the accreditation authority. The accreditation authority will, in turn, determine if the automated information system should be allowed to continue to process SAP information. All accreditation packages, after the discovery of the incident, will clearly identify the incident, its status, and any corrective action taken.

f. *Special situations.* The TMO in coordination with ODCSINT may direct that an investigation be initiated in situations where the action taken by the SAP manager or proponent did not fully address the potential compromise, or in other special situations.

Table 5-1
SAP security matrix

Criteria	N	I	II	III
ACCESS CONTROL				
Access Control Authority	*	Single	Single	Single
Access Approval Authority	*	Required	Required	Required
Billet Structure	*	Required	Required	Not Required
Levels of Access	*	Required	Not Required	Not Required
Access Roster	*	Required	Required	Required
Request for Access	*	Written	Written	Written
Indoctrination Forms, Non-disclosure Agreement	*	Required	Required	Required

Table 5-1
SAP security matrix—Continued

Criteria	N	I	II	III
SECURITY MANAGEMENT				
Security Manager	*	Full Time	Full Time	Part Time
Nickname (TMO)	*	Required	Required	Required
Code word (TMO)	*	Authorized	Authorized	Authorized
Document Control	*	Per AR 380-5	Per AR 380-5	Per AR 380-5
Secure Communication	*	Required	Required	Required
TSCM Survey	*	Required	Not Required	Not Required
Facility Security Risk Assessment	*	Required	Required	Required
Security Plan	*	Required	Required	Required
Information Management Support Plan (ISRP)	*	Required	Required	Required
ISRP	*	Required	Required	Required
Special Markings	*	AR 380-381	AR 380-381	AR 380-381
Foreign Knowledgeability	*	Not Authorized	Not Authorized	As Approved
Courier	*	Program cleared or DCS	Program cleared or DCS	Program cleared or DCS
SECURITY POLICY				
Minimum Level Security Clearance**	*	TS	TS or S	S
Type Investigation**	*	SSBI	SSBI or NAC/NACI	NAC/NACI
U.S. Citizen	*	Required	Required	Not Required
Polygraph ***	*	Random	Random	Random
Temporary Access	*	Authorized	Authorized	Authorized
Revalidation	*	Annual Required (SAPOC Brief)	Annual Required (SAPOC Brief)	Annual Required (SAPOC Brief)
PSAP Process	*	Required	Required	Required
INSCOM OPSEC Support (advise/assist)	*	Required	Required	Required
Special Mission Funds (SMF)	*	Authorized	Authorized	Authorized
"Carve-out" Contract	*	Not Authorized	Not Authorized	Not Authorized
Waivers		SAPOC Approved	SAPOC Approved	SAPOC Approved

Notes:

* In accordance with MOU between Army and SAP sponsor.

** Citizenship now required for SECRET clearance (May be waived by ODTUSD(P)(PS)).

*** When approved by SA.

Chapter 6 Access Control

6-1. Validation of access requirements

a. *The SAPOC.* The SAPOC validates each program's initial billet structure or access requirements and revalidates them annually until program disestablishment.

b. *TMO.* TMO provides management and oversight of access control and—

(1) Establishes the Army Baseline billet structure and manages baseline access as described in this chapter.

(2) Processes all requests for changes to program billet structures. Approves or disapproves requests for changes above the 5 percent or 100 billet annual change ceiling specified in paragraph 6-3 below.

(3) Directs changes to billet structures.

(4) Reviews and approves requests to double billet personnel for more than 90 days.

(5) Maintains a reference copy of access and billet data from each program. This data are updated by the programs no less than quarterly per paragraph 6-8.

c. *SAP proponents.* SAP proponents (MACOM/PEO/ARSTAF)—

(1) Appoint the Access Control Authority (ACA) and identify the ACA in the SAP security procedures guide. The ACA is a General Officer or SES employee in the chain of command for that program or activity. When the program manager is a General Officer or SES employee, the ACA responsibility falls to the next higher General Officer or SES employee. Besides the ACA, the Secretary, Under Secretary, Chief of Staff, and Vice Chief of Staff of the Army and the Chief, TMO, have authority to direct changes to billet structures and grant access to all Army SAP information.

(2) Provide direction and guidance to the ACA regarding management of access to the program.

d. *SAP access authorities.* SAP access control authorities (ACAs)—

(1) Specify access management controls in program security procedures guides.

(2) Appoint AAAs in writing. Appointment letters delineate the scope of the AAA's authority and authorize each AAA to indoctrinate and terminate access to the SAP. AAA authority cannot be further delegated.

(3) For Category I and II programs, identify that portion of the billet structure under the cognizance of each AAA.

(4) May delegate the authority to oversee the AAA's day-to-day activities to the program manager but retain access control responsibility for the program.

(5) Ensure that AAAs grant access to program information only to those persons essential to conducting the program, including those involved in management, execution, and oversight.

(6) Review indoctrination briefings annually and update as necessary.

e. *Access approval.* SAP AAAs—

(1) Approve/disapprove requests for access after verifying that they are correct and complete.

(2) Use the program approved briefing materials for indoctrinations.

(3) Send signed indoctrination and termination agreements to the office of record designated by the ACA. Individuals administratively debriefed will be notified in writing, if practical.

f. *Security managers.* Program security managers maintain each program's master access roster and are responsible for providing up-to-date security indoctrination briefings to program AAAs. Each program office is the office of record for program access.

6-2. Access levels

a. The complexity of the SAP or the special sensitivity of certain aspects of it may dictate the establishment of either additional levels of access or subcompartments.

(1) *Levels.* Levels of access are required within Category I SAPs. SAP proponents may define levels of access within Category II SAPs. Levels are designated numerically starting with Level I

(the lowest or most general administrative access) and leading to successively higher degrees of knowledgeability of the technical or operational details of the SAP. Level I access applies to administrative, clerical, or support personnel who are aware of the general nature of the program but do not require unrestricted access or knowledge of all details of the SAP. The highest level of access applies to individuals requiring unlimited access to all facts relating to the SAP. SAP proponents establish the number of levels and specify these in the program's security procedures guide.

(2) *Subcompartments.* Upon approval of TMO, proponents may devise subcompartments to limit knowledge of extremely sensitive aspects of the program. Proponents register all subcompartments with TMO. TMO assigns a nickname and/or a code word for each subcompartment. Individuals with access to subcompartments require at least an administrative level of access to the parent SAP and access only to those additional program subcompartments required. The SAP category of the subcompartment must be the same as the parent SAP.

b. Levels and subcompartments will not be established to avoid oversight. ACAs ensure that sufficient access is afforded to all levels and subcompartments to allow effective oversight.

c. The program manager will complete the following actions upon establishment of a subcompartment:

(1) The PM will establish the criteria for access to the subcompartment in accordance with SAPOC and TMO guidance.

(2) An individual accessed to only specific subcompartments of a SAP will sign an indoctrination statement that lists the specific subcompartments. The PSM will annotate BSMS records to show subcompartment access.

(3) The PSM will assist the PM in developing a subcompartment SCG.

(4) If required, a separate subcompartment PM and PSM will be designated in writing.

(5) If required, a separate SPG will address security responsibilities and countermeasures for personnel accessed to that subcompartment.

(6) When the subcompartment occurs outside of the program manager's Command, an MOU will be developed between the program manager's Command and the subcompartment program manager's command to outline program and security responsibilities. The MOU will be reviewed and approved by TMO prior to signature.

(7) Program managers review and inspect subcompartment management practices and procedures.

(8) DSS will be "carved in" for facility clearance inspections and industrial security reviews for all subcompartment contractor facilities.

6-3. Billet structure

a. *Category I and II.* Category I and II SAPs require a billet structure. Within 60 days following PSAP approval for a proposed Category I or II SAP, the proponent develops and submits to TMO a proposed billet structure. The proponent for the PSAP presents the billet structure to the SAPOC during the SAP approval process and makes adjustments as necessary before the annual revalidation process. TMO maintains a copy of all program billet structures.

b. *Baseline billets structure.* The Army SAP baseline billet structure identifies positions at HQDA and subordinate commands that require access to all baseline SAPs to fulfill leadership, oversight and management responsibilities. TMO determines SAPs to be included in the baseline, maintains the baseline billet structure, distributes changes to the structure, and publishes the complete baseline billet structure annually.

c. *Essential functions.* The individual SAP billet structure provides for essential program functions to include contractor, security, clerical and communications support, as well as staffing for other organizations necessary to implement and oversee the program. For baseline programs, the baseline billet structure is automatically incorporated into the program billet structure. For non-

baseline programs, the billet structure must include all program execution, management review, and oversight positions.

d. *Preparing billet structures.* Program managers use BSMS to prepare billet structures. Program managers should coordinate with TMO for instructions regarding the specific format of a billet structure.

e. *Modifications.* Within a 12-month period, each PM, on his or her own authority, may make modifications to the program billet structure that equate to 5 percent of the personnel accessed to the program, or 100 billets, whichever is less. If the PM requires more than 5 percent or 100 billet modifications during a given 12-month period, Chief, TMO must approve additional modifications. Program managers summarize changes to their billet structure during SAPOC revalidation briefings.

f. *Updates.* As billet structure changes occur, PMs forward updated pages to appropriate AAAs. After each SAPOC revalidation, PMs provide TMO and SRIA with an updated billet structure.

6-4. Rosters

a. Using BSMS software, SAP PMs maintain the master roster of individuals with access to the SAP. Access rosters contain full name, social security number, security clearance, date granted, type of investigation, investigation date, MACOM, organization, office, date access granted, and access level if appropriate. Additionally, PMs maintain an inactive roster listing all personnel debriefed from their program, recording the date of debriefing.

b. For programs with billet structures, AAAs slot individuals only against an approved vacant billet.

c. PSMs may double billet incoming personnel in the same billet with the incumbent for 90 days. TMO must approve extensions beyond 90 days. PSMs will not double billet personnel to satisfy short-term read-on requirements.

d. PMs notify access roster holders when individuals are read-off and provide quarterly updates of BSMS data to SRIA.

e. PMs must address disposition of program access rosters in the disestablishment concept plan.

f. Anyone may verify an individual's access to Army SAP information by—

(1) Contacting the program security staff.

(2) Contacting a duly appointed access approval authority having cognizance over the individual's organization.

(3) Using a current access roster.

(4) Checking BSMS.

6-5. Request for access

a. Possession of a valid security clearance does not by itself justify access to SAP information. Individuals must have a valid need-to-know, an approved billet (if applicable), and approval from the program ACA or designated AAA for access to a SAP.

b. Individuals nominating personnel for access to a SAP submit to the program AAA a request for access, DA Form 5749-R (Special Access Program Request for Access). A copy of DA Form 5749-R is at the back of this regulation for local reproduction on 8 1/2- by 11-inch paper. An authorized security official (for example, the security manager) verifies the individual's clearance data before signing and submitting the DA Form 5749-R to commander or PM for signature. Final approval for access rests with the ACA or designated AAA. The SAP PM maintains the DA Form 5749-R (RCS exempt, AR 335-15, para 5-2b(4)) for 2 years after reading off an individual, after which it is destroyed. Upon disestablishment of the SAP, the program disestablishment concept plan must address disposition of DA Forms 5749-R less than 2 years old at the time of disestablishment.

6-6. Indoctrination

a. Once an AAA has determined that an individual requires access to a SAP, the AAA indicates his or her approval on the DA Form 5749-R and signs the form.

b. AAAs can limit the duration of an individual's access. In these cases, the AAA or person conducting the read-on notifies the individual of the date when his/her access will end. This expiration date

is annotated on the indoctrination form (DA Form 5399-R (Special Access Program Initial Security Briefing)) (RCS exempt, AR 335-15, para 5-2b(4)). A copy of DA Form 5399-R is located at the back of this regulation for local reproduction purposes on 8 1/2- by 11-inch paper. The expiration date (if any) is included as an entry in the BSMS data base. When the expiration date arrives, if the individual has not already been debriefed, the PSM arranges for a debriefing. Examples of limited duration access are—

- (1) Short-term studies and analyses.
- (2) Normal tour of duty.
- (3) Limited duration operations.

c. Individuals authorized to indoctrinate personnel as follows:

(1) Verify the information on the DA Form 5399-R, including the individual's data and the program's nicknames. (Note "baseline" or "all Army SAPS" may be submitted for individual program names when appropriate.)

(2) Require individuals to read, agree to, and sign DA Form 5399-R before being indoctrinated.

(3) Provide a copy of the signed initial security briefing to the office of record, normally the program office.

(4) Include in the briefing program specific briefing security requirements (for example, what is sensitive about the program and why), procedures for OPSEC and COMSEC, EEFI, classification guidelines, SAEDA reporting, and how to report fraud, waste, and abuse without compromising security.

(5) Sign the DA Form 5399-R as the witness.

6-7. Termination

a. PSMs ensure individuals completing their duties with a SAP are debriefed by an authorized program representative. Once debriefed, the individual is no longer authorized access to SAP information and is not allowed to disclose program information in the future. PSMs, AAAs, or their designated representatives will use the locally reproducible DA Form 5401-R (Special Access Program Security Termination Briefing) (RCS exempt, AR 335-15, para 5-2b(4)) for termination briefings. (A copy is at the back of this regulation for local reproduction on 8 1/2- by 11-inch paper.)

b. In those instances when an individual cannot sign a termination briefing statement, the PSM will administratively terminate the individual's access and place the individual's name and date of termination on the inactive roster. Additionally, the person making the determination that an individual should be debriefed administratively will fill out a DA Form 5401-R (except for the individual's signature) and forward it to the office of record.

c. PMs and AAAs continuously review rosters, deleting individuals no longer requiring access to the SAP. The PM retains SAP access briefing and debriefing statements (for both actual and administrative debriefs) for 2 years after debriefing an individual after which they are destroyed.

6-8. Billet structure management system

a. The billet structure management system (BSMS) is an automated system for maintaining access and billet roster information for Army SAPs.

b. PMs will—

(1) Use BSMS to manage and maintain access and billet roster information.

(2) Provide regular BSMS data updates quarterly to the central BSMS data base at SRIA.

(3) Perform a comprehensive review and reconciliation of BSMS data at least annually.

(4) Provide an annual BSMS data base backup to the central BSMS data base at SRIA.

(5) Provide funding for BSMS hardware and software requirements.

c. SRIA will—

(1) Develop, document, maintain, develop training for, distribute, and upgrade the BSMS software.

(2) Provide regular updates of the BSMS data to the program managers and other designated users.

(3) Maintain the central BSMS data base for all Army SAPs.

(4) Provide customer service and training support for BSMS users as required.

(5) Provide projected budget data to BSMS sites.

Chapter 7 Industrial Security

7-1. Defense contractors

For purposes of this regulation, a defense contractor is any individual or entity that submits an offer for and is awarded a Government contract or conducts business with the Government as an agent or representative of another contractor.

7-2. National Industrial Security Program

a. The NISPOM specifies the baseline security procedures for contractors working on Federal Government projects. A supplement to the NISPOM specifies additional procedures that apply to SAPs.

b. The NISPOM Supplement specifies required security enhancements and provides a menu of optional security enhancements for use by SAPs. Programs may select from a menu of options to tailor SAP security based on the program's vulnerabilities to the threat. Any security enhancements above those specified as required or optional in the NISPOM Supplement must be approved by the OSD SAPOC.

7-3. Contractor Personnel Security

a. The basic personnel security requirements of the NISPOM and paragraph 5-4 of this regulation apply to contractors and subcontractors participating in Army SAPs. Contractors are cleared at the minimum level of classification commensurate with the level of work specified in the contract.

b. Defense contractor personnel requiring access to Army SAP information must consent to undergo random counterintelligence scope polygraph examinations. The PM must remove contractor personnel from the program who withdraw their consent to undergo a polygraph and report this action to the Contracting Officer.

7-4. Physical Security

a. The physical security standards contained in paragraph 5-2 of this regulation and the NISPOM with SAP Supplement provide basic guidance concerning physical security within contractor facilities. Each SAP's security procedures guide clarifies this basic guidance but cannot specify requirements greater than the NISPOM (with SAP Supplement) without OSD approval.

b. DSS coordinates exceptions to contractor facility construction standards to ensure standards do not conflict with NISPOM requirements.

c. DCI Directive (DCID) 1/21 applies to SAPs containing sensitive compartmented information.

7-5. Industrial Security Inspections

a. SAPs require fully documented comprehensive security inspections of contractors by qualified Government industrial security specialists. Under Army policy, the DSS conducts annual industrial security reviews of all contractor and subcontractor facilities containing Army SAP material. DSS has an inspection cadre for Army SAPs which follows contract security inspection standards set by the NISPOM, the NISPOM Supplement, and the program SPG.

b. SAP program offices or proponents coordinate DSS inspections. The SAP security office extracts appropriate security procedures from the NISPOM Supplement, highlights these in the program SPG, and provides them to the appropriately cleared DSS inspectors. Program offices attend DSS inspections only when a change in situation requires detailed program attention. Examples include the initial industrial security (IS) inspection of a facility, a new contractor, a new IS representative, a new contract security officer, or an anticipated security problem.

c. Army contracts excluding DSS are “carve-out” contracts. Requests to carve-out DSS from the industrial security inspection requirement for SAP contracts must include extensive justification and a detailed description of proposed carve-out contracting procedures. Programs submit such requests to TMO for Secretary of the Army review and DEPSECDEF approval. Carve-out procedures must comply with NISPOM Supplement, AR 380–49, and the Federal, Defense, and Army Acquisition Regulations. Normally, the Army does not approve carve-out requests.

(1) INSCOM inspects industrial security for approved carve-out contracts.

(2) Army SAPs with approved carve-out contracts report the status of these contracts at their annual SAPOC. This report includes the number of active carve-out contracts, number of contracts awarded during past year, total dollar value of all active carve-out contracts, the names of each carved-out prime and subcontractor, the total number of employees who have access to the SAP, justification for the need to continue the carve-out status of each contract and a summary of the results of the industrial security inspections conducted by INSCOM.

(3) When contracts no longer require carve-out status, proponents transfer the industrial security inspection responsibility to DSS and update the DD Form 254 (Contract Security Classification Specification Form) to reflect this change.

7–6. Contract Management

a. The program manager or proponent for a SAP, in coordination with his/her contracting officer, determines whether the program will employ secure environment contracting procedures and how the program and contracting officer will ensure positive fiscal and legal control. The PSM participates in these discussions and reviews the security practices of the supporting contracting office. The PM manages this process to provide control over potential financial and legal abuses.

b. The Defense Contract Audit Agency (DCAA) provides audit support by properly cleared auditors.

c. Supporting contracting organizations report SAP contract awards by preparing and submitting a DD Form 350, (Individual Contracting Action Report) in accordance with AR 715–30, Secure Environment Contracting.

d. SAP research and development contracts are assigned to the Defense Contract Management Command (DCMC) for secure environment contract administration under FAR Subpart 42.2 and Defense and Army FAR Supplements.

e. Contracting Officers will use a DD Form 254 (Contract Security Classification Specification) for each SAP contract. This document makes security requirements a legally binding part of the contract. The contracting officer forwards a copy of each DD Form 254, including all revisions, to TMO.

f. The PSM indoctrinates personnel involved in soliciting, evaluating, negotiating, approving, and awarding a SAP-related contract at an appropriate level. Those indoctrinated include the contracting officer, a legal representative, and appropriate contracting support personnel.

7–7. Security infractions, violations, and compromises at contractor facilities

a. Contractor personnel report compromises, suspected compromises, or other security infractions involving SAP information to the contractor security manager, who, in turn, immediately reports to the DSS industrial security representative and the PM who, in turn, immediately reports to the PSM and DSS. The contractor is required to conduct a preliminary investigation that outlines the details of the incident and submit a copy of the report of investigation if there is a probable compromise to the program office and DSS. DSS will conduct an administrative inquiry if they determine further action is necessary, or at the request of the program office. The PSM must inform DAMI–CHI through SAP reporting channels within 24 hours.

b. The contractor will include a statement of the administrative

actions taken against an employee in the report to DSS when an individual is found culpable and one or more of the following factors are evident:

(1) The violation occurred due to a deliberate disregard of security requirements.

(2) The violation involved a pattern of negligence or carelessness.

(3) There was a violation of the security terms of the contract.

c. Based on the investigation results, the PM makes a decision whether to terminate contractor access to the program.

7–8. Contract security requirements

a. The following security guidance is intended for industry.

(1) Program SCGs outline classification guidance for contractors.

(2) DD Form 254 specifies OPSEC requirements determined by the SAP PM.

(3) SAP PSMs prepare and sign the DD Form 254 for each SAP-related contract and the contracting officer reviews it prior to issue. This applies whether the contract itself is classified, an enclosure (such as the statement of work) is classified, or the contractor requires access to classified information. The PSM annotates block 16 of the DD Form 254 adding TMO to the distribution.

(4) For carve-out contracts, the DD Form 254 identifies all areas, material or information for which DSS retains security inspection responsibility and those remaining under Army security administration. The PSM annotates blocks 10c and d and block 15 of the DD Form 254 stating the contract contains certain carve-out information and provides a copy of the DD Form 254 to the responsible DSS security office.

(5) Army SAP contracts list AR 380–19, NISPOM, and this regulation in block 15 of the DD Form 254 as documents governing accreditation of contractor’s AIS.

(6) The program updates DD Forms 254 every 2 years or when there is a change to the program SCG. The PSM provides a copy of revisions to TMO.

(7) The SAP program manager is responsible for resolving questions or issues regarding the DD Form 254 or the classification guide.

b. Once a contract is complete, the contracting officer and PSM ensure the contractor—

(1) Inventories and returns all Government material to Government control.

(2) Processes contractor requests for post contract retention of classified material. Only the VCISA can approve such requests for contractor retention of documents other than that mandated by the Federal Acquisition Regulation (FAR).

(3) Disposes of classified material according to Army policies and regulations and provides a list of all material destroyed to the PSM.

Chapter 8 Information Mission Area

8–1. General

a. This chapter describes the essential parameters and procedures to follow to ensure the Information Management Area (IMA) support provided to Army SAPs and sensitive activities is secure. The IMA encompasses communications, automated information systems (AIS), audio/visual support, records management, printing and publications.

b. TMO establishes SAP-specific IMA policy and validates new requests for IMA support.

c. DISC4 approves all requests for Information Management (IM) support to SAPs and sensitive activities.

d. The USACECOM is the Army’s executive agent for information systems support of sensitive activities and serves as the DA focal point for staff management and oversight of IM support to sensitive activities.

e. At the direction of USACECOM, the Technology Application

Office (TAO) performs project management support of Army SAPs and sensitive activities.

8-2. Information Systems Requirements Package

SAP activities must document initial IM support requirements (for example, secure voice, data, facsimile systems) in an Information Systems Requirements Package (ISRP) and submit it as an enclosure to the initial request for PSAP status. A suggested format for an ISRP is at appendix K.

8-3. Information Management Support Plan

a. Following SAP establishment, program managers prepare detailed IMSPs. This plan identifies IM resources necessary to accomplish the assigned information mission throughout the program's life-cycle, drawing from ISRP requirements. The IMSP defines the system architecture, establishes configuration management, property accountability, acquisition strategy, information security oversight and command and control structure. The IMSP identifies the PM's future IS objectives, the current system and the strategy of how special access program IM goals are achieved.

b. The program manager oversees formulation and promulgation of the IMSP. Upon request, the TAO provides technical advice and support to PMs in preparing the IMSP.

c. Program managers submit the IMSP through TMO for review and concurrence to HQDA, DISC4, for validation and approval. The IMSP is the baseline for all IMA support of the program. Upon approval, the program manager will provide a copy of the IMSP to TMO who retains a copy of the plan to facilitate oversight. Appendix L outlines the suggested format for the IMSP.

8-4. Accreditation

a. Program managers are required to have all IM that process SAP information accredited under AR 380-19. Additionally—

(1) SAPs will operate systems in the dedicated security mode unless a waiver has been approved by HQDA (DAMI-IM).

(2) Program managers will request accreditation at the sensitivity level appropriate to the classification of the material involved. The accreditation authority for systems processing SAP information is the MACOM commander, or DA Staff agency director, unless the system is a single user system such as a personal computer. SAP managers accredit personal computers in accordance with AR 380-19. Army managers of SAPs with SCI content must accredit their IS in accordance with DCID 1/16 and agency-specific guidance. Accreditation for non-Army SAPs with no SCI content will be in accordance with AR 380-19 and program-specific guidance.

b. Program managers provide a coordinated accreditation package, any coordination reports, and their recommendations to the accrediting authority, who then determines if the automated system may process SAP information.

(1) Programs normally prepare accreditation packages without including SAP information and process them through the security office (of the command owning and operating the computer in question), to the appropriate accreditation authority. Security personnel need not be in an approved SAP billet to process this documentation.

(2) In those rare instances where an accreditation package must include SAP information, program managers will process the package through SAP channels to the appropriate accreditation authority.

8-5. System Maintenance

When maintenance or programming must be performed on IS that process SAP information, only the Information Systems Security Manager or Information Systems Security Officer for the SAP site may authorize the removal of system components from the SAP automation site including magnetic media. Systems components that cannot be declassified will not be removed from the automation site for maintenance. Programmers and maintenance personnel must have a security clearance commensurate with the highest level of information stored on the system in question.

8-6. Information Management support

a. Army sensitive activities and SAPs requiring IM support (as authorized in an approved IMSP) should submit their request to the U.S. Army Communications-Electronics Command, Technology Applications Office (TAO) (AMSEL-TA) with information copies to HQDA (DACS-DMP and SAIS-PAJ-O). The USACECOM TAO will review support requests for conformity with the approved program IMSP and justify, if appropriate, the use of special procedures in lieu of normal/routine support procedures. The USACECOM TAO will redirect all taskings which fall beyond the scope of an approved IMSP to TMO.

b. Army sensitive activities and SAPs requiring IM support, not reflected in an approved IMSP, will submit requests through TMO (DACS-DMP) for review and concurrence, to DISC4 (SAIS-PAJ-O) for validation and approval. DISC4 will subsequently forward approval support taskings to USACECOM-TAO for execution.

8-7. Records management

a. The PM will determine the records which are necessary to maintain "Adequate and Proper Documentation" of the program and its operations. SAP PMs will create and maintain a comprehensive documentation system in the form of record files to explain how decisions were reached and how business was conducted. Although access to these files is restricted, the records remain subject to appropriate HQDA and DOD oversight inspections. Program managers must ensure that needed records are recorded and maintained in official files. Program managers will also ensure that like requirements are included in the design and implementation of electronic systems supporting their programs. Records Management provisions must be included in the establishment and disestablishment planning process for each SAP.

b. Program Managers will maintain the record files per AR 25-400-2. File definitions, retention and disposition instructions for SAP-related files are found in the MARKS 380-381 file series. As a minimum, the SAP record file shall include—

- (1) Establishment files;
- (2) Policy file;
- (3) Operational files (to include access files);
- (4) Contract management files;
- (5) Financial management files;
- (6) Oversight files;
- (7) R&D specifications and drawings files;
- (8) Security management files;
- (9) Recurring report files;
- (10) Disestablishment files;
- (11) SAP congressional reporting files;
- (12) SAP critical technical data files;

c. The PM identifies, maintains, and forwards historical documents to be archived. When a PM identifies SAR-related records that are of no current use, but have historical value, he or she will contact the SRIA to place these records into the SAP archive. PMs will forward to SRIA only those permanent records that cannot be archived at another records holding area or Army records center. When a PM is preparing a SAP for disestablishment, he or she must contact SRIA, before developing a disestablishment concept, to coordinate archiving responsibilities. The 380-381 file series, AR 25-400-2, contains detailed retention and disposition instructions for SAP files. Detailed procedures to effect transfer of records are established in the SRIA Records Management Memorandum of Instruction.

d. Records submitted to the SRIA will include, as a minimum, the following:

- (1) SAP establishment files
- (2) SAP congressional reporting files
- (3) SAP critical technical data files
- (4) SAP annual and recurring reports files
- (5) SAP disestablishment files;

e. PMs will send retirement requests for SAP and SAP related sensitive records to SRIA (DACS-DMP-SR), Chief of Staff, 200 Army Pentagon, Washington, DC 20310-0200. PMs must submit

the following information in their archiving request: the originating agency; the SAP program; highest classification of enclosures; number of documents and total number of pages being forwarded; method of transfer; desired dates of transfer; program POC name, address, telephone, and FAX numbers. Transfer of records to HQDA (SRIA) will be governed by the SRIA Memorandum of Instruction for Transfer of Records and by procedures found in AR 25-400-2.

Chapter 9 Funding

9-1. SAP funding

The Army will fund only properly registered and approved SAPs. TMO is required to report all Army-funded SAPs to Congress on an annual basis.

9-2. Establishment phase

a. During the SAP establishment phase, the MACOM/PEO submits a memorandum proposing the program for SAP status (see app B). This proposal must include an estimated amount of funds needed for the program, listed by appropriation (for example, RDTE, procurement and OMA funds).

b. The ARSTAF proponent, PA&E, and ASA(FM) evaluate the proposed funding and management structure. The management structure must specify distinct program elements (PE), project codes and standard study numbers (SSN). The ARSTAF proponent also assigns the program to the appropriate Management Decision Package (MDEP).

c. MACOM/PEO/PMs are prohibited from providing funds to PSAP requirements without prior written authorization of Chief, TMO. Chief, TMO can authorize funds for administration and security purposes for a PSAP until SAP status is granted by OSD (30 days after congressional notification).

9-3. Maintenance phase

a. *Budget estimate submission.* Program managers justify a continuing need to fund a program by submitting a budget estimate submission (BES) every August. The BES identifies resources necessary to maintain the program and provides information on the prior year, the current year and the 2 budget years. OSD publishes guidance annually regarding the format and suspense dates for Budget Exhibits.

b. *Program budget decision.* Program budget decisions (PBDs) are issued between October and December, after OSD's review of the BES. Using the PBD, OSD proposes changes to the Army Budget. The Army then has the opportunity to submit reclaims (counter-arguments) to OSD. To facilitate the preparation of these reclaims, MACOMs/PEOs provide input to appropriate ARSTAF proponents who validate the input and forward reclaims through TMO to ASA(FM&C).

c. *SAP reprogramming.* Reprogramming includes transfers between appropriations, transfers between program elements (PE) internal to an appropriation, and transfers within a PE from one project code to another.

(1) Reprogramming requests must be evaluated in terms of DOD guidance provided in DODFMR Volume 3, on requirements for Congressional notification and/or prior approval. If congressional notification or prior approval is required, the USA will be the Army's approval authority for reprogramming.

(2) When USA approval is not required, the ARSTAF proponent can approve SAP reprogramming requests after review by the offices listed in (3) below. ARSTAF proponents for SAPs at HQDA are: ASA(RDA) for acquisition SAPs, ODCSINT for intelligence SAPs, and ODCSOPS for operations and support SAPs. (Reprogramming Format is at app I.)

(3) Regardless of the approving official, all requests to reprogram SAP funds must be reviewed by: ASA(FM&C), TMO, OTJAG,

OGC and PAED. ASA(FM&C) will ensure the reprogramming action complies with HQDA directives and DOD guidance. Requests en route to the USA will also be reviewed by the VCSA.

(4) TMO will prepare a summary report in October, for the USA, listing all SAP reprogramming executed during the fiscal year.

9-4. Disestablishment

When disestablishing a SAP, the MACOM/PEO prepares a disestablishment concept plan that addresses fiscal control (app F). The plan identifies SAP budget lines that will have funds remaining when the program disestablishes and proposes disposition of these funds.

9-5. Annual SAP reports

In the first quarter of each fiscal year, SAP managers submit a SAP Report through the ARSTAF proponent to TMO. OUSD(A&T)/DSP provides the report format and preparation instructions in a memorandum to the Services. SAP reports cover program activities of the past fiscal year, planned activities and funding requirements, and justification for continued SAP status. TMO consolidates these SAP reports and submits them to OUSD(A&T)/DSP. OUSD(A&T)/DSP consolidates the reports of each Service for submission to Congress. These reports collectively become the justification book for the classified portion of the President's Budget. OSD publishes guidance annually regarding format and suspense dates for SAP reports.

Appendix A References

Section I Required Publications

AR 11-2

Management Control. (Cited in para 4-2a.)

AR 25-400-2

Modern Army Recordkeeping System (MARKS). (Cited in para 2-31a.)

AR 380-5

Information Security Program. (Cited in paras 4-2e(4), 4-2l, 5-2d, 5-3c, 5-3h(1), 5-3l, 5-3j, 5-8b(3).)

AR 380-19

Information Systems Security. (Cited in para 7-8a(5), 8-5a(2), and 8-8c.)

(U) AR 380-19-1

Control of Compromising Emanations (C). (Cited in para 5-3c(1).)

AR 380-67

Personnel Security Program. (Cited in para 5-4b(1) and 5-4e.)

(U) AR 381-14

Military Intelligence Technical Surveillance Countermeasures (S). (Cited in para 5-5c(3).)

AR 530-1

Operations Security (OPSEC). (Cited in para 4-2 and 5-8e.)

AR 715-30

Secure Environment Contracting. (Cited in para 7-6c.)

DOD 5220.22-M

National Industrial Security Program Operating Manual. (Cited in paras 5-2d, 5-3e, 5-4b(1), 7-2, 7-3a, 7-4a, 7-5a.)

DOD 5220-22-M Supplement

National Industrial Security Program Operating Manual Supplement. (Cited in 7-2b.)

Section II Related Publications

A related publication is a source of additional information. The user does not have to read a related publication in order to understand or use this regulation.

AR 1-1

Planning, Programming, Budgeting and Budgeting Execution System

AR 11-7

Internal Review

AR 20-1

Inspector General Activities and Procedures

AR 25-1

The Army Information Management Resources Program

AR 25-55

Army Freedom of Information Act Program

AR 37-47

Contingency Funds of the Secretary of the Army

(U) AR 37-64

Finance and Accounting for Special Mission Funds (C)

AR 37-100-Series

The Army Management Structure

AR 70-1

Systems Acquisition Policy and Procedures

AR 70-6

Management of the Research, Development, Test, and Evaluation Army Appropriation

AR 70-9

Army Research Information Systems and Report

AR 70-10

Test and Evaluation During Development and Acquisition of Materiel

AR 70-11

Dissemination of Scientific and Technical Information

AR 71-3

User Testing

AR 71-9

Materiel Objectives and Requirements

AR 195-2

Criminal Investigative Activities

AR 195-6

DA Polygraph Activities

AR 335-15

Management Information Control System

AR 380-10

Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives.

AR 380-28

Army Special Security Officer and Office System

AR 380-40

Policy for Safeguarding and Controlling COMSEC Materiel

AR 380-49

Industrial Security

AR 380-53

Communications Security Monitoring

AR 381-10

U.S. Army Intelligence Activities

AR 381-11

Threat Support to U.S. Army Force, Combat, and Materiel Development

AR 381-20

The Army Counterintelligence Program

AR 381-25

Safeguarding Information Pertaining to Certain HUMINT Activities

(U) AR 381-26

Foreign Materiel Exploitation Program (C)

(U) AR 381-47

USA Counterespionage Activities (S)

(U) AR 381-102

Intelligence Operational Support Activities (S)

(U) AR 381-141

Provisions for Administration, Supervision, Control, and Use of Intelligence Contingency Funds (C)

(U) AR 381-143

Logistics Policies and Procedures (C)

AR 600-50

Standards of Conduct

DOD 5200.1-R

Information Security Program

DOD 5200.2-R

Personnel Security Program

DOD 5205.7

Special Access Programs

DOD 5210.48-R

DOD Polygraph Program

DOD 5210.74

Security of Defense Contractor Telecommunications

DOD 5230.11

Disclosure of Classified Military Information to Foreign Governments and International Organizations

DOD 5505.2

Criminal Investigations of Fraud Offenses

(U) DOD S-5105.21-M-1

Sensitive Compartmented Information Administrative Security Manual (C)

(U) DOD TS-5105.21-M-2

Sensitive Compartmented Information (SCI) Security Manual, COMMINT Policy (S)

(U) DOD TS-5105.21-M-3

Sensitive Compartmented Information (SCI) Security Manual, TK Policy (TS)

(U) DOD S-5210.36

Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the U.S. Government (S)

DOD 7000.14-R Volume 5

Department of Defense Financial Management Regulation (Disbursing Policy and Procedures)

DOD 7250.5

Reprogramming of Appropriated Funds

DOD 7600.7-M

Internal Audit Manual

DFAS 37-1

Finance and Accounting Policy Implementation

Section III

Prescribed Forms

DA Form 5399-R

Special Access Program Initial Security Briefing (Prescribed in para 6-6.)

DA Form 5401-R

Special Access Program Security Termination Briefing. (Prescribed in para 6-7.)

DA Form 5749-R

Special Access Program Request for Access. (Prescribed in para 6-5.)

DA Form 5750-R

Inadvertent Disclosure Oath. (Prescribed in para 5-9.)

Section IV

Referenced Forms

DD Form 254

(Contract Security Classification Specification)

DD Form 350

(Individual Contracting Action Report)

Appendix B

Establishment

B-1. Establishment Checklist/Timeline

The following (table B-1) is a list of the major events required to establish a SAP.

**Table B-1
SAP establishment timeline**

Day	Event
0	Memo requesting PSAP status sent to TMO.
15	PSAP memo staffed within HQDA.
40	TMO approves PSAP and dispatches PSAP approval memo to PMSAP security controls applied. Guidance on request for SAP establishment memo given. Knowledgeability roster started.
60	Proponent submission of proposed structure and manning proposal to USAFMSA for preliminary validation.
100	PM submits draft security plan/billet structure, draft SAPOC briefing slides, and Request to Establish SAP memo to TMO.
120	USAFMSA manpower report submitted.
130	TMO conducts working SAPOC.
160	HQ DA SAPOC meets.
180	TMO submits SAPOC paperwork to OSD.
220	DEPSECDEF approves SAP.
Tbd	OSD submits notification letters to Congress.
Tbd+30	SAP can obligate funds.

B-2. Format for requesting establishment of a prospective Special Access Program

a. The proponent submits a request to establish a PSAP in the format shown below through the chain-of-command to TMO.

b. Format of the request follows.

(1) Agency/proponent of the PSAP and chain of command from program office to HQDA.

(2) Relationship to other programs in DOD or other Government agencies.

(3) Rationale for PSAP establishment.

(a) Critical elements (essential program information, technologies, and systems (EPITS)) of the program which cannot be adequately protected under the provisions of AR 380-5 and reasons why collateral measures are inadequate.

(b) Recommendation and justification of category for the SAP.

(4) Funding sources and funding profile by appropriation.

(5) Key Program Personnel

(a) Agency POC (position, address, and phone).

(b) Program manager (address and phone).

(c) Program security manager (address and phone).

B-3. Format for requesting establishment of a Special Access Program (SAP)

The proponent submits a request to establish a SAP to TMO in the format shown below.

a. Agency/proponent and chain of command from Program Office to HQDA.

b. PSAP establishment date.

c. Relationship to other programs in DOD or other Government agency.

d. Rationale for SAP establishment.

(1) Critical elements of the program which cannot be adequately protected under the provisions of AR 380-5 and reasons why collateral measures are inadequate.

(2) Multidisciplined counterintelligence threat to the program.

(3) Recommended SAP category with rationale.

e. Access.

(1) Access Control Authority

(2) Access Approval Authorities.

(3) Estimated number of people with access.

f. Program Security Plan (include Security Classification Guide, Security Procedures Guide, OPSEC Plan, billet structure and program indoctrination briefing).

g. Key Program Personnel (include address and phone numbers).

(1) Program manager.

(2) Program security manager.

(3) Contracting office and its location.

h. Information Systems Requirements Package

i. Any Memoranda of Understanding (MOUs) (if applicable).

j. Anticipated cost, proposed funding profile and location of accounting support.

k. Management control for the program.

l. Proposed manpower requirements and personnel profile displayed by officer, warrant officer, enlisted, and DA civilian. Include proposed grade and MOS/job series.

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

(2) Has the Secretary or the Deputy Secretary of Defense approved the program for SAP status?

(3) Does the Program Manager have a copy of the SAP approval document?

(4) Have manpower authorizations been validated by DCSOPS within the past 12 months?

(5) Is the program's nickname and subcompartment nicknames or code words, if appropriate, assigned by the Technology Management Office (TMO)?

(6) Is the SAP revalidation approval briefing presented annually to the SAPOC?

b. *CATEGORY: SAP Security Management.*

(1) Are the program's security measures commensurate with the program's category level (UP AR 380-381) and the threat?

(2) Is the security officer's status (full time or part time) consistent with the program's category?

(3) Does the program have a current security plan which includes a security procedures guide, classification guide and OPSEC plan?

(4) Are CAT I and II program billet structures current, accurate and sufficient (that is, meet security and operational needs)?

(5) Are program access rosters current and accurate?

(6) Is the classification guide current? Did the TOP SECRET original classification authority (OCA) approve the SCG?

(7) Does the program have required counterintelligence documentation to include a comprehensive OPSEC assessment, annual OPSEC assessment and technical services plan (when required)?

(8) Has the ACA identified in writing all access approval authorities (AAA) for the program?

(9) Do all access approval authorities (AAAs) have a listing of their duties and responsibilities?

c. *CATEGORY: Secure Environment Contracting (SEC).*

(1) Do vendors have adequate protection for SAP material?

(2) Has the DD Form 254 been forwarded to TMO and DSS?

(3) If a patent contains SAP information, was FAR Clause 52.227-10 included in the contract? Did the vendor forward the proposed patent through the Procuring Contracting Officer (PCO) to the SAP program manager? Did the Program Manager forward the patent filing information through HQDA, ASA(RDA) ATTN: SARD-SO, to TMO for VCSA approval?

d. *CATEGORY: Financial Management.*

(1) Does the Program report accurate information to the HQDA SAP Program Performance and Budget Execution Review System (PPBERS) committee?

(2) Are all reprogrammed funds approved by the Under Secretary of the Army or by the ARSTAF proponent?

(3) Are the program's SAP funding nicknames assigned by the TMO?

(4) Does the program prepare and submit a congressional descriptive summary (CDS) annually?

(5) Are annual budgets submitted to support timely receipt of funding for program operations?

e. *CATEGORY: Audits and Inspections.*

(1) Has the program manager coordinated with the supporting IRAC office to ensure the SAP is included in the command's auditable entity file?

(2) Has an IRAC auditor reviewed the MCP annual assurance statement for SAP considerations?

(3) Do auditors have program access to conduct reviews?

(4) Has the SAP had an USAAA audit or SAIG-IO inspection within the past 2 years?

(5) Are non-IRAC audit and inspection findings formally incorporated into the Fix-It process and tracked until resolved?

f. *CATEGORY: Information Systems and SAP Records Management.*

(1) Is the program IMSP current and has it been submitted through the TMO for approval by DISC4?

(2) Are the Program's Automated Information Systems (AIS) accredited?

(3) Does the Program security procedures guide address AIS and comply with appropriate regulations?

Appendix C Management Control Evaluation Checklist

C-1. Function

Use this management control evaluation checklist for Special Access Programs (SAPs), AR 380-381

C-2. Purpose

Use of this checklist assists MACOM commanders, program executive officers, and program managers in their key management controls. It is not intended to cover all controls.

C-3. Instructions

Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, interviewing, sampling, simulation, other). Answers that indicate deficiencies must be explained and corrective action indicated in the supporting documentation. These management controls must be evaluated every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2-R (Management Control Evaluation Certification Statement). DA Form 11-2-R is at the back of this publication to be locally reproduced on 8 1/2-by 11-inch paper.

C-4. Test questions

The test questions below are divided into categories involving separate areas of SAP management controls.

a. *CATEGORY: SAP Management.*

(1) Has the Army SAPOC recommended the program for SAP status?

(4) Has the Program office established SAP files in accordance with AR 25-400-2?

(5) Does the program office review and separate permanent files and other appropriate documents for transfer to SRIA?

(6) Does the Program office destroy SAP temporary files and working documents in accordance with AR 25-400-2 and AR 380-5?

C-5. Comments

Help make this a better review tool. Submit comments to the HQDA functional proponent: Chief of Staff (Technology Management Office (DACS-DMP)), 200 Army Pentagon, Washington, DC 20310-0200.

**Appendix D
Format for SAPOC Briefing**

D-1. Program description (fig D-1)

- Mission statement or purpose.
- Program origin.

D-2. Justification for SAP category (fig D-2)

- What requires protection.
- Security objectives.
- Justification for category 1 status (if applicable).

D-3. Relationship to other programs (fig D-3)

- DA, AF, Navy.

D-4. Foreign targets and technology (fig D-4)

D-5. External threat assessment (fig D-5)

D-6. Security assessment (fig D-6)

D-7. Access status (fig D-7)

- Total number of billets (CAT I & II).
- Current total number having access.
- Number change from previous year.
- ACA and list of AAAs.

D-8. Milestone chart (fig D-8)

- Highlight any past SAPOC decisions affecting program.

D-9. Funding profile (fig D-9)

- Current/projected funding (amount and source).
- Location of FAO support.

D-10. Manpower profile (fig D-10)

- Personnel number (working in the program).
- Date of last manpower survey.

D-11. Contracting (fig D-11)

D-12. SAP inspections and audits (fig D-12)

D-13. Issues/problems (fig D-13)

D-14. Decision sought (fig D-14)

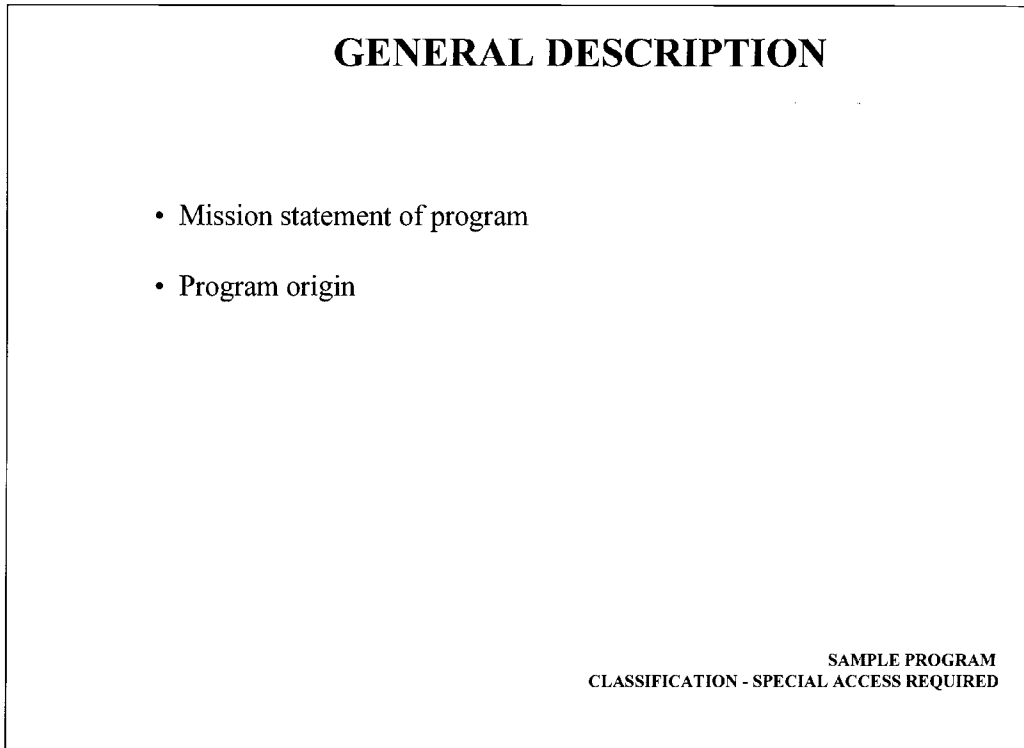


Figure D-1. Program description

SAP JUSTIFICATION

- What requires protection
- Program security objectives
- Category I justification (if applicable)

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-2. Justification for SAP category

RELATIONSHIP TO OTHER PROGRAMS

- Relationship to another Army program or other service program
- Dependency on other SAPs
- Impact on other SAPs

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-3. Relationship to other programs

FOREIGN TARGETS & TECHNOLOGY

- Those adversary systems the SAP will attack
- Those countermeasures the adversary could pursue to defeat our SAP technology
- Any foreign interest/progress in similar technology

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-4. Foreign targets and technology

EXTERNAL THREAT ASSESSMENT

- **HUMINT**
 - Open Source Data
 - Collection Efforts
- **SIGINT**
 - ELINT
 - COMINT
- **IMINT**
 - Overhead
 - Hand held
- **MASINT**
- **OTHER**

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-5. External threat assessment

SECURITY ASSESSMENT

- Extent of external interest in SAP technology
- Scope of collection efforts against the SAP
- Compromise(s) in the past year
- Damage assessment of compromise(s) - if applicable
- Assessment of overall security posture

* Identify the activity providing security support

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

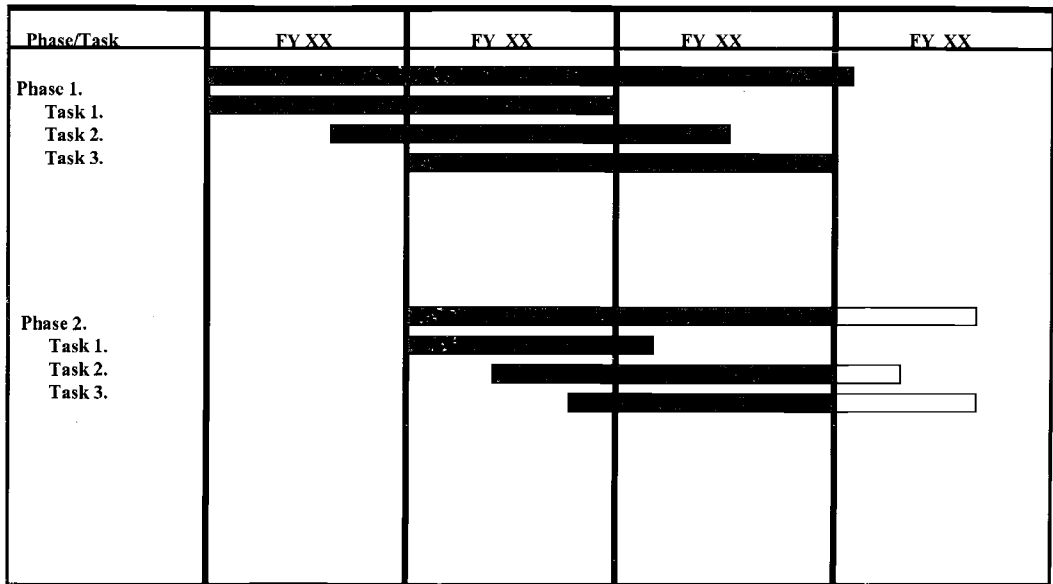
Figure D-6. Security assessment

ACCESS AND SECURITY STATUS

- **TOTAL NUMBER OF BILLETS**
 - PREVIOUS YEAR
 - THIS YEAR
- **TOTAL NUMBER WITH ACCESS**
 - PREVIOUS YEAR
 - THIS YEAR
 - PERCENT +/-
- **IDENTIFY ACA**
- **IDENTIFY ACCESS APPROVAL AUTHORITIES**

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-7. Access status



Legend
 Funded
 Unfunded

SAMPLE PROGRAM
 CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-8. Milestone chart

FUNDING PROFILE (\$M)						
PROGRAM BY YEAR	FYDP					TOTAL OUT YEAR COST
	PGM COST PRIOR YEARS	CURRENT				
		FY	FY XX	FY XX	FY XX	
RDTE (PE/PROJ)	82.2	2.3	3.4	1.2	0.2	---
	---	---	---	---	---	---
PROCUREMENT (SSN)	---	---	1.2	0.2	3.4	2.1
OMA	---	---	---	---	0.1	---

* FAO Support Provided by _____

SAMPLE PROGRAM
 CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-9. Funding profile

MANPOWER PROFILE

OFFICER	4
WARRANT OFFICER	----
ENLISTED	24
CILIVIAN	6
CONTRACTOR	----

LAST USAFMSA MANPOWER SURVEY: _____

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-10. Manpower profile

CONTRACTING

- IDENTIFY SAP CONTRACTING OFFICER
- LIST MAJOR CONTRACTORS
- REAFFIRM SAP HAS NO CARVE-OUT CONTRACTS
- PORTRAY EXTENT OF DCAS/DCAA/DCMC INVOLVEMENT

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-11. Contracting

SAP INSPECTIONS & AUDITS

<u>AGENCY</u>	<u>DATE</u>	<u>RESULTS</u>
DODIG	FEB XX	OUTSTANDING - NO FINDINGS
AAA	JUN XX	SATISFACTORY - 2 FINDINGS
DIS	MAY XX	UNSATISFACTORY - 4 FINDINGS
MACOM IR	JAN XX	SATISFACTORY

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-12. SAP inspections and audits

ISSUES/PROBLEMS *

- SECURITY
- PROGRAMMATIC
- FUNDING
- LEGAL
- CONTRACTING
- TECHNICAL

* IDENTIFY AS APPROPRIATE - OR NONE

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-13. Issues/problems

DECISIONS SOUGHT

•RECOMMENDATION OPTIONS:

- Revalidate SAP status
- Approve SAP status
- Disestablish SAP
- Transfer SAP to another DOD entity

SAMPLE PROGRAM
CLASSIFICATION - SPECIAL ACCESS REQUIRED

Figure D-14. Decision sought

Appendix E Guidance on Preparing the Standard SAPOC Slide (QUAD Chart)

The following is guidance to be used to prepare the standard SAPOC slide (QUAD Chart).

UPPER LEFT HAND SIDE:

1. Photo/line drawing/artist sketch of item being developed. If a technology, an illustration of the technology application. An explanatory caption may be included.
2. "A picture is worth a thousand words."

UPPER RIGHT HAND SIDE:

1. Program status.
2. Important issues affecting program status or progress.

LOWER LEFT HAND SIDE

1. BRIEF program description. What is it? Where is program going? What need does it fill? Why is it a SAP?
2. Highlight major points and successes or problems.

LOWER RIGHT HAND SIDE:

1. Include current FY and next two FYs as a minimum.
2. Include most recent or next (whichever is closer) milestone or DAB level review.

3. FY total includes all types of \$ (R&D, Procurement, O&M, and so forth)
4. Schedule bars should be accurate to the month if possible.

FORMAT INSTRUCTIONS:

1. Slide generated using Powerpoint software.
2. Slide is black background — Words and lines are white unless otherwise specified.
3. Page setup is 9.4 by 7.4 inches. Box is 9.0 by 6.6 inches centered on the page.
4. All fonts are HELVETICA.
5. Classification is red (RD8), bolded, 18 point.
6. Major headings (STATUS — ISSUES, XXX YYYY PROGRAM, and BUDGET & SCHEDULE) are bold, 14 point.
7. Bullets are 85 percent of character size — color yellow (YW8).
8. Program narrative and issues are 12 point, non-bold.
9. Budget & Schedule headings are 14 point, non-bold.
10. Budget & Schedule detail is 12 point, non-bold.
11. Follow-on slides use the same layout, letter sizes and color scheme except quad chart format not required.

ENTER CLASSIFICATION HERE (18PT ARIAL BOLD RED)

<p>PICTURE</p>	<p align="center">STATUS - ISSUES (ARIAL 14 PT BOLD)</p> <ul style="list-style-type: none"> • BULLETS FORMAT (ARIAL, 12PT NORMAL) • BRIEF STATUS SUMMARY • IMPORTANT ISSUES • BULLETS IN YELLOW 																																								
<p align="center">XXX YYY PROGRAM (ARIAL 14PT BOLD)</p> <p>PROGRAM DESCRIPTION, BRIEF NARRATIVE FORM</p> <ul style="list-style-type: none"> • BULLETS FORMAT (ARIAL 12PT NORMAL) • ITEM 1 • ITEM 2 • BULLETS IN YELLOW 	<p align="center">BUDGET AND SCHEDULE (ARIAL 14PT BOLD RED)</p> <table border="1" style="width:100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="font-size: small;">TASK</th> <th style="font-size: small;">FY XX</th> <th style="font-size: small;">FY XX</th> <th style="font-size: small;">FY XX</th> </tr> </thead> <tbody> <tr> <td style="font-size: x-small;">GO AHEAD</td> <td>▲</td> <td></td> <td></td> </tr> <tr> <td style="font-size: x-small;">DESIGN/FAB</td> <td colspan="3" style="background-color: black; height: 10px;"></td> </tr> <tr> <td style="font-size: x-small;">INTEG/TEST</td> <td></td> <td colspan="2" style="background-color: black; height: 10px;"></td> </tr> <tr> <td style="font-size: x-small;">DEPLOY</td> <td></td> <td></td> <td style="background-color: black; height: 10px;"></td> </tr> <tr> <td style="font-size: x-small;">COMPLETE</td> <td></td> <td></td> <td>▲</td> </tr> <tr> <td style="font-size: x-small;">RDTE</td> <td>1.1</td> <td>2.5</td> <td>.5</td> </tr> <tr> <td style="font-size: x-small;">OPA</td> <td></td> <td>1.1</td> <td>2.2</td> </tr> <tr> <td style="font-size: x-small;">OMA</td> <td>2</td> <td>2</td> <td>1.0</td> </tr> <tr> <td style="font-size: x-small;">TOTAL</td> <td>1.3</td> <td>3.8</td> <td>3.7</td> </tr> </tbody> </table>	TASK	FY XX	FY XX	FY XX	GO AHEAD	▲			DESIGN/FAB				INTEG/TEST				DEPLOY				COMPLETE			▲	RDTE	1.1	2.5	.5	OPA		1.1	2.2	OMA	2	2	1.0	TOTAL	1.3	3.8	3.7
TASK	FY XX	FY XX	FY XX																																						
GO AHEAD	▲																																								
DESIGN/FAB																																									
INTEG/TEST																																									
DEPLOY																																									
COMPLETE			▲																																						
RDTE	1.1	2.5	.5																																						
OPA		1.1	2.2																																						
OMA	2	2	1.0																																						
TOTAL	1.3	3.8	3.7																																						

ENTER CLASSIFICATION HERE (18PT ARIAL BOLD RED)

Figure E-1. Quad chart

**Appendix F
Disestablishment Concept Plan**

F-1. Format

There is no prescribed format for the disestablishment concept plan.

F-2. Content

Each disestablishment concept plan must address the following:

- a. Basis/rationale for disestablishment.
- b. Fiscal controls. What is the plan for funds not obligated and funds obligated but not disbursed? What is the plan for transfer and control of prior year accounting records?
- c. Recommended disposition of SAP records and files.
- d. Disposition of any Government-owned property, both GFE or purchased by vendor.
- e. Recommendation on security level of remaining program, if any (collateral, incorporated into another SAP, unclassified, and so forth).
- f. Legal considerations.
- g. Coordination with appropriate ARSTAF proponent, DAMI-CHS, and TMO to ensure new security guidance is applied to any related DOD program.
- h. How debriefings are to be handled.
- i. How documents are to be remarked.

j. Contracting considerations. Close out and final contract payment reconciliation with funds obligated in accounting records.

Note. Contractor turns over all SAP material to the PSM.

**Appendix G
Disestablishment Certification Checklist**

G-1. Checklist

MACOMs/PEOs and PMs use this checklist to certify SAP disestablishment is complete:

- a. Access controls eliminated.
- b. Normal oversight restored.
- c. Disposition of SAP funds finalized (current and prior year).
- d. LOAs and EADs for SMF or ICF canceled, if applicable.
- e. Status of open contracts compared with funds available.
- f. Project funds reprogrammed.
- g. Nickname and/or code words no longer in use.
- h. Indoctrination forms no longer used.
- i. Special markings no longer used.
- j. Polygraph program terminated (if applicable).
- k. DSS notified.
- l. Updated SCG published and distributed.
- m. SAP security plan no longer used.
- n. SAP hardware properly disposed.
- o. SAP files and records properly disposed.

p. Debriefings complete.

q. Updated DD Form 254 issued to the contractor by contracting officer detailing his or her actions concerning program material and security.

r. USAFMSA notified.

G-2. Certification memorandum

After the MACOM/PEO, in coordination with INSCOM/902nd MIG, certifies that disestablishment is complete, the program managers will forward a memorandum through the chain of command to TMO specifying all actions specified in this checklist are complete.

Appendix H Program Performance and Budget Execution Review System Charts

Use the following instructions to complete the PBBERS charts (figs H-1 and H-2).

H-1. Paper and markings

Prepare a PBBERS chart for each program appropriation on 8 1/2- by 11-inch white bond paper and place proper security classification markings at the top and bottom of each chart. See figure H-1.

H-2. Fiscal year and quarter

In the upper left block entitled "FY" and "Qtr," enter the fiscal year and quarter under review.

H-3. Program nickname

In the upper middle block entitled "PGM," enter actual program nicknames. Do not use funding nicknames.

H-4. Current year

Directly under the "Overall Program Objective," display bar graphs of planned and actual obligations and disbursements for current FY funding. Enter the type of appropriation (that is, RDTE, OMA or PROC) at the top center of the bar graph. The "X" axis shows the quarters of the fiscal year; the "Y" axis on the left side shows the program dollars in millions. The columns represent amounts cumulative by quarter. The "Y" axis on the right side shows the percent of total program.

H-5. Obligations and disbursements

The block directly under the bar graph entitled "Resource Details" contains cumulative amounts of obligations and disbursements and is divided as follows:

a. "QTR/FY" – Use the first line to display the previous year cumulative amounts (plan and actual obligations; actual disbursements). Break out current year amounts by quarter.

b. "Plan" – Equals the cumulative amount of funds planned for obligation. This figure does not include prior year funding carried over.

c. "Actual" – Reflects actual cumulative obligations and disbursements shown at the end of quarter in official accounting reports.

d. "DA GOAL" – Shows the DA goal percentage.

e. "ACTUAL" (% Program) – Shows the percentage derived by dividing the actual obligations/disbursements by the total programmed amount for that FY (that is, the amount shown in the resource summary block). Address all deviations > 10 percent in the analysis section.

H-6. Deviation

In the top upper right-hand corner of the chart, rate the program RED (deviation > 15 percent), AMBER (deviation 10-15 percent), or GREEN (deviation < 10%).

H-7. Program office

In the upper right-hand block entitled "Proponent," enter the name of the program office, POC, and telephone number.

H-8. Funding

Directly under "Proponent" is the "Resource Summary" block. The first subheading shows funds "appropriated" by Congress for the current and previous year. The "Programmed" amount is the appropriated amount minus adjustments for Small Business Innovation Research (SBIR), closed account, and approved reprogrammings. In the upper right corner of the block, enter the Program Element (PE).

H-9. Discussion

In the "Analysis" block, discuss—

a. Plans for funds carried over from previous FY.

b. Why actual obligations or disbursements differed from plan (if > 10 percent), and how and when the program will be back on track.

c. What unresolved issues remain.

d. Differences between appropriated and programmed amounts (that is, SBIR, closed account, and reprogrammings).

e. Current personnel strength for military and civilian employees, including matrix support. Here you must show all personnel who spend at least 50 percent of their time in support of the program. Totals must be in whole numbers and must be updated quarterly.

f. Date of the last audit (DAIG, DODIG, AAA, and so forth).

H-10. OMA funds

Prepare a separate PBBERS chart for OMA funds. Enter current fiscal year data only. Track obligations only. See OMA sample at figure H-2.

H-11. Procurement funds

Prepare a separate PBBERS chart for procurement funds. Enter the same data as shown on the RDTE sample PBBERS chart (figure H-1). Since procurement SAPS are funded for 3 years, prepare a summary line for each of the 2 preceding years above the current year's quarterly breakdown in the "resource details" box.

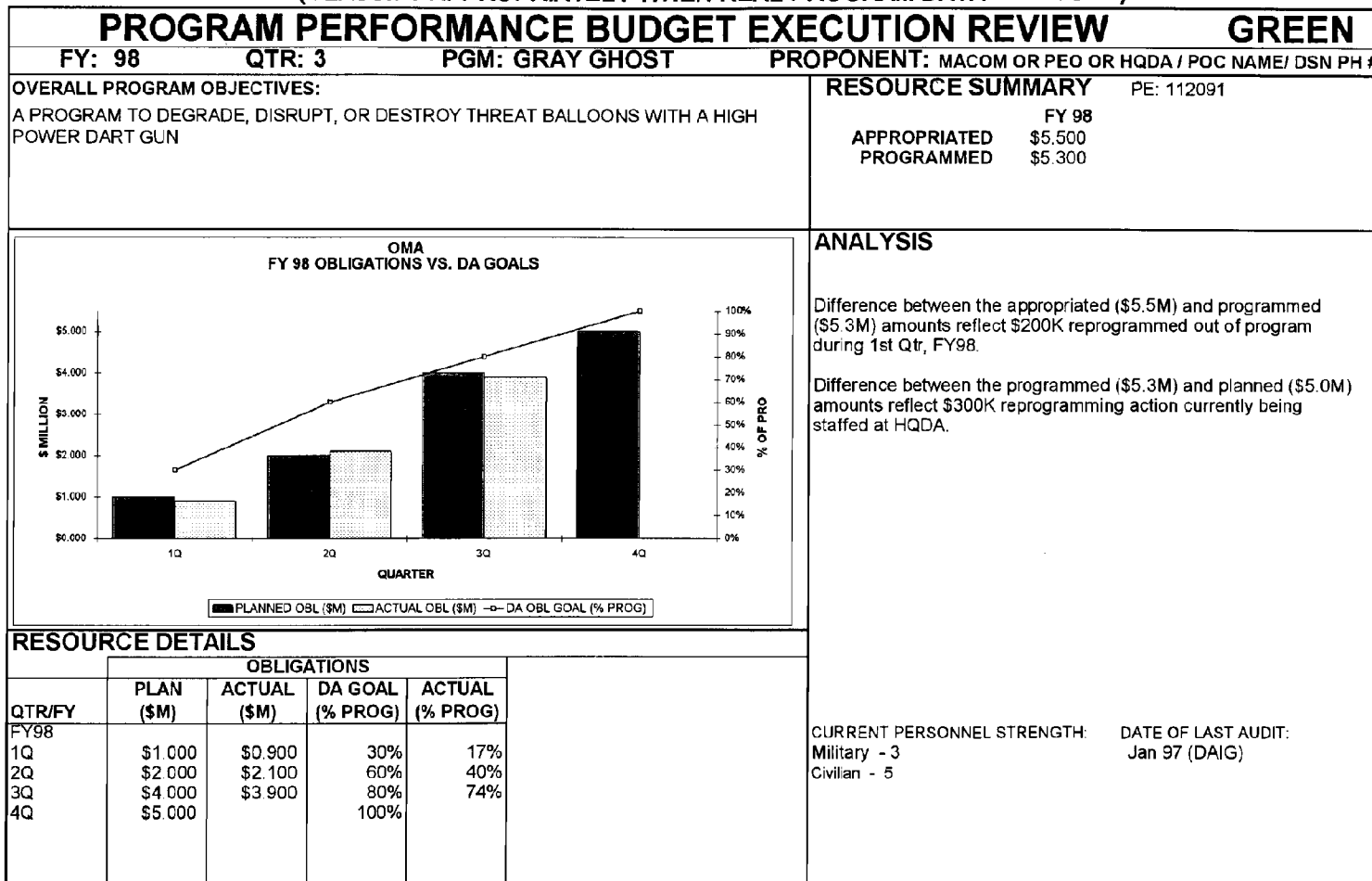
(CLASSIFY APPROPRIATELY WHEN REAL PROGRAM DATA ARE USED)

PROGRAM PERFORMANCE BUDGET EXECUTION REVIEW					RED																														
FY: 98	QTR: 3	PGM: GRAY GHOST	PROPOSER: MACOM OR PEO OR HQDA / POC NAME/ DSN #																																
OVERALL PROGRAM OBJECTIVES: A PROGRAM TO DEGRADE, DISRUPT, OR DESTROY THREAT BALLOONS WITH A HIGH POWER DART GUN			RESOURCE SUMMARY PE: 62040/AD70 <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px; text-align: center;">FY 98</td> <td style="padding: 2px; text-align: center;">FY 97</td> </tr> <tr> <td style="padding: 2px;">APPROPRIATED</td> <td style="padding: 2px; text-align: center;">\$5.500</td> <td style="padding: 2px; text-align: center;">\$5.200</td> </tr> <tr> <td style="padding: 2px;">PROGRAMMED</td> <td style="padding: 2px; text-align: center;">\$5.300</td> <td style="padding: 2px; text-align: center;">\$5.100</td> </tr> </table>				FY 98	FY 97	APPROPRIATED	\$5.500	\$5.200	PROGRAMMED	\$5.300	\$5.100																					
	FY 98	FY 97																																	
APPROPRIATED	\$5.500	\$5.200																																	
PROGRAMMED	\$5.300	\$5.100																																	
<div style="text-align: center;"> RDTE FY 98 OBLIGATIONS/DISBURSEMENTS VS. DA GOALS </div> <table border="1" style="margin-top: 10px; width: 100%; border-collapse: collapse; font-size: small;"> <caption>Chart Data Summary</caption> <thead> <tr> <th>Quarter</th> <th>Planned Obl (\$M)</th> <th>Actual Obl (\$M)</th> <th>Actual Disb (\$M)</th> <th>DA Obl Goal (% Prog)</th> <th>DA Disb Goal (% Prog)</th> </tr> </thead> <tbody> <tr> <td>1Q</td> <td>1.000</td> <td>0.900</td> <td>0.300</td> <td>19%</td> <td>6%</td> </tr> <tr> <td>2Q</td> <td>2.000</td> <td>2.100</td> <td>0.825</td> <td>62%</td> <td>20%</td> </tr> <tr> <td>3Q</td> <td>4.000</td> <td>3.200</td> <td>2.000</td> <td>83%</td> <td>38%</td> </tr> <tr> <td>4Q</td> <td>5.000</td> <td>5.000</td> <td>5.000</td> <td>95%</td> <td>57%</td> </tr> </tbody> </table>			Quarter	Planned Obl (\$M)	Actual Obl (\$M)	Actual Disb (\$M)	DA Obl Goal (% Prog)	DA Disb Goal (% Prog)	1Q	1.000	0.900	0.300	19%	6%	2Q	2.000	2.100	0.825	62%	20%	3Q	4.000	3.200	2.000	83%	38%	4Q	5.000	5.000	5.000	95%	57%	ANALYSIS FY98 Difference between appropriated and programmed amounts reflect \$100K reprogrammed out of program during 1st Qtr to support HOUND DOG, a higher priority program and \$100K HQDA withhold for SBIR. Difference between programmed (\$5.3M) and planned (\$5.0M) amounts reflect \$300K reprogramming action currently being staffed at HQDA. Low obligation rate caused by postponement of test to the 4th quarter and resulting delay in award of contract. We expect contract award in late July which should fully obligate funding. FY97 Difference between appropriated and programmed amounts reflect \$100K HQDA withhold for SBIR. Carry-over (\$100K) from FY97 is being reprogrammed out of GRAY GHOST to support LOST CAUSE, a humanitarian effort. FY97 actual disbursements (59%) are below HQDA goal (87%) because of a delay in the billing cycle between the contractor and finance office. Program manager is working with both the contractor and finance office to resolve this problem. CURRENT PERSONNEL STRENGTH: Military - 1 Civilian - 4 DATE OF LAST AUDIT: Jan-97 (DAIG)		
Quarter	Planned Obl (\$M)	Actual Obl (\$M)	Actual Disb (\$M)	DA Obl Goal (% Prog)	DA Disb Goal (% Prog)																														
1Q	1.000	0.900	0.300	19%	6%																														
2Q	2.000	2.100	0.825	62%	20%																														
3Q	4.000	3.200	2.000	83%	38%																														
4Q	5.000	5.000	5.000	95%	57%																														
RESOURCE DETAILS																																			
	OBLIGATIONS			DISBURSEMENTS																															
QTR/FY	PLAN (\$M)	ACTUAL (\$M)	DA GOAL (% PROG)	ACTUAL (% PROG)	ACTUAL (\$M)	DA GOAL (% PROG)	ACTUAL (% PROG)																												
FY97 ALL	\$5.100	\$5.000	100%	98%	\$3.000	87%	59%																												
FY98																																			
1Q	\$1.000	\$0.900	19%	17%	\$0.300	6%	6%																												
2Q	\$2.000	\$2.100	62%	40%	\$0.825	20%	16%																												
3Q	\$4.000	\$3.200	83%	60%	\$2.000	38%	38%																												
4Q	\$5.000		95%			57%																													

(CLASSIFY APPROPRIATELY WHEN REAL PROGRAM DATA ARE USED)

Figure H-1. RDTE PPBERS chart (example)

(CLASSIFY APPROPRIATELY WHEN REAL PROGRAM DATA ARE USED)



(CLASSIFY APPROPRIATELY WHEN REAL PROGRAM DATA ARE USED)

Figure H-2. OMA PPBERS chart (example)

**Appendix I
Reprogramming Request Format**

The following (fig I-1) is a sample reprogramming request.

(CLASSIFICATION)	
OFFICE SYMBOL	DATE
MEMORANDUM THRU CHIEF, TECHNOLOGY MANAGEMENT OFFICE THE JUDGE ADVOCATE GENERAL GENERAL COUNSEL ARSTAF PRINCIPLE	
FOR UNDER SECRETARY OF THE ARMY	
SUBJECT: Special Access Program (SAP) Reprogramming Request (CLASSIFICATION)--ACTION MEMORANDUM	
1. Purpose: To obtain Under Secretary of the Army (USA) approval of "SAP, NICKNAME" request for reprogramming at Encl 1.	
2. Discussion:	
a. Attached at Encl 1 is a request from XXXXX to reprogram FY 9x, (OMA, OPA, RDTE, etc.) funds in the amount of \$XXXX from (name of program) to (name of program). Enclosure 1 also provides a justification for the reprogramming and a current funding profile.	
b. This is a below threshold reprogramming that does not require congressional notification.	
3. Recommendation: That the USA approve the reprogramming request.	
Encl as	ARSTAF Proponent Signature Block
XXXXXXXXXXXXXXXXXXXX	
COORDINATION:	
MACOM Resource Manager	_____ Date _____
ARSTAF/PEO Principal	_____ Date _____
DAMO-FD	_____ Date _____
Approp Director	_____ Date _____
ASA(FM)	_____ Date _____
PAED	_____ Date _____
Under Secretary of the Army Decision	<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved DATE _____
(CLASSIFICATION)	

Figure I-1. Sample reprogramming request

Appendix J
Fix-It Status Sheets

Figure J-1 is an example of a Fix-It Status Sheet.

3189	CATEGORY: Financial Management	LEAD: AMC
	PROGRAM: WHITE CLOUD	
	INSPECTION DATE: May 1994	
	SUBJECT: Low Disbursing Rate	
FINDING: The Army WHITE CLOUD Program has consistently maintained a low Disbursing rate falling short of DA Goals by more than 20%.		
RECOMMENDATION: The Program Manager institute a joint review program with the local Finance Office to determine why disbursing rates are not meeting DA Goals.		
STATUS: 13-14 JUL 1994 UNRESOLVED. Narrative Follows.		
STATUS: 12 OCT 1994 UNRESOLVED. Narrative Follows.		
STATUS: 25 JAN 1995 RESOLVED. Narrative Follows. (Closed Working Fix-it 25 Jan 95.)		

NOTES:		
1.	DAIG will assign finding numbers for their findings; TMO will assign numbers for all other findings.	
2.	The Category will be one of the following choices:	
	a.	Program Management
	b.	Property
	c.	Procurement
	d.	Financial Management
	e.	Security
3.	The date of inspection will be the date of the finding (Month/Year).	
4.	The program name is the current nickname in the event of a name change.	

Figure J-1. Sample Fix-It Status Sheet

Appendix K Format for Information Systems Requirements Package

Use the following format when preparing the Information Systems Requirements Package.

1. General

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

2. Scope of Requirement

3. Urgency

- a. Priority need.
- b. Implementation
- c. Date initial operational capability required.
- d. Date final operational capability required.
- e. Impact if service is not provided.

4. Existing Capability

- a. Common user or dedicated information systems capabilities that presently exist or are available.
- b. How capabilities satisfy any portion of IM requirement in their present or modified state.

5. Security Management

- a. Name of security manager.
- b. Unique security requirements.
- c. Appropriate extracts of the program security plan and classification guide.

6. Funding

Type and source of funds to be used for information systems acquisitions.

7. Procurement

Concept for procurement of information systems.

8. Accountability

Describe the concept for property accountability.

9. Technical Requirements

- a. Type of service required.
- b. Type of traffic to be transported.
- c. Interfaces with existing systems, networks or equipment.
- d. Different capabilities required for different phases of the project.
- e. For COMSEC material/equipment, the supporting COMSEC account number(s), name, address, and telephone number(s) of COMSEC custodian(s).
- f. Resource requirements, engineering, fabrication, installation, operations, training, and maintenance necessary to provide service.

Appendix L Format for Information Management Support Plan

Use the Format for Information Management Support Plan (IMSP) to identify the finite IM requirements of a SAP or sensitive activity. The clarity provided in the IMSP merely amplifies the IM requirements generally referred to in the IMRP (see para 8–4). Prepare the plan in the following format.

1. Executive Summary

Describe project scope, background, overview, recommendations, and conclusions.

2. Purpose

Summarize the proponent's requirements.

3. System Description

Describe, in detail, the general system, network, facilities, equipment, services, and support required to satisfy the proponent's requirements.

4. Technical Analysis and Cost Estimates (TACE)

Provide a technical analysis of future IS systems, including a cost estimate covering five fiscal years and an annual estimate for sustaining O&M over the life-cycle of the project.

5. Management, Command, and Control

Indicate the management, command, and control structure of the project participants. Include personnel and organizations both internal and external to the command structure.

6. Financial Management

Identify the financial management structure, procedures, and methodologies to be applied against the project. It is the SAP manager's responsibility to budget for information management support.

7. Resource Management

- a. *Manpower.* Determine the realistic and prudent manpower requirements to support the IS initiative throughout its life-cycle.
- b. *Material.* Indicate the material required to support the project and identify issues and details relevant to the acquisition and implementation of the project.
- c. *Funds.* Indicate the methodologies to be applied against the project.

8. Security

- a. Billets and Access.
- b. Describe, in detail, the information systems security concept.

9. Operations Security

Describe the Security Plan for the project's Information Systems.

10. Architecture and Configuration Management

Identify systems, networks, and equipment fielded to ensure compatibility with the Army information architecture.

- a. Establish an information systems Configuration Control Board and procedures for controlling changes, enhancements, and system upgrades.
- b. Identify a Configuration Control Manager for the information systems project.

11. Project Implementation

Describe how the information systems project will be implemented over initial, expanded, and final phases.

12. Operations and Maintenance (O&M)

Identify roles, relationships, and responsibilities concerning the operation and maintenance of the information systems, networks, and equipment.

13. Memoranda of Understanding (MOU)/Interservice Support Agreements (ISSA)

Indicate any MOU/ISSA that would be required to effectively execute the project.

14. Integrated Logistic Support

Describe the integrated logistic support concept for the information systems and technical activities in support of the equipment and material during its life cycle.

15. Property Accountability

Provide details on how accountability of project equipment and material is maintained.

16. Approvals and Coordination

After the proponent has developed the IMSP, the IMSP is submitted via SAP channels through the MACOM or PEO, through TMO (DACS-DMP), to DISC4 (SAIS-PAJ-O) for approval. Following approval, DISC4 may task USACECOM-TAO (AMSEL-TA) to provide information system support.

Glossary

Section I Abbreviations

AAA

Army Audit Agency; access approval authority

ACA

access control authority

AMC

U.S. Army Materiel Command

ASA(FM)

Assistant Secretary of the Army for Financial Management

ASA(RDA)

Assistant Secretary of the Army for Research, Development, and Acquisition

CCF

U.S. Army Central Personnel Security Clearance Facility

CG

commanding general

CI

counterintelligence

CLL

Chief of Legislative Liaison

COE

Chief of Engineers

CPA

Chief of Public Affairs

DA

Department of the Army

DAA

designated accrediting authority

DAS

Director of the Army Staff

DASR

Department of the Army special roster

DCAA

Defense Contract Audit Agency

DCAS

Defense Contract Administration Services

DCI

Director of Central Intelligence

DCS

Defense Courier Service

DCSINT

Deputy Chief of Staff for Intelligence

DCSOPS

Deputy Chief of Staff for Operations and Plans

DCSPER

Deputy Chief of Staff for Personnel

DISC4

Director of Information Systems for Command, Control, Communication, and Computers

DISCO

Defense Industrial Security Clearance Office

DLA

Defense Logistics Agency

DOD

Department of Defense

DODIG

Department of Defense Inspector General

DSS

Defense Security Service

EEFI

essential elements of friendly information

FAR

Federal Acquisition Regulation

FIS

Foreign Intelligence Service

FOIA

Freedom of Information Act

HCA

head of contracting activity

HQDA

Headquarters, Department of the Army

ICF

intelligence contingency funds

IMSP

Information Management Support Plan

IRAC

internal review and audit compliance

IR&D

independent research and development

ISRP

Information Systems Support Package

ISSA

interservice support agreement

MACOM

major Army command

MOA

memorandum of agreement

MOU

memorandum of understanding

NACI

national agency check with written inquiries

NISPOM

National Industrial Security Program Operating Manual

OCA

original classification authority

OCSA

Office of the Chief of Staff, Army

ODUSD(P)(PS)

Office of the Deputy to the Under Secretary of Defense for Policy, Policy Support

OFCO

offensive counterintelligence operations

OPM

Office of Personal Management

OPSEC

operations security

OSD

Office of the Secretary of Defense

PAED

Program Analysis and Evaluation Directorate, OCSA

PEO

program executive officer

POC

point of contact

PPBERS

Program Performance and Budget Execution Review System

PSAP

Prospective Special Access Program

R&D

research and development

RDT&E

research, development, test, and evaluation

SA

Secretary of the Army

SAP

special access program

SAPOC

Special Access Program Oversight Committee

SAR

special access required

SSBI

single scope background investigation

SCI

sensitive compartmented information

SCIF
sensitive compartmented information facility

SES
senior executive service

SFAO
Special Finance and Accounting Office

SMF
special mission funds

SRIA
Sensitive Records and Information Agency

TIARA
tactical intelligence and related activities

TIG
The Inspector General

TJAG
The Judge Advocate General

TMO
Technology Management Office

TRADOC
U.S. Army Training and Doctrine Command

TSCM
technical surveillance countermeasures

USA
Under Secretary of the Army

USACIDC
U.S. Army Criminal Investigation Command

USAFMSA
U.S. Army Force Management Support Agency

USAINSCOM
U.S. Army Intelligence and Security Command

USAISC
U.S. Army Information Systems Command

USASMDC
U.S. Army Space and Missile Defense Command

VCSA
Vice Chief of Staff, Army

Section II **Terms**

Classified National Security Information
Information classified in accordance with Executive Order 12958 that could reasonably be expected to cause damage to national security if disclosed outside official government channels.

Collateral information
Classified information which can be adequately safeguarded using the ordinary security measures outlined in AR 380-5.

Security compromise
The disclosure of classified information to persons not authorized access thereto.

Security infraction
Any other incident that is not in the best interest of security that does not involve the loss, compromise, or suspected compromise of classified information.

Security violation
Any incident that involves the loss, compromise, or suspected compromise of classified information.

Sensitive Compartmented Information (SCI)
Classified information that can only be protected with security measures authorized by AR 380-28, Army Special Security Officer and Office System.

Extraordinary security measures
A security measure necessary to adequately protect particularly sensitive information but which imposes a substantial impediment to normal staff management and oversight. Extraordinary security measures are—

Program access non-disclosure agreements (read-on statements).

Specific officials authorized to determine “need to know” (ACA/AAA)

Nicknames/Codewords for program identification.

Special Access Required markings.

Program billet structure.

Access roster.

Use of cover.

Use of special mission funds or procedures.

Use of a SAP facility/vault.

Use of a dedicated SAP security manager.

Any other security measure above those required to protect collateral information in accordance with AR 380-5.

Index

This index is organized alphabetically by topic and by subtopic within a topic. Topics and subtopics are identified by paragraph number.

Army Audit Agency, 4-2

Access

Approval Authority, 4-5, 5-3, 5-4, 5-8, 6-1, 6-3, 6-4, 6-5, 6-6, 6-7

Control, 6-1, 6-5

Control Authority, 5-8, 6-1, 6-2, 6-5

Accountability, 2-3

Acquisition SAP, 2-3, 9-3

Army Audit Agency, 4-2

Auditor General, The, 2-9

Audits, 2-9, 4-2

Baseline

Billet Structure, 4-4, 6-1, 6-3

Billets, 5-4

Billet

Structure, 2-31, 3-3, 4-4, 5-1, 6-1, 6-3, 6-4

Structure Management System (BSMS), 2-31, 6-8

Carve-out, 1-4, 2-1, 2-21, 5-1, 7-5, 7-8

Category, 3-3, 4-1

I, 3-3, 5-2, 5-4, 5-5, 6-1, 6-2, 6-3

II, 3-3, 5-2, 5-4

III, 3-3, 5-4

N, 3-3

Chief

of Engineers (COE), 2-17

of Legislative Liaison (CLL), 2-19

of Staff, Army (CSA), The, 2-11, 2-18, 5-7

CI assessment, 4-1

Classification Guide, 2-14, 5-8, 6-2, 6-6, 7-8

Compromise, 1-4, 3-3, 4-2, 4-3, 5-7 through 5-9, 7-7

Cover, 4-2, 5-1, 5-3, 9-5

DD Form 254, 5-3, 5-8, 7-5, 7-6, 7-8

Debriefing, 6-4, 6-6, 6-7

Defense

Contract Audit Agency (DCAA), 4-2, 7-6

Contract Management Command, 4-2, 7-6

Contractor, 7-1, 7-3

Security Service, 2-30, 2-32, 4-2, 6-2, 7-4, 7-5, 7-7, 7-8

Department of the Army Staff (ARSTAF), 2-28

Deputy Chief of Staff for Intelligence (DCSINT), 2-14

Director,

Information, Systems for Command,

Control, Communications, and Computers, 2-6, 4-1, 4-2, 5-3, 8-1, 8-3, 8-6

Program Analysis and Evaluation

Directorate (PAED), 2-20

Deputy Chief of Staff for Logistics

(DCSLOG), 2-3, 2-14, 2-16, 4-1, 4-2

Deputy Chief of Staff for Operations and Plans (DCSOPS), 2-13, 2-15, 3-2, 4-1, 4-2, 4-4, 5-6, 9-3

Deputy Chief of Staff for Personnel

(DCSPER), 2-13, 4-1, 4-2

Disestablishment, 2-1, 2-21, 2-26, 4-2, 4-3, 6-4, 6-5, 8-7, 9-4

Disestablishment Plan, 8-7

Dissemination, 5-1, 5-3

Establishment, 2-1, 2-30, 4-1, 4-2, 5-5, 5-7

Exceptions, 7-4

External audits, 4-2

Extraordinary security measures, 1-4, 3-1, 4-3, 5-1

Facility

Risk assessments, 5-5

Security Risk Assessment, Fig 5-1

Fix-It, 2-12, 2-21, 4-2, 4-3

Freedom of Information Act, 5-3

Forces Command (CG, FORSCOM), 2-24

Foreign technology threat assessment, 4-1

General Counsel, The, 2-7, 4-4, 4-1, 4-2, 5-9, 9-3

Information

Management Support Plan (IMSP), 2-6, 8-3, 8-6

Systems, 2-6, 5-5, 5-8, 5-9, 7-8, 8-1, 8-1, 8-5

Systems Requirements Package (ISRP), 2-6, 8-2, 8-3

Inspections, 2-32, 4-2, 5-6, 5-8, 6-2, 7-5, 8-7

Inspector General, 2-8, 4-2, 4-4

Intelligence SAP, 2-14, 5-7, 9-3

Internal audits, 4-2

Inspector General, 2-8, 4-2, 4-4

Judge Advocate General (TJAG), The, 2-18, 4-1, 4-2, 4-4, 9-3

Legislative Liaison, 2-19

Limited dissemination, 5-1

MACOMs, 2-8, 2-14, 2-29, 4-2, 5-6, 5-7, 9-3

MOU, 5-6, 5-7, 6-2

Multi-discipline counterintelligence

(MDCI) assessment, 4-1

NISPOM, 5-3, 5-4, 7-2

Non-Army SAP, 2-8, 3-3

Operations and Support SAP, 2-15, 9-3

Patent, 5-3

Personnel Security, 2-4, 5-1, 5-4, 5-5, 5-8, 7-3

Physical security, 5-1, 5-2, 5-5, 5-8, 7-4

Polygraph, 2-14, 2-26, 5-4, 7-3

PPBERS, 2-2, 2-12, 2-21, 4-2

Procurement Management Reviews

(PMRs), 4-2

Program

Executive Officers, 2-29

Performance and Budget Execution Review System, Intro (CCA)

Proponent, 1-4, 2-14, 2-15, 2-29, 3-2, 4-1, 4-2, 4-3, 4-4, 5-5, 5-6, 5-7, 5-8, 5-9, 6-1, 6-2, 6-3, 7-5, 7-6, 9-2, 9-3, 9-5

Prospective Special Access Program

(PSAP), 1-4, 3-1

Reprogramming, 2-2, 2-20, 4-1, 9-3

Request for Access, 6-5

Revalidation, 2-14, 4-3, 6-3

SAP

Approval, 4-1, 5-8, 6-3

Matrix, 4-4

SAP reports, 9-5

SAPOC, 2-12, 2-14, 2-21, 3-3, 4-1, 4-2, 4-3, 5-5, 5-6, 6-1, 6-2, 6-3, 7-2, 7-5

Secretary of the Army (SA), The, 2-1, 2-3, 2-7, 2-21, 4-1, 4-2, 4-3, 4-4, 5-3, 5-4, 5-7

Secure

Communications, 4-1, 5-5

Environment contracting, 2-3, 2-8, 4-2, 7-6

Classification Guide, 2-14, 5-8, 6-2

Management, 3-3, 8-7

Manager, 4-2, 5-3, 5-8, 6-1, 6-2, 6-5, 7-7, 8-5

Personnel, 8-4

Plan, 5-8

Procedures Guide, 5-3, 5-8, 6-1, 6-2, 7-4

Special Access Program Oversight

Committee (SAPOC), 2-12, 4-2

SRIA, 2-21, 2-30, 2-31, 5-3, 6-3, 6-4, 6-8, 8-7,

Technology Management Office (TMO),

1-4, 2-6, 2-8, 2-9, 2-12, 2-14, 2-19, 2-20, 2-21, 2-25, 2-27, 2-29, 2-30, 3-1, 4-1, 4-2, 4-3, 4-4, 5-3, 5-4, 5-5, 5-6, 5-7, 5-8, 5-9, 6-1, 6-2, 6-3, 6-4, 7-5, 7-6, 7-8, 8-1, 8-3, 8-6, 9-1, 9-2, 9-3, 9-5

TEMPEST, 2-26, 5-3, 5-5

Termination, 1-4, 4-3, 5-4, 6-1, 6-7

TSCM, 2-26, 5-2, 5-5, 5-8

Two person integrity, 5-2

Under Secretary of the Army, The, 2-2, 4-2, 4-4, 5-7, 9-3

U.S. Army Criminal Investigation

Command (USACIDC), 4-2

U.S. Army Force Management Support

Agency (USAFMSA), 2-15, 2-29, 4-2

U.S. Army Intelligence and Security

Command (USAINSCOM), 2-26

U.S. Army Materiel Command (AMC), 2-23, 4-2

Vice Chief of Staff of the Army (VCSA),

2-8, 2-12, 3-3, 4-1, 4-2, 4-4, 5-3, 5-7, 7-8, 9-3

Working SAPOC, 2-14, 4-1, 4-2, 5-5, 5-6

MANAGEMENT CONTROL EVALUATION CERTIFICATION STATEMENT

For use of this form, see AR 11-2; the proponent agency is ASA(FM).

1. REGULATION NUMBER

2. DATE OF REGULATION

3. ASSESSABLE UNIT

4. FUNCTION

5. METHOD OF EVALUATION *(Check one)*

a. CHECKLIST

b. ALTERNATIVE METHOD *(Indicate method)*

APPENDIX *(Enter appropriate letter)*

6. EVALUATION CONDUCTED BY

a. NAME *(Last, First, MI)*

b. DATE OF EVALUATION

7. REMARKS *(Continue on reverse or use additional sheets of plain paper)*

8. CERTIFICATION

I certify that the key management controls in this function have been evaluated in accordance with provisions of AR 11-2, Army Management Control Process. I also certify that corrective action has been initiated to resolve any deficiencies detected. These deficiencies and corrective actions *(if any)* are described below or in attached documentation. This certification statement and any supporting documentation will be retained on file subject to audit/inspection until superseded by a subsequent management control evaluation.

a. ASSESSABLE UNIT MANAGER

(1) Typed Name and Title

b. DATE CERTIFIED

(2) Signature

SPECIAL ACCESS PROGRAM INITIAL SECURITY BRIEFING

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

DATA REQUIRED BY THE PRIVACY ACT OF 1974

Authority	Title 10, USC 3013.
Principal Purpose	Obtain accountability data for access to SAP information.
Routine Uses	None.
Disclosure	Disclosure of the information is voluntary. However, failure to provide the data may delay or preclude access to this program's information.

I, the undersigned, certify that I have received a security briefing concerning the below listed special access program(s).

I am aware that willful 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 could be detrimental to the interests of national security.

Program(s) _____
(Nickname or Codeword)

I understand that specific classification guidance exists for this program 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 willful 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 defense information or knowledge concerning the above special access program(s) except in the performance of my official duties or as authorized by 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 initial and random counterintelligence-scope polygraph examinations and urinalyses, if requested by proper authority, to determine my suitability for receiving and/or maintaining access to program information.

WITNESS:

(Signature)

(Date)

(Signature)

(Date)

(Printed Name)

(Printed Name)

(SSN)

(Position/Organization)

(Organization/Telephone Number/Position)

SPECIAL ACCESS PROGRAM SECURITY TERMINATION BRIEFING

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

DATA REQUIRED BY THE PRIVACY ACT OF 1974

Authority	Title 10, USC 3013.
Principal Purpose	Obtain accountability information for termination of access to this SAP.
Routine Uses	To brief individual that SAP access has terminated.
Disclosure	Disclosure is voluntary.

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 by a foreign nation.
- c. I have surrendered and no longer have in my possession, custody, or control any information or material concerning the below program.
- d. I shall not communicate or transmit any classified defense information concerning the below program, orally or in writing, to any unauthorized person or agency.
- e. I shall report to my Program Security (OPSEC) Manager, a local Federal Bureau of Investigation office, or an authorized official 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 on: _____
(Nickname or Codeword)

WITNESS:

(Signature)

(Signature)

(Date)

(Date)

(Printed Name)

(Printed Name)

(Position/Organization)

(Organization/Telephone Number/Position)

(SSN)

SPECIAL ACCESS PROGRAM REQUEST FOR ACCESS
For use of this form, see AR 380-381; the proponent agency is OCSA

1. DATE

DATA REQUIRED BY THE PRIVACY ACT OF 1974

Authority	Title 10, USC 3013.
Principal Purpose	Obtain accountability data for access to SAP information.
Routine Uses	Obtain security clearance status information and identify SAP for proposed access.
Disclosure	Disclosure of the information is voluntary. However, failure to provide the data may delay or preclude access to this program's information.

2. NAME (Last, First, MI)

3. GRADE/ RANK

4. SSN

5. DATE OF BIRTH

6. PLACE OF BIRTH/CITIZENSHIP

7a. SECURITY CLEARANCE

b. DATE CLEARANCE GRANTED

8. MACOM/ACTIVITY/ORGANIZATION/OFFICE

c. GRANTING AGENCY

d. TYPE OF INVESTIGATION

9. MAILING ADDRESS

e. DATE INVESTIGATION COMPLETED

f. DATE PR SUBMITTED TO CCF OR
COMPARABLE AGENCY (Required if
investigation date is more than five years old.)

10. INDIVIDUAL'S POSITION

11. PROGRAM(S) AND ACCESS LEVEL REQUIRED

12. DUTY PHONE

13. PROJECTED PCS/RETIREMENT

14. BILLET NUMBER

15. JUSTIFICATION/COMMENTS

Note: For access requests that do not identify a validated billet, the ACA must authorize approval (except when access has been authorized by the VCSA, the CSA, the Under Secretary of the Army or the Secretary of the Army.

16. SECURITY CLEARANCE VERIFICATION

a. DUTY PHONE

b. NAME AND TITLE

c. DATE

d. SIGNATURE

17. COMMANDER OR DIRECTOR OF ORGANIZATION

a. NAME AND TITLE

b. DATE

c. SIGNATURE

18. ACCESS APPROVAL AUTHORITY

a. NAME AND TITLE

b. DATE

c. SIGNATURE

INADVERTENT DISCLOSURE OATH

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

DATA REQUIRED BY THE PRIVACY ACT OF 1974

Authority	Title 10, USC 3013.
Principal Purpose	Obtain accountability information for inadvertant access to SAP information and provide safeguard warning.
Routine Uses	Make record of cases when inadvertant access to SAP data has taken place.
Disclosure	Disclosure of information is voluntary. Failure to provide information may impeded complete and proper identification.

I certify that I shall never divulge the classified information inadvertently exposed to me and I will not reveal to any person my knowledge of the existence of such information. I understand that transmission or revelation of this information in any manner to an unauthorized person may be punishable under U.S. Code, Title 18, Sections 793 and 794 and/or appropriate articles of the Uniform Code of Military Justice. I further certify that I shall never attempt to gain unauthorized access to such information. My signature below does not constitute an indoctrination into the program or clearance for the program, but acknowledges my understanding of the above.

(Signature)

(Date)

WITNESSING OFFICIAL:

(Signature)

(Date)

(Printed Name)

(Printed Name)

(SSN)

(Position/Organization)

(Organization/Telephone Number/Position)

UNCLASSIFIED

PIN 053596-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN: 053596-000
DATE: 09-22-98
TIME: 08:34:47
PAGES SET: 54

DATA FILE: a380381.fil
DOCUMENT: AR 380-381
DOC STATUS: REVISION