

Security

Special Access Programs (SAPs) and Sensitive Activities

Headquarters
Department of the Army
Washington, DC
21 April 2004

UNCLASSIFIED

SUMMARY of CHANGE

AR 380-381

Special Access Programs (SAPs) and Sensitive Activities

This regulation, dated 21 April 2004--

- o Amends the title of the regulation to reflect more accurately the intent and content.
- o Realigns the regulation to match the requirements of Department of Defense Directive 5220.22-M.
- o Makes administrative changes throughout.
- o Clarifies misconceptions about Army-specific special access programs access levels and SAP categories.
- o Rescinds DA Forms 5399-R, 5401-R, and 5749-R.
- o Formalizes the existing responsibilities of the Technology Management Office to include sensitive activities, not just special access programs (chap 1).
- o Clarifies required coordination before an Army special access program can provide resources to, or receive resources from, another Department of Defense or Federal agency special access program or sensitive activity (chap 2).
- o Standardizes annual reporting requirements (chap 4).
- o Adds detail on special access program disestablishment (chap 4).
- o Adds detail on automation support to special access programs by Headquarters, Department of the Army and the relationship between the supported and supporting offices (chaps 4 and 8).
- o Adds detail on physical security requirements for special access program facilities (chap 4).
- o Adds reporting requirements for security incidents related to special access programs (chap 5).
- o Adds baseline approval authorities (chap 6).
- o Clarifies the process to review and submit special access program resourcing documents (chap 9).
- o Adds information on international special access programs, to provide guidance on the unique issues involving special access programs with allies (chap 10).

Effective 21 May 2004

Security

Special Access Programs (SAPs) and Sensitive Activities

By order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation sets forth oversight guidance for Army sensitive activities or implementing instructions and procedures for establishing, maintaining, supporting, and disestablishing special access programs and participation in other component programs that restrict personnel access. This regulation implements applicable parts of Department of Defense Directive 5205.7.

Applicability. This regulation applies to units and activities of the Active Army, the 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 special access program.

Proponent and exception authority. The proponent of this regulation is the Chief of Staff, Army. The Chief of Staff, Army has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The Chief of Staff, Army may delegate this approval authority, in writing, to a division chief within the proponent agency or a direct reporting unit or field operating agency of the proponent agency in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

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 Chief of Staff, Army (DACS-ZDV-TMO).

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

Committee Continuance Approval. The Department of the Army 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, which were established by AR 380–381, 28 January 1986. The DA Committee Management Officer will review biennially the Special Access Program Oversight Committee, the Fix-It Committee, and the SAP Program Performance and Budget Execution Review System Committee for continuance, as required by AR 15–1.

Distribution. This publication is available in electronic media only and is intended for command levels D and E for the Active Army, the Army National Guard of the United States, and the 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 and alternative compensatory control measures • 1–4, page 1

Chapter 2

Responsibilities, page 2

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

*This regulation supersedes AR 380–381, dated 12 October 1998, and rescinds DA Forms 5399–R, 5401–R, and 5749–R.

Contents—Continued

The Under Secretary of the Army • 2-2, *page 2*
The Assistant Secretary of the Army (Acquisition, Logistics and Technology) • 2-3, *page 2*
The Assistant Secretary of the Army (Manpower and Reserve Affairs) • 2-4, *page 2*
The Assistant Secretary of the Army (Financial Management and Comptroller) • 2-5, *page 2*
The General Counsel • 2-6, *page 3*
The Department of Army Inspector General • 2-7, *page 3*
The Auditor General • 2-8, *page 3*
Chief of Public Affairs • 2-9, *page 3*
The Chief of Staff, Army • 2-10, *page 3*
The Vice Chief of Staff, Army • 2-11, *page 3*
The Director of the Army Staff • 2-12, *page 3*
The Deputy Chief of Staff, G-1 • 2-13, *page 3*
The Deputy Chief of Staff, G-2 • 2-14, *page 4*
The Deputy Chief of Staff, G-3 • 2-15, *page 4*
The Deputy Chief of Staff, G-4 • 2-16, *page 4*
The Chief Information Officer, G-6 • 2-17, *page 4*
The Deputy Chief of Staff, G-8 • 2-18, *page 5*
Commander, U.S. Army Corps of Engineers • 2-19, *page 5*
The Judge Advocate General • 2-20, *page 5*
Chief of Legislative Liaison • 2-21, *page 5*
Chief, Technology Management Office • 2-22, *page 5*
Commanding General, U.S. Army Training and Doctrine Command • 2-23, *page 6*
Commanding General, U.S. Army Materiel Command • 2-24, *page 7*
Commanding General, U.S. Army Forces Command • 2-25, *page 7*
Commanding General, U.S. Army Space and Missile Defense Command/Army Strategic Command • 2-26, *page 7*
Commanding General, U.S. Army Intelligence and Security Command • 2-27, *page 8*
Commanding General, U.S. Army Criminal Investigation Command • 2-28, *page 8*
Department of the Army Staff • 2-29, *page 8*
Major Army commands and program executive offices • 2-30, *page 8*
SAP program managers/program directors • 2-31, *page 8*
The program security manager • 2-32, *page 9*
The Program Executive Office, Enterprise Information Systems—Technology Applications Office • 2-33, *page 9*

Chapter 3

Procedures for Oversight of Sensitive Activities, *page 10*

Functions of oversight activities • 3-1, *page 10*
Inspections, audits, and reviews • 3-2, *page 10*
Reports • 3-3, *page 10*

Chapter 4

SAP Life Cycle and Design, *page 11*

Definitions • 4-1, *page 11*
SAP categories • 4-2, *page 11*
SAP types • 4-3, *page 11*
Establishment phase • 4-4, *page 11*
Maintenance phase • 4-5, *page 13*
Disestablishment • 4-6, *page 16*
Army participation with other DOD or Federal agency components SAPs • 4-7, *page 17*

Chapter 5

SAP Security, *page 17*

General • 5-1, *page 17*
Physical security • 5-2, *page 18*
Document/information security • 5-3, *page 19*
Personnel security • 5-4, *page 20*

Contents—Continued

Technical security • 5-5, *page 21*
Treaties • 5-6, *page 21*
Technology transfer/foreign disclosure • 5-7, *page 22*
Program security plan • 5-8, *page 22*
Security incidents involving SAP programs • 5-9, *page 23*

Chapter 6

Access Control, *page 24*

Validation of access requirements • 6-1, *page 24*
Subcompartments • 6-2, *page 25*
Personnel access ceiling and billet structure • 6-3, *page 25*
Rosters • 6-4, *page 26*
Request for access • 6-5, *page 26*
Indoctrination • 6-6, *page 27*
Termination of access • 6-7, *page 27*
Army Special Access Tracking System • 6-8, *page 27*

Chapter 7

Industrial Security, *page 27*

Defense contractors • 7-1, *page 27*
National Industrial Security Program and the program security guide • 7-2, *page 27*
Contractor personnel security • 7-3, *page 28*
Physical security • 7-4, *page 28*
Industrial security inspections • 7-5, *page 28*
Contract management • 7-6, *page 29*
Security infractions, violations, and compromises at contractor facilities • 7-7, *page 29*
Contract security requirements • 7-8, *page 29*
Automated information systems • 7-9, *page 30*

Chapter 8

Information Management Area, *page 30*

General • 8-1, *page 30*
Information systems requirements package • 8-2, *page 31*
Information management support plan • 8-3, *page 31*
Accreditation • 8-4, *page 32*
System maintenance • 8-5, *page 32*
Information management support • 8-6, *page 32*
Information assurance • 8-7, *page 32*
Continuity of operations planning and business continuance planning • 8-8, *page 33*
Removal of non-SAR data from systems approved to process SAR data • 8-9, *page 33*
Records management • 8-10, *page 33*

Chapter 9

Funding, *page 34*

SAP funding • 9-1, *page 34*
Establishment phase • 9-2, *page 34*
Maintenance phase • 9-3, *page 35*
Disestablishment • 9-4, *page 35*
Annual SAP reports • 9-5, *page 35*

Chapter 10

International Special Access Programs, *page 36*

Purpose • 10-1, *page 36*
International characteristics • 10-2, *page 36*
International SAP architectures • 10-3, *page 36*

Contents—Continued

- Information review team • 10–4, *page 36*
- Document marking and control procedures • 10–5, *page 37*
- Classified information categories • 10–6, *page 37*
- Accessing procedures • 10–7, *page 37*
- Project reviews, SAPOCs, inspections, and audits • 10–8, *page 37*

Appendixes

- A. References, *page 39*
- B. Reporting of Army Sensitive Activities—Data Call Sheets, *page 44*
- C. Program Performance and Budget Execution Review System Charts, *page 45*
- D. Guidance on Preparing the Standard QUAD Chart Slide, *page 48*
- E. Establishment, *page 50*
- F. Format for Working SAPOC Slides, *page 52*
- G. Fix-It Status Sheet, *page 64*
- H. Disestablishment Concept Plan, *page 65*
- I. Disestablishment Certification Checklist, *page 67*
- J. Format for Automated Information System Incident Checklist, *page 68*
- K. Procedures for Handling Security Incidents, *page 69*
- L. Format for Information Systems Requirements Package, *page 72*
- M. Format for an Information Management Support Plan, *page 73*
- N. Reprogramming Request Format, *page 74*
- O. Management Control Evaluation Checklist, *page 76*

Table List

- Table E–1: SAP establishment timeline, *page 50*
- Table H–3: SAP component disestablishment timeline, *page 65*

Figure List

- Figure C–1: RDT&E PBBERS chart, *page 46*
- Figure C–2: PBBERS chart for procurement fund, *page 47*
- Figure D–1: Sample slide format for Standard QUAD chart slide, *page 49*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37, *page 52*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 53*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 54*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 55*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 56*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 57*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 58*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 59*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 60*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 61*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 62*
- Figure F–1: Formats for Working SAPOC charts, slides 1–37—Continued, *page 63*
- Figure G–1: Sample fix-it status sheet, *page 64*
- Figure N–1: Sample reprogramming request, *page 74*
- Figure N–1: Sample reprogramming request—Continued, *page 75*

Glossary

Chapter 1 Introduction

1–1. Purpose

This regulation establishes implementing instructions and procedures for the establishment, maintenance, support, disestablishment, and oversight of Army special access programs (SAPs), sensitive activities, and Army participation in other Department of Defense (DOD) or Federal agency programs that restrict personnel access.

1–2. References

Required and related publications and prescribed 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 and alternative compensatory control measures

a. See Army Regulation (AR) 380–5 for a detailed discussion on security, excluding sensitive compartmented information (SCI) programs.

b. Alternative compensatory control measures (ACCMs) cannot use the extraordinary security measures reserved for SAPs (that is, access approval authority, signed indoctrination and termination statements, billet structures, and so on). ACCMs may be established only in accordance with Department of Defense Directive (DODD) 5200.1–R and only for intelligence and operations and support, when information requires enforcement of strict need to know but does not rise to the level requiring SAP protection. ACCMs are not authorized to protect acquisition programs. The proponent for an ACCM is the major Army command (MACOM) sponsoring the effort. Requests to establish ACCMs will be forwarded from the proponent through the appropriate Army Staff principal (for example, the Deputy Chief of Staff G–2 (DCS, G–2) or Deputy Chief of Staff, G–3 (DCS, G–3) to the Technology Management Office (TMO). The TMO will provide a working nickname for the ACCM and will forward requests for ACCMs to the Secretary of the Army (SA) for approval. After SA approval, the TMO will register the working nickname as an active nickname. Classification, marking, and reporting requirements are contained in DODD 5200.1–R. All ACCMs will be reported annually to the TMO in the annual SAP and sensitive activity data call (see app B).

c. Proponents of acquisition, intelligence, or operations and support activities who identify particularly sensitive information that is believed to merit 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 DCS, G–2 and the DCS, G–3 report this to the Chief, TMO, while the program executive office (PEO) (Acquisition) and the Army Materiel Command (AMC) or the appropriate MACOM report to the Director, Secretary of the Army, Acquisition, Logistics, and Technology–Systems Special Programs (SAAL–SSP), who coordinates a security review at Headquarters, Department of the Army (HQDA). SAPs are not programs or activities planned and executed with the intent to influence U.S. political processes, public opinion, policies, or media. The establishment of a SAP will be based on a determination that normal security protections are not adequate based on the threat and/or vulnerability or the information to be protected, and that enhanced security protections are required. Examples of potential SAPs include, but are not limited to—

(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 or unique capability 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) Extremely sensitive activities conducted in support of national foreign policy objectives abroad, which are planned and executed so that the role of the U.S. Government is not apparent or acknowledged publicly.

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

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

d. Army SAP program directors (PDs) or program managers (PMs) are strictly prohibited from providing resources to, in support of, or receiving resources from other DOD components or Federal agencies' SAPs or ACCMs until—

(1) HQDA access to the DOD or Federal agency SAP is provided in accordance with paragraph 4–7 of this regulation.

(2) Memorandums of Agreement (MOAs) are reviewed and approved by the TMO for security and oversight equities. MOAs are established between the SAP PD/PM and the DOD or Federal agency SAP or component.

(3) This restriction is not intended to limit the Army SAP PD/PM from providing SAP information to any properly cleared individual with a need to know when Army SAP material is not stored by the other DOD component or Federal agency.

e. HQDA, its MACOMs, and its activities will not establish, disestablish, implement, fund, categorize, create carve-

out status, or change the mission or scope of a SAP without written approval through the SA by the Deputy Secretary of Defense.

Chapter 2 Responsibilities

2-1. The Secretary of the Army

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

- a.* Make recommendations to the Deputy Secretary of Defense concerning the establishment, disestablishment, carve-out status, and changes of mission and scope of Army SAPs.
- b.* Ensure adequate oversight of Army SAPs.

2-2. The Under Secretary of the Army

The Under Secretary of the Army will—

- a.* Represent the Secretary of the Army at Office of the Secretary of Defense (OSD) Special Access Program Oversight Committee (SAPOC) meetings.
- b.* Serve as the approval authority for the SAP Program Performance and Budget Execution Review System (PPBERS).

2-3. The Assistant Secretary of the Army (Acquisition, Logistics and Technology)

The Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) 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.
- b.* Approve acquisition SAP reprogramming actions.
- c.* Ensure a single subordinate commander of a MACOM or PEO is responsible for each acquisition SAP throughout its life cycle.
- d.* Conduct regular reviews of secure environment contracting conducted in support of SAPs.
- e.* Ensure SAP protection and procedures for procurement and fielding of systems, components, and modifications are developed and acquired under SAP provisions.
- f.* Coordinate with the Office of the DCS, G-2 on issues concerning technology transfer.
- g.* Coordinate within Army and other DOD components to eliminate duplication of effort and ensure consistent security classification for similar technologies.
- h.* Coordinate technical review of acquisition prospective special access programs (PSAPs).
- i.* Ensure the occurrence of, or ensure MACOMs and PEOs conduct, an annual programmatic review of all acquisition SAPs. Such reviews will focus on security, cost, scheduling, performance, and transitions.
- j.* Evaluate proposed acquisition strategies and plans for Army SAPs.
- k.* Coordinate with the Office of the Deputy Chief of Staff, G-4 (DCS, G-4) to integrate logistics support and property accountability considerations into acquisition SAP efforts and products.
- l.* Develop staff oversight procedures to ensure regulatory compliance for Army acquisition SAPs and Army participation in other component and Federal agency acquisition SAPs or similar programs that restrict personnel access.

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 Army SAPs and Army supported SAPs.
- b.* Provide guidance concerning the documentation process to ensure that tables of distribution and allowances (TDA) 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 Assistant Secretary of the Army (Financial Management and Comptroller) (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 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 Service (DFAS) to ensure DFAS provides a secure finance and accounting network to process sensitive financial transactions.
- d.* Provide financial quality assurance oversight through the ASA(FM&C) Special Review Office (SRO).
- e.* Coordinate the Army's budget estimate submission for SAPs with the OSD.

2-6. The General Counsel

The General Counsel will—

- a.* Review Army SAPs, PSAPs, ACCMs, and Army participation in other DOD and Federal agency SAPs or programs that restrict personnel access, for legality and propriety.
- b.* Advise the SA on legal and policy issues.
- c.* Conduct policy reviews.

2-7. The Department of Army Inspector General

The Department of the Army Inspector General (DAIG) will—

- a.* Evaluate managerial procedures and practices pertaining to operations, personnel, materiel, financial management, secure environment, contracting, and security of SAPs, sensitive activities, and ACCMs.
- b.* Identify issues, situations, or circumstances that affect SAP and sensitive activity 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 noncriminal investigations as directed by the SA.
- e.* Inspect Army SAPs and sensitive activities and Army participation in DOD or Federal Agency SAPs and sensitive activities.
- f.* Develop and coordinate an annual inspection plan with the TMO, other inspection/audit agencies, MACOMs, and PEOs.

2-8. The Auditor General

The Auditor General will—

- a.* Maintain auditors with appropriate clearance and access to perform audits of SAPs, sensitive activities, and ACCMs.
- b.* Coordinate with the TMO and other inspection/audit agencies when planning and performing audits of SAPs and sensitive activities.
- c.* Conduct audits or reviews of Army SAPs, sensitive activities, and Army participation in DOD or other Federal agency SAPs.
- d.* Maintain effective liaison, through an individual well acquainted with SAP procedures, with the TMO to ensure effective audit coverage of SAPs and sensitive activities.

2-9. Chief of Public Affairs

The Chief of Public Affairs will—

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

2-10. The Chief of Staff, Army

The Chief of Staff, Army (CSA) will—

- a.* Develop, coordinate, review, and conduct oversight of all Army SAPs.
- b.* Provide guidance and direction to Chief, TMO.

2-11. The Vice Chief of Staff, Army

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

- a.* Review SAPs through the DA SAPOC and serve as chairman of the SAPOC.
- b.* Provide guidance and direction to the Chief, TMO.

2-12. The Director of the Army Staff

The Director of the Army Staff will serve as the chairman of the Executive Fix-It Committee.

2-13. The Deputy Chief of Staff, G-1

The Deputy Chief of Staff, G-1 (DCS, G-1) will—

- a.* Provide policy on SAP personnel matters.

- b. Coordinate with the DCS, G-3 to establish procedures ensuring MACOM SAPs properly use allocated personnel spaces to resource the SAPs.
- c. Ensure that the Human Resources Command coordinates designated DA-approved personnel assignment actions for SAPs.

2-14. The Deputy Chief of Staff, G-2

The DCS, G-2 will—

- a. Oversee Army intelligence SAPs and serve as the intelligence SAP Army Staff proponent.
- b. Approve intelligence SAP reprogramming actions.
- c. Establish security, counterintelligence (CI), and intelligence policy for SAPs in coordination with the TMO.
- d. Coordinate necessary CI support for the execution of Army SAPs.
- e. Provide intelligence threat assessments and CI vulnerability assessments for MACOMs and SAP PEOs, and present these to the Working SAPOC for inclusion in the Executive SAPOC as part of the annual revalidation.
- f. Advise the SAPOC on whether a program or activity warrants SAP protection.
- g. Review SAP security plans and guides for accuracy and completeness.
- h. Coordinate intelligence property issues for Army SAPs with the Deputy Chief of Staff, G-4 (DCS, G-4).
- i. Coordinate policy for CI 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 the TMO and Director for Special Programs, Office of the Deputy Under Secretary of Defense (Policy)(Policy Support)(ODUSD(P)(PS)) for release of information and technology identified by SAP proponents for release to foreign governments and international agencies.
- k. Develop staff oversight procedures to ensure regulatory compliance for Army intelligence SAPs and Army participation in other DOD or Federal agency intelligence SAPs or similar programs that restrict personnel access.
- l. Review and coordinate with the TMO SAP establishment/disestablishment actions, security plans, and CI support plans.

2-15. The Deputy Chief of Staff, G-3

The DCS, G-3 will—

- a. Oversee operations and support SAPs and serve as the Army Staff proponent.
- b. Approve operations and support SAP reprogramming actions.
- c. Provide policy guidance and standards for operations security (OPSEC) measures appropriate for Army SAPs.
- d. Develop Army policy and guidance for materiel requirements for SAPs.
- e. Establish and validate Army acquisition priorities for SAPs.
- f. Coordinate and approve manpower requirements, allocate manpower resources, and prepare TDA documents for SAPs.
- g. Conduct manpower and workload validations of SAPs to support HQDA and PEO/PMs.
- h. Task U.S. Army Force Management Support Agency (USAFMSA) to provide necessary support and analysis of SAP manpower requirements on a 2-year cycle.
- i. Develop staff oversight procedures to ensure regulatory compliance for Army operations and support SAPs and Army participation in other DOD or Federal agency operations and support SAPs and similar programs that restrict personnel access.
- j. Provide OPSEC assessments and support.
- k. Responsible for developing SAP apportionment documents for staffing through the joint planning process in coordination with the SAAL-SSP for apportionment to the combatant commander.
- l. Responsible for developing, reviewing, and staffing with Army Staff compartmented plans that require review and approval by the Army executive offices (The Judge Advocate General (TJAG), the Office of General Counsel, the VCSA, the Undersecretary of the Army, the CSA, and the SA).

2-16. The Deputy Chief of Staff, G-4

The DCS, G-4 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. The Chief Information Officer, G-6

The Chief Information Officer, G-6 (CIO/G-6) will—

- a. Serve as the primary approval authority for SAP automated information systems (AIS).
- b. Appoint a senior military or Government representative (lieutenant colonel or GS-14 or above) to serve as the designated accrediting authority (DAA) for SAP AISs.
- c. Develop information systems policy for SAPs.

d. Serve as the single central office for coordination of information systems support for SAPs. The CIO/G-6 will receive all requests for information technology (IT) support, validate the requested support, prioritize the requests, and then task the PEO Enterprise Information Systems—Technology Applications Office (EIS-TAO) or Network Enterprise Technology Command to provide the requested and approved IT support.

e. Review all IT support and acquisitions to ensure they comply with 40 USC 1401.

f. Validate and approve information system support plans and information management support plans (IMSPs) for SAPs.

g. Through PEO EIS-TAO—

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

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

(3) Provide one-stop IT support to include but not limited to the above and IT engineering, acquisition, implementation, fielding, operations and maintenance, and logistics support for all IT that processes SAP and/or sensitive activity information as defined in this regulation.

(4) Oversee SAP IT systems to ensure they are properly configured to protect SAP and sensitive data. This will be accomplished through periodic inspections of SAP IT systems and assisting other inspection agencies with developing inspection criteria and techniques.

h. Coordinate with the proponent for intelligence issues, the DCS, G-2 on SAP IT systems that process SCI.

2-18. The Deputy Chief of Staff, G-8

The Deputy Chief of Staff, G-8 (DCS, G-8) will—

a. Ensure that SAPs compete with other Army programs for resources in the program objective memorandum (POM) development process.

b. Coordinate with the Army Staff and the TMO to develop SAP program funding profiles and provide copies of approved profiles to the TMO.

c. Provide program analyses for reprogramming actions.

d. Coordinate SAP POM requirements during the program review process with OSD.

e. Participate in the Planning Program Budget Execution Review for SAP Programs.

2-19. Commander, U.S. Army Corps of Engineers

The Commander, U.S. Army Corps of Engineers (USACE) will provide secure architectural engineering, construction, real estate, and contracting support to SAPs and sensitive activities as required.

2-20. The Judge Advocate General

The Judge Advocate General (TJAG) will—

a. Review Army SAPs, prospective Army SAPs, ACCMs, and Army participation in other DOD and Federal agency SAPs or programs that restrict personnel access, for legality and propriety.

b. Provide legal and policy advice on SAP matters to the CSA and the Army Staff.

c. In conjunction with Office of the General Counsel (OGC), coordinate legal and policy issues on SAP matters with DOD and Federal agency legal advisors as appropriate.

2-21. Chief of Legislative Liaison

The Chief of Legislative Liaison (CLL) will—

a. Coordinate congressional briefings on Army SAPs.

b. Coordinate access requirements with OSD, through the TMO, for each separate congressional visit.

c. Provide required reports to selected congressional committees on Army SAPs.

d. Assist the TMO in updating clearance information for individuals in Congress accessed to Army SAPs.

e. Assist the TMO in verifying access of individuals in Congress.

2-22. Chief, Technology Management Office

The Chief, TMO, will—

a. Be designated the Chief, Army SAP Central Office.

b. Be the point of contact (POC) for Army sensitive support to DOD and non-DOD agencies.

c. Be an access approval authority for all Army SAPs and, when delegated authority by another component or Federal agency, for other component or Federal agency SAPs or programs that restrict personnel access.

d. Be the approval authority for establishment of PSAPs and establishment/disestablishment of SAP subcompartments.

e. Be the approval authority for billet structures for all Army SAPs and any billets allocated to the Army from another component or Federal agency SAP or programs that restrict personnel access.

f. Be authorized to indoctrinate personnel into all Army SAPs and, when delegated authority by another component or Federal agency, into other component or Federal agency SAPs or programs that restrict personnel access.

g. Be designated an original classification authority for information classified at the TOP SECRET (and below) level.

h. Serve as the single central office for oversight of Army sensitive activities, Army SAPs, and Army support to other component or Federal agency SAPs or programs that restrict personnel access.

i. Serve as the single central office, in coordination with Programs, Analysis, and Evaluation and Army Budget Office, through which all Army resource documents will be coordinated prior to submission to OSD.

j. Review and staff with the Army Executive Office (TJAG, OGC, VCSA, Under Secretary of the Army, CSA, and SA) the DCS, G-3's recommendations for apportionment of SAP capabilities in support of the combatant commanders.

k. Coordinate with DAIG, Army Audit Agency (AAA), SRO, and other Army or Federal agencies to ensure that Army sensitive activities, SAPs, and Army support to other component or Federal agency SAPs or limited access activities are appropriately inspected and audited.

l. Coordinate briefings and approve access for and indoctrinate Secretariat and Army Staff principals, DOD and Army special panels, and other personnel, as the TMO determines appropriate.

m. Review and staff with the Army Executive Office (VCSA, CSA, Under Secretary of the Army, and SA) all SAP and sensitive activity related actions, except for compartmented plans.

n. Coordinate Army agendas, brief or approve Army briefings and briefer, and approve Army attendance for the OSD SAP Senior Review Group and OSD specified approval process.

o. Report annually to the Chief of Staff and SA all Army SAPs, ACCMs, and participation in other component or Federal agency SAPs or programs that restrict personnel access.

p. Coordinate and approve all documents pertaining to the establishment, maintenance, and disestablishment of SAPs. Additionally, coordinate the approval process for ACCMs as defined in paragraph 1-4*b*.

q. Review and approve all Army SAP security classification guides (SCGs) and program security guides (PSGs). The TMO approves the classification guide format and content, not the classification (this is the responsibility of the original classification authority).

r. Approve the establishment/disestablishment of SAP subcompartments when there is no change to the carve-out status, mission, or scope of the parent SAP. In cases where establishment/disestablishment of a subcompartment will change the mission or scope of the parent SAP, the Chief, TMO will submit the action through SA to the Deputy Secretary of Defense for approval.

s. Coordinate Army SAPOC reviews.

t. Coordinate with the DAIG, AAA, field investigative unit (FIU), SRO, and DCS, G-2 quarterly the HQDA Fix-It process and report results to the Director, Army Staff for authentication.

u. Coordinate a quarterly financial review with the Army Acquisition Special Programs Office.

v. Provide regular update reviews to the senior Army leadership and HQDA staff principals.

w. Assist CLL in coordinating congressional SAP access briefings and congressional notifications.

x. Monitor budget and financial actions associated with SAPs.

y. Review Army sensitive activities, SAPs, prospective Army SAPs, ACCMs, and Army participation in other DOD and Federal agency SAPs or programs that restrict personnel access for compliance with applicable law and regulations, oversight, funding, and continued enhanced security measures.

z. Serve as the POC for Army sensitive support to DOD and non-DOD agencies.

aa. Maintain a registry of Army sensitive activities, SAPs, and Army participation in other component or Federal agency SAPs or programs that restrict personnel access.

ab. Maintain the Army baseline billet roster.

ac. Accept, review, process, archive, and destroy Army sensitive records in accordance with DODD O-5205.7, this regulation, and AR 25-400-2. Respond to requests for information. Conduct records review and disposition.

ad. Conduct Army-wide document searches for sensitive information; compile and prepare document indexes and responsive documents for forwarding to requesting agencies; and coordinate declassification reviews.

ae. Establish policy and provide oversight and management for the Army SAP Enterprise Portal (ASEP).

af. Maintain direct contact with all Army SAPs to coordinate oversight issues. MACOMs and PEOs will be kept appropriately informed.

ag. Participate in the review and approval process of cover plans for non-Army SAPs and sensitive activities.

ah. Represent the coordinated Army position at the OSD Special Access Program Coordination Office (SAPCO) senior review group for apportionment of Army SAP capabilities into the Joint Planning System.

2-23. Commanding General, U.S. Army Training and Doctrine Command

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

a. Institute procedures to ensure early identification and protection of combat developments, concepts, and systems with SAP potential.

- b. Identify war-fighting requirements and concepts that may warrant SAP protection.
- c. Identify support requirements for SAP-developed products deployed to the field.
- d. Provide SAP management and oversight to TRADOC installations.
- e. Conduct an annual review of SAPs to ensure technology is aligned with future needs.

2-24. Commanding General, U.S. Army Materiel Command

The CG, AMC, will—

- a. Institute procedures to ensure early identification and protection of potential research and development breakthroughs that may warrant SAP protection. If AMC deems that SAP protection is warranted for a new technology, a PSAP package will be initiated by AMC and forwarded to the TMO using the procedures prescribed in this regulation.
- b. Review all SAPOC, programmatic and security material relative to AMC SAPs, and sensitive activities prior to that material being forwarded to the TMO, SAAL-SSP, and the Director of Technology (ASA(ALT)).
- c. Provide security and oversight for AMC SAPs.
- d. Conduct a thorough security and programmatic review of all AMC SAPs and provide the results to the Director of Technology (ASA(ALT)).
- e. Initiate all reprogramming actions for AMC SAPs and sensitive activities.
- f. Ensure that all AMC SAPs and sensitive activities adhere to the guidance of this regulation.
- g. Conduct technical reviews of technology base SAPs for continuation or redirection. Review and approve prospective SAP programs prior to submission to the DCS, G-2 and the TMO.
- h. Coordinate and conduct regular review of secure environment contracting in support of SAPs.
- i. Coordinate with HQDA and other DOD components to eliminate duplication of effort and ensure consistent security classification for similar technologies.
- j. Coordinate technical reviews by convening the Technical Review Committee (TRC) to assess the technology base SAPs and recommend continuation or redirection of programs based on program standing and prioritization of each SAP. Additionally, the TRC will review and approve PSAPs prior to submitting to the DCS, G-2 and the TMO. AMC organizations that anticipate the review of programs to be reviewed as a SAP are required to contact the AMC DCS, G-2 to coordinate with the Research, Development and Engineering Command to convene the TRC. Upon TRC approval, proponents may submit written justification for PSAP status through the AMC DCS, G-2 to Army Staff principal to the TMO.
- k. Conduct and coordinate an annual programmatic review of all AMC SAPs by convening a war fighter technical council to evaluate the cost, scheduling, performance, and transition of each SAP.
- l. In coordination with HQ TRADOC, conduct an annual review of new SAP initiatives focused on validating Army requirements. This process is to review, prioritize, and recommend new SAP initiatives to the TRADOC Deputy Command General for Development; the Office of the ASA (ALT) through SAAL-TT (Research and Technology); and the DCS, G-8.

2-25. Commanding General, U.S. Army Forces Command

The CG, U.S. Army Forces Command, will institute procedures to ensure early identification and protection of activities, operational concepts, and combat developments requiring SAP status.

2-26. Commanding General, U.S. Army Space and Missile Defense Command/Army Strategic Command

The CG, U.S. Army Space and Missile Defense Command (USASMDC)/Army Strategic Command, will—

- a. Institute procedures to ensure early identification and protection of activities, operational concepts, combat developments, and potential research and development breakthroughs within USASMDC/Army Strategic Command that may warrant SAP protection and will coordinate potential release of special access required (SAR) information through the DCS, G-2 to SAAL-SSP and the TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. The DCS, G-2 will coordinate, as required, with Director for Special Programs, ODUSD(P)(PS), prior to any release.
- b. Oversee command SAPs and SAP activity.
- c. Ensure all command SAPs undergo required security and programmatic reviews and reports the results appropriately.
- d. Ensure proper reporting of all reprogramming actions for command SAPs and sensitivities.
- e. Ensure all command SAPs and sensitive activities adhere to the guidance of this regulation.
- f. Conduct technical reviews of technology base SAPs for continuation or redirection.
- g. Review and approve prospective SAP programs prior to submission to the DCS, G-2 and the TMO.
- h. Ensure compliance with secure environment contracting requirements for SAPs.

i. Coordinate with HQDA and other DOD components to eliminate duplication of effort and ensure consistent security classification for similar/related efforts.

2-27. Commanding General, U.S. Army Intelligence and Security Command

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

- a.* Institute procedures to ensure early identification and protection of sensitive intelligence activities that may warrant SAP protection.
- b.* Provide dedicated CI and security countermeasures support to commanders, PDs/PMs, or heads of DA activities having proponentcy for Army SAPs or Army-supported SAPs.
- c.* Provide the DCS, G-2 with CI assessments of the threat posed to SAPs by foreign intelligence services and technology assessments of foreign research and development efforts related to SAP technologies. Coordinate with the DCS, G-2 to provide this information to organizations and installations supporting SAPs.
- d.* Provide to the DCS, G-2 an annual CI evaluation of Army SAPs and Army-supported SAPs.
- e.* Manage and execute the Army CI polygraph program in support of SAPs.
- f.* Provide technical surveillance countermeasures (TSCM), TEMPEST, AIS security and counter-signals intelligence support to SAPs.
- g.* Review SAP establishment/disestablishment actions, security plans, and CI support plans.
- h.* Conduct carve-out security compliance reviews of contractor facilities when Defense Security Service is restricted from inspection responsibilities.
- i.* Provide an annual report identifying cover plans and contracting support to SAPs.

2-28. Commanding General, U.S. Army Criminal Investigation Command

The CG, U.S. Army Criminal Investigation Command, will—

- a.* Provide dedicated 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 program procedures, with the 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, DODD O-5205.7, DOD Instruction (DODI) 5505.2, and AR 195-2.
- d.* Conduct periodic economic crime threat assessments.
- e.* Conduct crime prevention surveys on SAPs.

2-29. Department of the Army Staff

The Army Staff 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.

2-30. Major Army commands and program executive offices

The MACOMS and PEOs that supervise managers of SAPs will—

- a.* Assist PDs/PMs in managing their programs.
- b.* Establish internal inspection programs for SAPs and sensitive activities.
- c.* Conduct periodic property reviews to validate new requirements and document materiel assets in support of SAPs.
- d.* Coordinate with the Army Staff for SAP intelligence, CI, and force protection 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 the DCS, G-2 to ASA(ALT) and the TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. The DCS, G-2 will coordinate with the Director for Special Programs, ODUSD(P)(PS), prior to any release.
- g.* Coordinate with USAFMSA for manpower support for TDA documentation.

2-31. SAP program managers/program directors

SAP PDs/PMs and PDs/PMs of Army offices that participate in another non-DOD or Federal agency SAP will—

- a.* Appoint a program security manager (PSM) who is a fully qualified Government/military individual who works directly for and is rated or senior rated by the PD/PM.
- b.* Maintain essential SAP information, including establishment, documentation, security plans, access rosters, and security inspection records.
- c.* Plan, prepare, and implement security and OPSEC programs designed to protect critical program information.
- d.* Report annually to the TMO any program participation in other DOD or Federal agency SAPs or programs that

restrict personnel access, when such participation includes providing resources to, in support of, or receiving resources from, another DOD or Federal agency SAP or sensitive activity.

e. Ensure all MOAs are reviewed by the TMO (Intelligence, Operations and Support, and Acquisition) and coordinated with SAAL-SSP (Acquisition) for security and oversight equities established between the SAP PD/PM and any DOD SAPs. The PD/PM will ensure all MOAs between the SAP PD/PM and any non-DOD or Federal agency SAP are reviewed and approved by the TMO (Intelligence, Operations and Support, and Acquisition) and coordinated with SAAL-SSP (Acquisition). This restriction is not intended to limit the Army SAP PD/PM from providing SAP information to any properly cleared individual with a need to know when Army SAP documents or equipment are not stored by the other non-DOD component or Federal agency.

f. Coordinate with the CIO/G-6 all information systems purchases, technical requests, and support.

g. Establish and maintain a viable records management program in accordance with AR 25-400-2.

h. Coordinate with the Defense Security Service (DSS) or USAINSCOM (when DSS is carved out) for industrial facility reviews.

i. Coordinate potential release of SAR information through DCS, G-2 to ASA(ALT) and the TMO prior to initiating or engaging in preliminary discussions with a foreign government or international organization. The DCS, G-2 will coordinate with Director for Special Programs, ODUSD(P)(PS), prior to any release.

j. Submit to the TMO request for approval any contracting agreement in which DSS will be excluded from providing industrial security inspections (carve-out contracts).

2-32. The program security manager

a. The PSM is a fully qualified Government/military individual who works directly for and is rated or senior rated by the PD/PM (see para 4-5j). Each SAP will have a full time PSM. Programs requesting part-time or shared PSMs will submit a fully justified waiver request to the TMO for approval. PSMs—

(1) Advise PDs/PMs on classification, declassification, downgrading and upgrading of SAP information.

(2) Prepare and submit program security plans to their PDs/PMs.

(3) Maintain a personnel access roster on the ASATS database.

(4) Ensure through MACOM/PEO security officers that personnel with access to the program have the appropriate level of personnel security clearance (see para 5-4).

(5) Through the use of the Defense Clearance and Investigation Index or Joint Personnel Adjudication System (or follow-on DOD authorized system), ensure that personnel requesting access to the program have the appropriate type/level of personnel security investigation. Additionally, PSMs must verify that the clearance is based on the correct type of investigation and that the clearance is current (see para 5-4 for additional guidance). PSMs will verify at least yearly that all personnel briefed to their program have a current security clearance. PSMs are not responsible for conducting a yearly check on Army baseline briefed personnel as these personnel are tracked by the TMO. MACOM security officers will assist SAP security managers if, because of technical reasons (for example, AIS failure), the SAP security manager is unable to conduct investigation type/level verification.

(6) Serve as the program point of contact for all security-, CI-, and OPSEC-related issues.

(7) Review SAP contract requirements, prepare and sign the contract security classification specification (DD Form 254)

(8) Review and report suspected and confirmed program compromises and advise their PDs/PMs on required actions (see para 5-9a).

(9) Accredite (in writing) SAPFs for their program.

b. In cases of Government and contractor facilities that maintain SAP material but are not program officers, a full-time security manager will be designated in writing as the SAP security manager. No facility may be accredited or maintain accreditation as a SAPF without a full-time security manager. Waivers to this policy may be approved only by the TMO.

2-33. The Program Executive Office, Enterprise Information Systems—Technology Applications Office

The Chief, PEO EIS-TAO, after appropriate tasking by the Deputy Chief of Staff, G-6 (DCS, G-6), will—

a. Provide centralized life-cycle management, engineering, purchasing, fielding, testing, evaluating, accrediting, maintaining, clearing, purging, destroying, and disposal of IT systems and software supporting HQDA approved SAPs, sensitive activities, and other Army agencies processing SAR information.

b. Provide technical advice and assistance in preparing ISRPs, during the PSAP process.

c. Provide technical support and advice in developing and implementing IMSPs for HQDA-approved SAPs, sensitive activities, and other Army agencies processing SAR information.

d. Provide technical support and advice to the CIO/G-6 and the TMO on strategies to securely implement or prohibit technological advances in IT systems within the Army SAP and sensitive activities community.

- e. Provide life-cycle management to include programming, budgeting, POM cycle management, engineering, purchasing, accrediting, fielding, maintaining, disposal, network management and help desk support for the ASEP.
- f. Engineer/design, field, operate, and maintain the Army Special Access Tracking System (ASATS) for all Army SAPs as part of the ASEP.
- g. Develop and fund user training modules for secure operation, proper use, and disposal of ASEP, ASATS, and other IT systems/components.
- h. Provide operational support in identifying, developing, testing, and evaluating emerging technologies (both hardware and software) for interoperability and integration into existing and future IT systems and networks.
- i. Provide technical support and assistance to the CIO/G-6 and the DCS, G-2 (for SCI), in the preparation and approval of the AIS accreditation packages for all Army SAPs, sensitive activities, and other Army agencies processing SAR information in accordance with applicable Army and OSD guidance.
- j. Provide logistics support consisting of property accountability and disposal of IT equipment that processes SAP or sensitive information as defined herein. This support will primarily consist of the equipment connected to the ASEP system that processes SAP data and IT systems that operate in a stand-alone mode.

Chapter 3

Procedures for Oversight of Sensitive Activities

3-1. Functions of oversight activities

- a. The SA will review and approve the list of designated Army sensitive activities.
- b. The SA will biennially publish guidance for the DAIG and AAA specifying specific areas of interest during assessments of sensitive activities.
- c. The TMO is designated the HQDA single central office to coordinate, review, and report oversight of Army sensitive activities and SAPs.

3-2. Inspections, audits, and reviews

- a. The TMO, DAIG, AAA, SRO, and CID-FIU will regularly schedule inspections and audits of Army sensitive activities and Army participation in other DOD SAPs and Federal Agency sensitive activities.
- b. Reports of inspections and audits of sensitive activities will be staffed through the TMO to the Army executive office.
- c. The TMO will co-chair, with the DAIG, AAA, SRO, and CID-FIU as appropriate, a quarterly review, with the inspected activity, of open inspection and audit findings. The Director of the Army Staff will authenticate results of this review.
- d. The Director of the Army Staff will chair an annual executive review with the inspected activities.
- e. For Army SAP programs, or Army participation in other DOD or Federal agency SAPs, the VCSA will chair an annual SAPOC review to validate the continuation of the program as a SAP or Army participation in other DOD or Federal agency SAPs.
- f. For Army SAP programs, the TMO will co-chair with the Director, SAAL-SSP a quarterly PPBERS to review obligations and disbursements (see app C).

3-3. Reports

- a. *Responsibility to report.* All Army (active, reserve, and National Guard when support is provided during Federalized service) units have the responsibility to respond accurately to the annual SAP data call (see app B).
- b. *Process.* The TMO report mentioned in paragraph 4-5 provides the basis to report and register the activity at the TMO. The basis of this report is an annual reconciliation of the official Army TMO registry, against data on SAPs and SAP-like activities collected from across the Army during an annual data call issued by the TMO. The report format for the annual data call (see app B) will at a minimum consist of a detailed program description and quad chart (see app D). The TMO consolidates these SAP reports and submits them to Office of the Principal Deputy Under Secretary of Defense (Acquisition and Technology) (OPDUSD(A&T)/Director, Special Programs), which 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. It also becomes the SA annual certification to the Secretary of Defense that—
 - (1) The Army has reported to OSD and Congress every SAP the Army sponsors.
 - (2) Any Army involvement in DOD-sponsored programs is properly reported and registered at HQDA.
 - (3) The Army has reported to OSD and Congress all ACCMs and other "SAP-like" control measures.
- c. *What is reported.* All Army involvement in acquisition, intelligence, operations and support SAPs; ACCMs; and SAP-like programs (whether they are Army SAPs or Army participation in other DOD and Federal agency SAPs) must be reported to HQDA, the TMO, regardless of type, category, sponsor, executive agent, dollar cost, or level of support.

Army participation is defined as receiving resources from, providing resources to, or supporting other DOD or Federal agency SAPs. Resources are defined as: information (hard copy or electronic requiring storage), technology, equipment, facilities, manpower, or funding (see app B for additional guidance).

d. Sensitive activities. Army organizations will report those activities that meet the definition of a sensitive activity (para 1–3a) annually in November to the TMO.

e. SAPs. Army SAP directors or managers will report annually in November to the TMO other DOD or Federal agency SAPs or programs from which the SAP has received resources or to which the SAP has directly provided resources or supported. This report is not intended to include "information sharing" when Army SAP documents are not stored by the other DOD or Federal agency component. Resources are defined as: information (hard copy or electronic requiring storage), technology, equipment, facilities, manpower, or funding.

f. Security incidents. These will be reported in accordance with guidance in paragraph 5–9 of this regulation.

Chapter 4

SAP Life Cycle and Design

4–1. Definitions

a. SAP. A SAP is a security program established under the provisions of Executive Order (EO) 12958 and approved by the Deputy Secretary of Defense to apply extraordinary security measures to protect extremely sensitive information. SAP status is defined by DODD 5200.1–R.

b. PSAP. A PSAP is an interim security program to apply extraordinary security measures to protect extremely sensitive information pending approval of SAP status by the Deputy Secretary of Defense. The Chief, TMO approves PSAP status for Army programs.

4–2. SAP categories

a. The DOD 5220.22–M Supplement Overprint (also referred to as the NISPOM Supplement Overprint) recognizes three categories of SAPs: acquisition, intelligence, and operations and support.

b. Acquisition SAPs protect sensitive research, development, testing, modification, and evaluation or procurement activities in support of sensitive military and intelligence requirements. The Army Acquisition Executive is the Army proponent for acquisition SAPs.

c. Intelligence SAPs protect the planning and execution of especially sensitive intelligence or CI units or operations, including the collection, analysis, and exploitation of intelligence. Intelligence SAPs also protect especially sensitive programs to procure and exploit foreign materiel. The DCS, G–2 is the Army proponent for intelligence SAPs.

d. Operations and support 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. The DCS, G–3 is the Army proponent for operations and support SAPs.

4–3. SAP types

a. There are two types of SAPs, acknowledged and unacknowledged. An acknowledged SAP may be openly recognized or known, however, specifics within the SAP will be classified. The existence of an unacknowledged SAP, or an unacknowledged portion of an acknowledged SAP will be made known only to those personnel properly authorized to receive the information.

b. Three levels of SAP protection are applied: Waived SAP; unacknowledged SAP; and acknowledged SAP. These levels of protection are further explained in DODD 0–5205.7 and DODI 0–5205.11.

c. During the PSAP process, based on the mission, the program will refer to this regulation and the NISPOM Supplement Overprint.

4–4. 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 the MACOM commander (if applicable) and Army Staff proponent to the TMO using the format shown in appendix E. The TMO reviews the request and staffs it with the appropriate staff directorate(s). If the review is favorable, the TMO notifies the proponent in writing of the PSAP approval. This notification includes PSAP nickname and registration date, critical program elements, PSAP category and protection level, funding guidance, and date to present the PSAP to the SAPOC. The Army Staff 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 the TMO. During that period, the MACOM/PEO proponent, the Army Staff proponent, and the TMO determine whether to recommend SAP status. The SA, through the Army SAPOC, recommends approval to the Deputy Secretary of Defense. If the Deputy Secretary of

Defense 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 obligate funds without written TMO approval. PSAPs will receive only those minimum obligated funds necessary for program security and administration until the Deputy Secretary of Defense 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 the TMO keep knowledgeability rosters so that indoctrination statements can be executed if and when SAP status is approved. If the Chief, TMO has determined that the PSAP will become part of the Army baseline, it is not necessary to add baseline-briefed personnel to the knowledgeability roster.

e. The SAP approval process follows:

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

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

(3) The PSAP program office, MACOM/PEO proponent and the TMO initiate separate knowledgeability rosters to maintain a record of all personnel knowledgeable of the PSAP. The program will consolidate these rosters and include them in the formal PSAP package to the TMO.

(4) The program prepares the necessary supporting documentation (SCG and PSG, first draft) to request creation of a SAP and submits it to the TMO prior to being granted PSAP status (see para 5-8 and app E). The MACOM/PEO assists the PSAP program office in coordinating with the working SAPOC members as indicated below.

(5) The ASA(ALT) evaluates the proposed acquisition strategy and acquisition plan for acquisition SAPs.

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

(7) The ASA(ALT), DCS, G-3, and DCS, G-2 evaluate the availability of funds, manpower, and reprogramming actions for acquisition SAPs, operations and support SAPs, and intelligence SAPs, respectively.

(8) The CIO/G-6 validates information management and secure communications requirements for the PSAP and ensures these requirements are documented in the ISRP. The PSAP requestor must include the ISRP as an appendix to the initial PSAP package. The CIO/G-6 will task TAO to accomplish a site review to ensure compliance with standards for compartmented information and assist the PSAP primary security officer with creating all necessary accreditation documentation. IT systems used by the PSAP will normally consist of secure voice, secure fax, and standalone computer workstation(s) or local area network systems, and connection to ASEP.

(9) The DCS, G-2 ensures USAINSCOM conducts an assessment of the foreign collection threats to the program, and provides a CI assessment of the program's vulnerability to that collection threat. The DCS, G-3 ensures the program conducts force protection and OPSEC assessments, using the intelligence and vulnerability assessments as a base for evaluation.

(10) The DCS, G-1 evaluates the personnel assets required and conducts a personnel affordability and supportability assessment.

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

(12) If applicable, the DCS, G-4 evaluates the proposed SAP materiel development or acquisition plan in light of integrated logistics support.

(13) The DCS, G-8, SAAL-SSP, and ASA(FM&C) evaluate the proposed funding profile required and conduct an affordability assessment.

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

(15) The 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, the 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.

(16) If the prospective SAP deals with special operations/low intensity conflict activities, the SA memorandum must be coordinated with ASD Special Operations/Low Intensity Conflict before submission to the respective OSD-level SAP central office.

(17) The TMO, with the staff proponent office or the PD/PM, briefs the OSD senior review group. The OSD senior review group recommends SAP approval and scheduling for the OSD SAPOC.

(18) The TMO, with the staff proponent office or the PD/PM, briefs the OSD SAPOC. If the OSD SAPOC approves the SAP, the Deputy Secretary of Defense notifies Congress. The PSAP becomes a SAP 30 days after congressional notification unless Congress raises an objection.

4-5. 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 as executed in accordance with the management control evaluation checklist (see app O); and the internal review and audit control program (under provisions of AR 11-7 as modified by this regulation).

b. Annual reports.

(1) Army organizations will report those activities that meet the definition of a sensitive activity (para 1-3a) annually in November to the TMO in accordance with paragraph 3-3c(1) of this regulation.

(2) Army SAP PDs/PMs or managers will report annually in November to the TMO, other DOD or Federal agency SAPs or programs from which the SAP has received resources or to which the SAP has directly provided resources or supported, in accordance with paragraph 3-3c(1) of this regulation.

c. Reviews.

(1) *SAPOC.* The 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 the ASA(ALT), OGC, DCS, G-2, DCS, G-3, DAIG, and TJAG. Frequently invited members include the ASA(FM&C), CIO/G-6, DCS, G-4, DCS, G-8, DCS, G-1, Chief of Engineers, program analysis and execution, CLL, Auditor General, AMC, U.S. Army Criminal Investigation Division Command (USACIDC) and USAINSCOM.

(b) Executive secretary. The Chief, TMO is the executive secretary of the SAPOC.

(c) SAPOC reviews. The SAPOC—

1. Reviews requests for the establishment, restructure and disestablishment 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. The 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, as requested.

(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. The Chief, TMO chairs the Working SAPOC. The Working SAPOC is primarily a security review and as such should be attended at a minimum by a program's PD/PM and program security manager (PSM). Standing members include points of contact from SAAL-SSP, the DCS, G-2, DCS, G-3, DAIG, TJAG, CIO/G-6, and OGC. Other attendees include POCs from each of the major Army Staff elements and HQ Intelligence Command/902d MI Group, AMC, DSS, and the AAA. The working SAPOC reviews each program prior to its presentation to the SAPOC (format for the SAPOC briefing is shown in app F). During its review, the working SAPOC identifies issues and formulates recommendations to present to the SAPOC.

(2) *The SAP Program Performance and Budget Execution Review System (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. Standing members of the committee are the TMO, ASA(ALT), OGC, ASA(FM&C), DCS, G-2, DCS, G-3, DCS, G-8, and TJAG. Additional members may include the CIO/G-6, DCS, G-4, DCS, G-1, Chief of Engineers, CLL, AAA, and DAIG, depending on the agenda. The committee's executive secretary is the Chief, TMO. The executive secretary will submit the results of the Working SAP PPBERS Committee to the VCSA and the Undersecretary of the Army twice annually (the second and fourth quarter of the fiscal year). The Under Secretary of the Army and the VCSA will jointly authenticate the committee minutes.

(c) PPBERS review. The PPBERS reviews—

1. Overall program performance objectives.

2. Obligation and disbursement data.

3. Budget year issues or problems.

4. Deviations from planned performance and HQDA goals.

5. Recommended corrective actions or reprogramming of funds.

(d) Administrative support. The TMO provides administrative support to the SAP PPBERS Committee

(e) Working PPBERS Committee. The 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 the 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, through the MACOM, submits data to the TMO in the format given in appendix C.

(3) *Fix-It Committee.*

(a) *Purpose.* The Fix-It Committee provides oversight of sensitive activities, SAP audits and inspections. It convenes annually to brief the Director of the Army Staff on progress made during the year to resolve issues and correct deficiencies identified in audits and inspections. Also reviewed are the SA areas of interest for possible trends, and a review of the next fiscal year SA areas of interest.

(b) *Composition.* The Fix-It Committee is a general officer forum chaired by the Director of the Army Staff. Standing members are the ASA(ALT), ASA(FM&C), OGC, DCS, G-2, DCS, G-3, TJAG, AAA, DAIG, DCS, G-8, and the USACIDC. The VCSA or the Director of the Army Staff designates other members of the Fix-It Committee based on the agenda for a specific meeting. Additional attendees may include representatives of the DCS, G-8, CIO/G-6, DCS, G-4, and DCS, G-1 and the CG, USAINSCOM; CG, AMC; CG, Military District of Washington; and the Chief of Engineers. The Chief, TMO is the executive secretary of the Fix-It Committee.

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

(d) *Working Fix-It Committee.* The Chief, TMO co-chairs the Working Fix-It with the DCS, G-2, DAIG, AAA, SRO, and FIU. 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. Two weeks prior to a meeting of the working Fix-It Committee, respondents provide the TMO with fix-it status sheets (see app G). If a respondent is recommending that a finding be closed, the respondent 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 followup IRAC review (under provisions of AR 11-7).

d. *Audits.* Audits are detailed examinations of any SAP and or sensitive activity following generally accepted auditing standards issued by the General Accounting Office (GAO). Audits include financial audits, performance audits (economy and efficiency audits, program audits), and the SA special area of interest.

(1) *Internal audits.* Internal audits include those performed by the AAA as well as those done by IRACs. All Army SAPs and or sensitive activities are subject to internal audit. The TMO integrates the AAA audit plan with the DAIG 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 the 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 the GAO, Office of the Inspector General, and the Defense Contract Audit Agency. The TMO functions as the entry point for all SAP-related external audits entering Army channels except standard Defense Contract Audit Agency (DCAA) contract support audits. The TMO notifies the cognizant MACOM SAP central office or IRAC after being notified of an external audit. The 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 Agency and the DCAA for contract audits as well as accounting and financial advisory services regarding contracts for Army SAPs.

(4) *Findings.* Findings from AAA audits, DAIG inspections, and SRO reviews of SAPs and sensitive activities and all non-Army (for example, DAIG and the GAO) audits of Army SAPs and sensitive activities are addressed in the fix-it process.

e. *Inspections.*

(1) The DAIG conducts inspections of SAPs and sensitive activities under the authority of AR 20-1. These inspections include an assessment of compliance with AR 380-381, command and control, program management, financial management, security, contract management, intelligence oversight and SA special areas of interest. DAIG inspectors will have full access to Army participation in other component SAPs, to ensure complete reporting to the SA.

(2) The Department of Defense Inspector General (DODIG) or other DOD agencies conduct audits and inspections of SAPs or sensitive activities on the basis of special concerns or unusual events. Programs should coordinate with the TMO before contacting any DOD agencies concerning inspections.

(3) The ASA(ALT), U.S. Army Contracting Agency, conducts procurement management reviews of secure environment contracting in support of SAPs and sensitive activities.

(4) USAFMSA conducts biennial manpower management reviews. No later than 120 days prior to their annual SAPOC, SAP PDs/PMs coordinate a manpower and workload validation with the USAFMSA SAP representative to accommodate an onsite visit if USAFMSA deems it necessary. The PD/PM reports findings of the USAFMSA during the annual SAP revalidation at the SAPOC.

(5) The SRO conducts quality assurance reviews of financial activity under the authority of AR 11-37. SRO refers any serious or repeat deficiency to the Fix-It Committee for resolution. SRO reviews the finance and accounting offices that have sensitive support missions annually and quarterly 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 are required to include SAPs in their organizational inspection programs.

f. Investigations.

(1) Each PD/PM, commander, or director of a SAP or sensitive activity must publicize procedures for reporting fraud, waste, abuse, and corruption without compromising sensitive information. The DAIG Intelligence Oversight Office is the designated agency for these matters.

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

(3) The DODIG and GAO also have investigative branches. Before a DODIG or GAO investigation, the TMO must be notified. The TMO will facilitate the granting of necessary SAP access for these investigations.

(4) Security related incidents involving SAPs are investigated and reported in accordance with AR 380-5 and SAP security guidelines. Items of CI interest will be investigated by USAINSCOM in accordance with AR 381-12, AR 381-20, and SAP security procedures. Summaries of all CI investigations involving SAPs will be provided to TMO security. A copy of the results of an investigation under the provisions of AR 15-6, involving SAP security-related incidents, will be provided to the TMO and DCS, G-2 within 30 days of approval by the appointing authority.

(5) PDs/PMs, 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.

(6) Each SAP will have a written OPSEC program plan from conception to disestablishment. The OPSEC survey is a method used to determine what the critical information is and if there is adequate protection of critical information during planning, preparation, and execution.

(a) OPSEC programs use the following evaluation steps, but do not have to follow them in any particular sequence:

1. Identification of critical elements.
2. Analysis of the threat.
3. Analysis of vulnerabilities.
4. Assessment of risks.
5. Applications of appropriate countermeasures (OPSEC measures).

(b) The objective of the OPSEC survey is to identify vulnerabilities in the program's operations or activities that an adversary could exploit.

(c) The OPSEC survey checks how well a unit executes its plan to protect critical program information. To be effective, an OPSEC survey requires careful prior planning, thorough data collection, and thoughtful analysis.

(d) The OPSEC survey attempts to reproduce the intelligence that a specific program projects. From that image it identifies exploitable information and sources. The objective of the survey is to assist the PD/PM in identifying and correcting weaknesses, which could disclose critical program information. The survey is conducted annually and a written memorandum will be maintained identifying the results and findings. The program is responsible for the conduct of this annual survey. USAINSCOM CI assets may be called upon to assist in the process, but in accordance with AR 530-1, the program will use its own resources to conduct the survey.

g. Management control program. If Army participation in another DOD or Federal Agency SAP requires 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.

h. Internal review and audit compliance program.

(1) The IRAC program (under provisions of 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, coordinating audit results, and audit follow-on.
- (c) Ensure that SAPs are included in the auditable entity files of the responsible IRAC office.

(2) MACOMs/PEOs or Army Staff 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/Army Staff 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.

i. Restructure.

- (1) SAPs may require restructuring to:
 - (a) Create a new subcompartment.
 - (b) Disestablish an existing subcompartment.
 - (c) Alter an existing charter or create a new one.

(d) Change security requirements.

(2) A SAP PD/PM desiring to restructure the SAP will submit a memorandum through the chain of command to the TMO. The memorandum will include the specifics of the restructure, the reason for the restructure, and a statement regarding impact on security, manpower, or funding, and a POC for the restructure.

(3) The TMO reviews and staffs the request. If the 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, the 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 Deputy Secretary of Defense.

j. *Training.* PSMs follow the guidance in AR 380–5, paragraph 9–12. Additionally, Army SAP security personnel must complete the DSS Academy basic course curriculum for SAP security professionals within 12 months of assignment to a SAP or SAP oversight/support office (for example, the TMO; DAIG; DCS, G–2; AMC, G–2; and so on). Security personnel who have been assigned continuous full-time duties as an Army PSM for 5 or more years may request a waiver to this requirement from the TMO. The DCS, G–2 will act as the quota manager for Army positions and will verify accomplishment of DSS Academy set prerequisites prior to forwarding student attendance requests to the DSS Academy. Changes to required coursework for SAP security professionals will be published by the TMO (in coordination with the DCS, G–2) as required.

4–6. Disestablishment

a. *Removal of SAP security controls.* The Army Staff/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 includes, but is not limited to—

(1) The research, development, test, and evaluation procurement, training, or other requirements during a program's life cycle significantly increase the number of personnel requiring knowledge.

(2) The tactical or strategic impact or value of the system, operation, or activity lessens significantly from when it was first established.

(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 use of 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 Deputy Secretary of Defense 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 (see app H), staffs it with the MACOM/PEO for review and concurrence, then submits it to the TMO.

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

(5) If the SA recommends disestablishment, the TMO will forward the SA recommendation to OSD with congressional notification letters. If Congress does not object within 14 days, the TMO notifies appropriate Army Staff, MACOMs, 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 the TMO that the actions specified in appendix I have been accomplished. The TMO refers to the Fix-It Committee for followup on all SAPs not completing disestablishment actions and gaining certification (under provisions of app I) as disestablished by the end of the 6-month period.

4-7. Army participation with other DOD or Federal agency components SAPs

a. A DOD or other Federal agency SAP for which the Army is designated the executive agent is considered an Army SAP for purposes of this regulation and will fully comply with this and all other Army regulations.

b. Army organizations may participate in SAPs sponsored and executed by non-Army organizations without establishing a separate Army-executed SAP. However, the Army organization and the SAP sponsor must establish, and keep current, a MOA.

c. No DA organization, command, activity, or individual will negotiate an MOA with any non-DOD activity without prior coordination with the TMO. After the MOA has been drafted, it will be forwarded to the TMO for review and approval prior to it being signed by the Army entity entering into the MOA. These programs will be managed based on their individual requirements and may have more limited access than the Army baseline billet structure. All MOAs, including Army entities and DOD activities, will be forwarded to the TMO for review.

d. The MOA must minimally address program access, security, oversight, and financial resourcing and management. At a minimum, the other DOD component or Federal agency must consent to approve access when required for the following personnel:

- (1) SA.
- (2) Under Secretary of the Army.
- (3) General Counsel, Deputy General Counsel, and a special programs staff officer.
- (4) Chief of Staff, Army.
- (5) Vice Chief of Staff, Army.
- (6) Appropriate principals of HQDA staff (for example, the DCS, G-3, DCS, G-2, ASA(ALT)).
- (7) DAIG; Chief, Intelligence Oversight Division; and appropriate intelligence oversight division action officers.
- (8) TJAG and a special programs staff officer.
- (9) The Chief, TMO; the Deputy Chief, TMO; the Director of Security; the legal advisor; the finance officer; and appropriate action officers.
- (10) The SAAL-SSP Director, Deputy Director, and appropriate action officers.
- (11) AAA auditors as required.
- (12) Appropriate principals of MACOM/PEO staff.

e. Any involvement in DOD or Federal agency SAPs that does not afford at least the minimum access defined 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 the Chief, TMO, for approval by the SA.

f. This restriction is not intended to limit the Army SAP PD/PM from providing SAP information to any properly cleared individual with a need-to-know when Army SAP documents are not stored by the other DOD component or Federal agency.

g. The MOA will comply with the format of AR 25-50 and includes the effective date and requirement for biennial review. Army MOA signature authority is based on the level of agreement. MOA/Memorandums of Understanding (MOUs) for annual support should be in accordance with DOD Instruction 4000.19, Interservice and Intergovernmental Support. Work performed on a reimbursable basis should be in accordance with DOD 7000.14-R, volume 11, chapter 1.

h. 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.

i. Army support to other DOD and Federal agency SAPs is governed by DODD S-5210.36.

j. See paragraph 5-2 of this regulation and the NISPOM Supplement Overprint for use of co-utilization agreements when SAPs from multiple programs are stored in a single location.

Chapter 5 SAP Security

5-1. General

Army SAPs will implement the provisions of the NISPOM Supplement Overprint to ensure consistency within the Army, DOD, and industry. Conflicts among Army intelligence, security regulations, DOD 5220.22-M, DOD 5220.22-M Supplement, and the NISPOM Supplement Overprint will be resolved by the TMO. All reference to a program security officer within the DOD 5220.22-M Supplement and the NISPOM Supplement Overprint is intended to identify the individual assigned as the Government program security manager for a specific program. With respect to SAP security guidance, in cases involving policy clarification, conflicts, or incomplete guidance, written requests must

be submitted to Director of Security, TMO. Written procedures or guidance will be provided to the PM/PSM within 30 days.

5-2. Physical security

a. Security level. All Army SAP information will be stored in an accredited SAP facility (SAPF). A SAPF is an area, room, building, or installation that is accredited to store, use, discuss or electronically process SAP information. MOAs (co-utilization agreements) are required prior to allowing other SAPs to share spaces. SAP security managers are required to accredit (in writing, documenting each standard prescribed below) all facilities to be used as SAP facilities for their program, to include discussions, storage, and AIS processing. As a general rule, SAPs base the level of physical security on the classification level of the information processed or stored by the SAP. The first SAP in the space is the senior SAP and will act as the cognizant security authority for the space unless an alternate arrangement is specified in the co-utilization agreement. The standards prescribed in the following paragraphs pertain to continental U.S. SAPFs. SAPFs operating outside the continental United States must meet the same minimum standards prescribed for continental U.S. facilities as well as the standards prescribed in AR 380-5, paragraph 7-7. All Army SAPFs have 12 months from the effective date of this publication to meet the physical security standards prescribed herein.

(1) SAPs processing or storing TOP SECRET/SAR, unacknowledged, or SCI adhere to standards established by Director, Central Intelligence Directives (DCID) 6/9 and the applicable requirements of DOD S-5105.21M-1. If a SAP is co-utilizing an SCI facility, the SAP security manager must do so with the agreement of the cognizant senior official intelligence community for the facility or a designee. A MOA will be entered into between the senior official intelligence community and the SAP security manager for security administration within the facility. This does not preclude an Army office from establishing SCI standards (that is, establishing a DCID for a SAP if the risk assessment completed for the PD/PM establishes the requirement).

(2) SAPs processing or storing SECRET/SAR that do not contain unacknowledged or SCI will establish a SAPF using the following physical standards.

(a) Floor, walls, and roof. The walls, floor, and roof construction of SAPFs must be of permanent construction materials (plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of, unauthorized entry into the area). Perimeter walls will be extended from the true floor to the true ceiling and attached with permanent construction materials.

(b) Ceiling. The ceiling will be constructed of plaster, gypsum, wallboard material, hardware, or other similar material that the command security manager judges to be of equivalent strength.

(c) Doors.

1. The access door to the room will be constructed of wood or metal. Acceptable types of doors are:

a. Solid wood core door, a minimum of 1-3/4 inches thick.

b. Sixteen-gauge metal cladding over wood or composition materials, a minimum of 1-3/4 inches thick (the metal cladding will be continuous and cover the entire front of the door).

c. Metal fire or acoustical protection doors, a minimum of 1-3/4 inches thick (a foreign manufactured equivalent may be used if approved by the General Services Administration (GSA)).

d. A joined metal rolling door, minimum of 22 gauge, used as a loading dock or garage structure must be approved case by case.

2. The hinge pins of out-swing doors will be pinned, brazed, or spot-welded to prevent removal.

3. The access door will be equipped with a built-in GSA-approved combination lock.

4. For open storage areas approved under previous standards, the lock can be the previously approved GSA combination lock. However, upon retrofit, the door must be fitted with a GSA combination lock.

5. Doors, other than the access door, will be secured from the inside, for example, by using a deadbolt lock, panic deadbolt lock, rigid wood or metal bar that extends across the width of the door, or any other means that will prevent entry from the outside. Key operated locks that can be accessed from the exterior side of the door are not authorized.

(d) Windows. Windows that are less than 18 feet above the ground when measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, will be constructed from or covered with materials that will provide protection from forced entry, and must be permanently sealed. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

(e) Openings. Utility openings, such as ducts and vents, will be kept at less than a person-passable, 96-square-inch opening. Openings larger than 96 square inches will be hardened in accordance with DCID 6/9 (para 3.3.4), which provides guidance to ensure that appropriate physical security considerations are included in the design of facilities.

(f) Sound. All SAPF perimeter walls will meet Sound Group 3 (sound transmission class of 45 or better, where loud speech can be faintly heard but not understood and normal speech is unintelligible), unless additional protection is required for amplified sound. If compartmentation is required within the SAPF, the dividing office walls must meet Sound Group 3.

(g) Establishing SAPFs. The following Government/military personnel are authorized to establish Army SAPFs, SAP secure working areas (no storage authorized), and temporary secure working areas (temporary use as a SAPF): SAP security managers (for their program); Chief, TMO (all Army programs); Director of Security, TMO (all Army

programs); Director, SAAL–SSP (all Army Acquisition programs); and security manager, SAAL–SSP (all Army Acquisition programs).

(h) *TOP SECRET/SAR, unacknowledged or SCI SAPs located inside a tenant SCIF.* Constructing a SAPF to DCID 6/9 standards inside a tenant SCIF is not required if a determination (in writing) has been made by an authorized command official (PD/PM or PSM) that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility (security in depth). Examples include, but are not limited to use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard patrols throughout the facility, especially during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during nonworking hours. If all personnel working in the SCIF are not briefed to the SAP, and the PD/PM or PSM has determined that security in depth exists, the SAPF must meet only the standards prescribed in paragraph 5–2a(2)(a) through (g).

(i) *Inactive SAPF.* If a previously accredited SAPF becomes inactive for a period not to exceed 1 year, the SAP accreditation will be reinstated (in writing by the PSM) by the gaining accrediting agency, provided the following is true:

1. The threat in the environment surrounding the SAPF has not changed.
2. No modifications have been made to the SAPF that affect the level of safeguarding.
3. The level of safeguarding for the new program is comparable to the previous program.
4. The SAPF has not lost its SAP accreditation integrity and the Government has maintained continuous control of the facility.

(j) *Intrusion detection systems.* SAP facilities must comply with the requirements outlined in DCID 6/9, annex B.

b. *Risk assessment.*

(1) PDs/PMs of SAPs will conduct risk assessments to determine the physical security standards (using para 5–2a(1) and (2)) for program facilities.

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

(3) The risk assessment incorporates—

(a) *Counterintelligence assessment.* The CI assessment is an indepth analysis of the program's vulnerability to foreign collection efforts.

(b) *Program security assessment.* PDs/PMs will review information from the CI assessment and the OPSEC assessment to determine whether the program requires further technical protection. If required, the PD/PM will request a TSCM survey.

c. *Two-person integrity.* See the NISPOM Supplement Overprint, paragraph 1–204.

d. *Entry/exit searches.* MACOM/PEOs, program offices, and the SAP central office for the Army may establish entry/exit programs in accordance with AR 380–5 and DOD 5220.22–M.

5–3. Document/information security

a. *Authorization.* The TMO is the only office authorized in the Army to store in one location a list or compilation of all Army SAPs to include a briefing that outlines all Army SAPs, or all Army SAPs in a single category (without waiver). In order to avoid the compromise of a significant portion of Army SAPs, Government and contract organizations are prohibited from assembling, in a single reference, a significant compilation of Army SAP programs. A single reference includes, but is not limited to, briefing books, reference books, reference lists, and "cheat sheets." A significant compilation is the assembly of documents for five or more SAPs. This prohibition is not intended to preclude the centralized storage of documents from a significant number of SAPs (five or more) when information from different SAPs are stored separately and not assembled into a single reference. Requests for exception will be submitted to the TMO for approval or disapproval.

b. *Marking.* Authors of classified information will mark documents in accordance with AR 380–5 and the NISPOM Supplement Overprint.

c. *Transmission.* SAP material will be transmitted in accordance with NISPOM Supplement Overprint procedures in paragraph 5, section 4–00.

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) All requests for congressional access or access by other Government agencies must be staffed through the TMO for approval by the appropriate OSD SAP central office. Army SAP PDs/PMs, or subordinates are not authorized to grant access to Members of Congress or their professional or personal staffs.

(2) DOD grants SAP access to select members of Congress and their staffs. When indoctrinating these individuals, access approval authorities 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, the ASA(ALT)) 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.

(3) 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 DD Form 254 (Department of Defense Contract Security Classification Specification) must state, "Public release of information concerning any aspect of this contract is prohibited."

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

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

(6) Patent applications containing SAP information are submitted through ASA(ALT) 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, the Chief, TMO will notify the Director, OSD SAPCO, of the proposed release of SAP information.

e. Physical construction standards. See 5–2a(1) and (2) for guidance.

f. Destruction. Responsible offices destroy SAP material in accordance with AR 380–5, the NISPOM Supplement Overprint, AR 25–400–2, and applicable program security classification guides.

g. Archiving. The TMO 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 in accordance with AR 25–400–2 and send SAP related documents to the TMO 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 PSG and the NISPOM Supplement Overprint (in situations where the two conflict, the more restrictive guidance applies until the conflict is resolved by the TMO).

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

i. Receipting. Use classified information receipts 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 the command, in which case transmitters and recipients follow the provisions of AR 380–5 and paragraph 5–31.

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

k. Courier. The PSM will follow the courier instructions provided in AR 380–5, chapter 8. Additionally, personnel acting as couriers of SAP material, whether inside or outside the continental United States, must transport, directly and without delay, SAP material from one SAPF to another SAPF. While transporting the material outside of a SAPF, designated couriers will not open, examine, read, or otherwise expose SAP information while in any public or private area (hallways, places of business, public conveyance, and so on). A comprehensive list (DA Form 3964 (Classified Document Accountability Record)) of all material transported, to include titles for all documents contained on AIS media, will be prepared by the PSM (prior to courier departure). Couriers will receive a courier briefing (which will include the information provided in AR 380–5, as well as the information listed in this paragraph) prior to being authorized to courier SAP material. Couriers are required to sign a statement acknowledging the fact that they have received the briefing. PSMs will retain a copy of the signed courier acknowledgement for 24 months.

5–4. Personnel security

a. Clearances. The Army grants access to SAP information based on requirements in AR 380–5, the NISPOM Supplement Overprint, and DOD O–5205.7. At a minimum, the following standards apply:

(1) *Standard for TOP SECRET and SECRET.* Candidates must meet the standards prescribed in DOD O–5205.7 and must have a clearance current within the past 5 years (entry national agency check and national agency check with inquiries investigations and INTERIM Clearances do not qualify for SAP access).

(2) *Exceptions.* If a candidate for access to a TOP SECRET or SECRET SAP possesses a qualifying clearance older than five years, an access approval authority may approve the candidate for access to the SAP as long as ALL of the following information/actions are true/taken:

(a) The candidate meets the standards prescribed in DOD O–5205.7, a periodic reinvestigation has been submitted, and verification of receipt from the investigating organization has been received, and the PM/PSM has reviewed the Standard Form (SF) 86 for potentially derogatory information..

(b) The candidate has been in a continuously cleared status during the time period after the 5-year mark expired.

(c) The 6-year mark has not been reached.

(3) *Waivers.* The TMO may grant waivers to these requirements case by case and only for Army SAPs or for SAPs for which the Army has been designated executive agent.

b. 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.

c. 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 PD/PM must report valid derogatory information to the DCS, G–2 or FIU as appropriate for an independent impartial investigation. The PD/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. Contractor personnel will make reports of derogatory information in accordance with DD Form 254. At a minimum, contractors will report derogatory information to their cognizant security agency and Government PSM.

5–5. Technical security

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

(1) Use systems listed in the National Security Agency’s Information Systems Security Products and Services Catalog. Refer to AR 381–14 for specific requirements. Use of items not included in National Security Agency’s Information Systems Security Products and Services Catalog must be requested and coordinated with the CIO/G–6 to obtain a waiver approved by the TMO.

(2) Limit nonsecure 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 will follow the standards specified in DCID 6/9.

b. TEMPEST. AR 381–14 implements national TEMPEST policies and procedures. SAP security managers will utilize the decision matrix in AR 381–14, chapter 4, to determine if a TEMPEST countermeasures review is required. A TEMPEST review will be performed for new IT systems, as specified in previous reviews, and prior to the programming and expenditure of funds for TEMPEST. The TAO (at the direction of the CIO/G–6) will coordinate the requirement for any TEMPEST facility and equipment test with USAINSCOM. Information copies of TEMPEST review requests and reviews will be provided to the TMO and DCS, G–2. To preclude unnecessary expenditures, program offices must consult with the TAO (through the CIO/G–6) representative at the earliest possible stage in the planning process regarding the application of TEMPEST countermeasures.

c. TSCM. Programs should request TSCM support, with the assistance of the supporting USAINSCOM CI element to expedite the process, to USAINSCOM, G–3. TSCM surveys requested by the TMO will be conducted within 30 days of the date on the memo requesting the survey (dependent upon asset availability). Offices of the senior leadership will also receive a survey at least annually. Verification of senior leadership office surveys will be provided to the TMO in the form of a postsurvey briefing to the Director of Security, TMO (within 7 days of the survey). AR 381–14 prescribes the physical and technical security standards for implementation in certain facilities where SAP information is electronically processed or routinely discussed aloud.

(1) SAPs request TSCM services only when the facility risk assessment indicates the threat or vulnerability of the facility requires a technical security evaluation. PDs/PMs will include the risk-assessment results in the SAP establishment package.

(2) Annually, USAINSCOM reviews the program facility risk assessments and the TSCM schedules for each program. USAINSCOM provides its results and recommendations to the PD/PM and DCS, G–2 as part of the working SAPOC brief.

(3) USAINSCOM will conduct TSCM surveys only on finished facilities that 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 in order to have access. Upon completion of TSCM surveys, the PD/PM 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 will consult with USAINSCOM 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.

b. Treaty proponent. The DCS, G–3 is the Army staff proponent for implementation and compliance for arms control treaties. The ASA (Installations, Logistics and Environment) serves as the Army’s arms control implementation and compliance review manager.

c. Treaty security measures. Because of the short notification times and 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 alert SAPs resident in their facilities quickly.

(1) SAP PDs/PMs, assisted by supporting CI 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) PDs/PMs must educate program personnel on the potential security threat treaties pose.

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

(4) The TMO, DCS, G-2, 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 DCS, G-2 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, the 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 this regulation, 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 (for example, an MOA; data exchange agreement; information exchange agreement in accordance with DODD 5530.3; and a DCS, G-2 approved delegation of disclosure authority letter) and, in cases of waived SAP information, Deputy Secretary of Defense approval.

c. PDs/PMs 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. PDs/PMs must ensure the program SCG and PSG clearly identify the release authority. As with all international efforts, a subcompartment must be established to protect information that will be exchanged.

d. PDs/PMs, MACOMs, and SAP proponents that identify the need for foreign release of SAP and SAP-related information/technology must submit the required documentation to the DCS, G-2 for review and approval. The DCS, G-2 will coordinate with SAAL-SSP and the TMO (see chap 10 of this regulation for additional guidance).

e. The PD/PM 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, SAP, or SAP-related information without the written approval of the DCS, G-2 (see AR 550-51).

f. Any person who has any indication that a foreign government has compromised SAP information will report the compromise immediately (within 24 hours) to the TMO and DCS, G-2. The TMO will report to the OGC, TJAG, the VCSA, the CSA, the Under Secretary of Defense, and the SA as well as to the National Disclosure Policy Committee. The program affected will conduct a damage assessment (and may request assistance from the DCS, G-2) and provide copies of the completed case report and damage assessment to the Chair, National Disclosure Policy Committee (see AR 550-51).

5-8. Program security plan

a. Security plan. The PD/PM will develop and submit a final security plan to the TMO within 60 days of PSAP approval. The MACOM/PEO and Army Staff 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, program security guide, OPSEC plan, CI assessment, indoctrination briefing, and a treaty plan (if applicable). Ensure submission of an initial TEMPEST countermeasures review to PEO EIS-TAO CTTA during PSAP status, and a TEMPEST countermeasures review to the USAINSCOM CTTA upon accreditation as a SAPF. Update TEMPEST risk assessment to USAINSCOM CTTA every 3 years or upon a substantive AIS equipment, network, or physical change to the SAPF.

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

(1) The PSM assists the PD/PM and program technical personnel in preparing the SCG.

(2) The original classification authority signs the SCG.

(3) The TMO, in conjunction with DCS, G-2 and the SAP Army Staff proponent, approves the SCG prior to original classification authority signature and SAP approval.

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

(5) 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 and approved at HQDA. Revised or proposed SCGs should be submitted by the PD/PM through the Army Staff proponent to the TMO for approval 60 days prior to implementation unless otherwise directed by the Chief, TMO. The TMO will coordinate Army Staff review and return the SCG with comments.

(7) The program office conducts an annual review of the SCG to verify currency. The PSM completes a Memorandum for the Record verifying the review has been conducted and forwards a copy through the MACOM/PEO intelligence officer to the TMO (within 30 days of the review) for retention. The SCG must be republished through the formal staffing process every 5 years.

d. PSG. The PD/PM develops a PSG to provide indoctrinated personnel specific security procedures for protecting program information. In addition to identifying the access control authority (ACA) and access approval authorities, the PSG 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 PSG also addresses treaty verification inspections and foreign travel/contact. As with the SCG, the following occurs:

(1) The PSM prepares the PSG.

(2) The TMO approves the PSG prior to PD/PM signature and PSAP approval.

(3) PSM ensures everyone handling program information has access to a PSG.

(4) DD Form 254 for contractors references applicable PSGs.

(5) The program office conducts an annual review of the PSG to verify currency. The PSM completes a Memorandum for the Record verifying the review has been conducted and forwards a copy to the TMO (within 30 days of the review) for retention. The PSG must be republished through the formal staffing process every 5 years.

e. OPSEC assessment. OPSEC is the responsibility of the SAP PD/PM. The PD/PM prepares and approves an OPSEC annex to the security plan (in accordance with AR 530-1) with the assistance of the TMO, DCS, G-3, and USAINSCOM. The program provides final copies to the TMO and DCS, G-2.

(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. At a minimum, the OPSEC annex addresses the critical elements (formerly essential elements of friendly information), threat, travel/mail procedures, testing, media and public release, and program signatures reduction.

5-9. Security incidents involving SAP programs

a. Notification. Individuals who become aware of a security incident involving classified information and/or a serious incident that could reasonably impact program security will contact the program office immediately. Upon learning of the incident, the PD/PM and PSM will take immediate steps aimed to minimize further damage and regain custody of the information, material or mitigate damage to program security. Within 24 hours of notification of the incident, the PD/PM will notify the DCS, G-2, the TMO (Security,) and the normal SAP reporting chain of command (to include the covering CI agent). The PD/PM will provide an updated report to the DCS, G-2 and TMO not later than 72 hours after the incident. The PD/PM will provide the DCS, G-2 and the TMO a final report in every case, however the due date is case specific (reasonable time period to be decided by the DCS, G-2 and the TMO). With respect to the types of incidents that must be reported to the DCS, G-2 and TMO (Security), refer to chapter 10 of AR 380-5.

b. 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 (see para 5-9a) and requests a new nickname or code word. The TMO takes the necessary action to cancel the compromised nickname/codeword and designates a new name(s) (in accordance with Chairman Joint Chiefs of Staff Memo (CJCSM) 3150.29B).

c. Security incidents involving AIS. In addition to the reporting requirements specified in 5-9a., if a compromise of SAP information involves AIS, the PD/PM will immediately consult HQDA (DCS, G-2) 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 information. After the discovery of the incident (the DCS, G-2 will provide guidance on timing), all accreditation packages will clearly identify the incident (or type of incident if the fact of the incident is classified and the accreditation document is unclassified), its status, and any corrective action taken. The DCS, G-2 and the TMO will coordinate the response to the security incident. The information assurance security officer or information system security representative will comply with the procedures listed in appendixes J and K.

d. Inadvertent disclosure. In the event that a person inadvertently gains access to classified information, the PD/PM

of PSM will request that the person read and sign a DA Form 5750 (Inadvertent Disclosure Oath) and discuss the disclosure with the individual to ensure that the information is properly protected. If the inadvertent disclosure was to a person with an appropriate level of clearance, but without a need to know, further debriefing may not be necessary. If, however, the disclosure was to a person without the appropriate level of clearance, a formal debriefing is required. If the person refuses to sign DA Form 5750, the PD/PM or PSM will advise the person that refusal to sign is grounds for denying that person future access to classified materials, and may be grounds for administrative action (see AR 380–5 for additional information).

e. Special situations. The TMO 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.

f. Review and update. The PSM will review and update PSGs and SCGs every 12 months (see para 5–8 for additional direction).

g. SAP security incident response team. At the discretion of the Chief, TMO, the DCS, G–2, TJAG, USACIDC (FIU), reporting units, and other organizations will, on order, provide a senior action officer (04/GS–13 or above) to the TMO to form a security incident response team (SIRT). The SIRT will establish operations within TMO office space in order to receive information updates on security incidents affecting SAPs, provide guidance to program or unit security managers, and provide a single, central point for information flow to the Army and DOD senior leadership. The security incident response team works under the administrative control of the Director of Security, TMO, who directs the team’s actions and assists in determining the duration of the team’s mission. SIRT duties take precedence over any other duties the team members may have within their respective agencies/activities. The team stands down on order of the Chief, TMO.

Chapter 6

Access Control

6–1. Validation of access requirements

a. The SAPOC validates each program’s initial personnel access ceiling (PAC) or billet structure requirements and revalidates them annually until program disestablishment.

b. The 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 PAC requirements. Approves or disapproves requests for changes above the 5 percent or 100-person annual change ceiling specified in paragraph 6–3.
- (3) Directs and approves changes to program PAC and billet structure.
- (4) Reviews and approves requests to double slot personnel for more than 90 days.
- (5) Maintains a reference copy of access and billet data from each program. These data are updated real time by the programs, or no less than quarterly in accordance with paragraph 6–8.

c. The TAO will—

- (1) Develop, document, maintain, develop training for, distribute, and upgrade ASATS software that supports program PACs.
- (2) Provide real-time updates of the data via wide area network to PDs/PMs and other designated users.
- (3) Maintain the central ASATS database for all Army SAPs. The TMO will maintain a backup database.
- (4) Provide customer service and training support for ASATS users as required.
- (5) Establish and maintain a central database of all SAP and sensitive activity IT systems that process SAP information.

(6) Establish, test, and maintain a continuity of operations plan for ASATS to enable the SAP automation backbone to remain operational with minimal disruption in the event of natural or man made catastrophes that render the primary ASATS site incapable of operations. The ASATS continuation of operation plan will be tested annually under the direction of the Chief, TAO and the Chief, TMO, with lessons learned documented and implemented in order to validate the continuity of operations plan.

d. SAP proponents (MACOM/PEO/Army Staff) will—

(1) Appoint the ACA and identify the ACA in the SAP PSG. The ACA is a general officer or Senior Executive Service (SES) employee in the chain of command for that program or activity. When the PD/PM is a general officer or SES employee, the ACA responsibility falls to the next higher level general officer or SES employee. Besides the ACA, the SA, Under Secretary of the Army, CSA, VCSA, and the Chief, TMO have authority to direct changes to the PAC and billet structures, grant access and indoctrinate personnel to all Army SAP information.

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

e. SAP ACAs—

- (1) Specify access management controls in the PSG.

(2) Appoint access approval authorities in writing. Appointment letters delineate the scope of the access approval authority's authority and authorize each access approval authority to indoctrinate and terminate access to the SAP. The authority of the access approval authority cannot be further delegated. The Chief, TMO is an access approval authority for all Army SAPs or DOD SAPs for which the Army is the executive agent. The Deputy Chief, TMO and the Director of Security, TMO are access approval authorities for all programs resident on the Army baseline.

(3) May delegate the authority to oversee access approval authority day-to-day activities to the PD/PM but retain access control responsibility for the program.

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

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

f. A SAP access approval authority—

(1) Must be an Army employee (Government or military). Requests for waiver to this policy must be submitted to the TMO for approval.

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

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

(4) 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.

g. PSMs maintain each program's master access roster (in ASATS) and are responsible for providing up-to-date security indoctrination briefings to program access approval authorities. Each program office is the office of record for program access.

6-2. Subcompartments

a. Upon approval by the TMO, proponents may devise subcompartments to limit knowledge of extremely sensitive aspects of the program. Subcompartments may be established only to conduct work that falls within the charter of the parent SAP. The TMO determines whether or not the work being proposed or conducted meets this standard. Proponents register all subcompartments with the TMO, which assigns a nickname and/or a code word for each subcompartment.

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

c. The PD/PM is responsible for the following actions upon establishment of a subcompartment:

(1) The PD/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 ASATS records to show subcompartment access.

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

(4) If required, a separate subcompartment PD/PM and PSM will be designated in writing by the proponent and approved by the TMO as part of the subcompartment establishment process.

(5) The TMO will determine if a separate PSG is required to address security responsibilities and countermeasures for personnel accessed to that subcompartment.

(6) PDs/PMs review and inspect subcompartment management practices and procedures.

(7) DSS or USAINSCOM (in case of carve-out) will be granted access for facility clearance inspections and industrial security reviews for all subcompartment contractor facilities.

6-3. Personnel access ceiling and billet structure

a. *Approval.* The TMO reviews and approves PACs and billet structures for Army SAPs and billets allocated to Army by other DOD or Federal agency SAPs.

b. *Personnel access ceiling and updates.* A PAC is an administrative recommendation made by the proponent and initially approved by the TMO and validated through the SAPOC. The PAC is an access ceiling that provides the total number of personnel who require access to a program. The PAC is not duty position specific but simply indicates the total number of personnel in a program authorized accessed. Changes to the PAC will be made in accordance with paragraph 6-3h.

c. *Billet structure and updates.* A billet structure is an administrative recommendation made by the proponent and initially approved by the TMO and validated through the SAPOC. The billet structure is duty position specific. Changes to the billet structure will be made in accordance with paragraph 6-3h.

d. *Billet structure and PAC requirements.* A billet structure is required only for waived SAPs and the TMO administered "SAP baseline." Unacknowledged and acknowledged Army SAPs are required to submit a PAC for review and approval to the TMO. Proponents for unacknowledged and acknowledged SAPs may request approval from the TMO for a billet structure in lieu of a PAC.

e. *Process.* Within 60 days following PSAP approval for a proposed SAP, the PD/PM develops and submits to the

TMO a proposed PAC. The PD/PM for the PSAP presents the PAC to the SAPOC during the SAP approval process and makes adjustments as necessary before the annual revalidation process. The TMO maintains a copy of all approved PACs. The process is identical for those programs required to have (or are requesting) a billet structure.

f. Army SAP baseline. The Army SAP baseline billet structure identifies positions at HQDA, subordinate commands, other DOD agencies and other Federal agencies that require access to all baseline SAPs to fulfill leadership, oversight, and management responsibilities. The 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. The Chief, TMO is the only approval authority for restructure (for example, billet additions and deletions) of the baseline. The Chief, Deputy Chief, and Director of Security, TMO are the only personnel authorized to approve requests for access to the Army SAP baseline.

g. PAC and billet structure essential functions. Both the PAC and a billet structure provide 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. Personnel briefed to the Army SAP baseline will not be counted against the PAC or billet structure of those programs on the baseline. For nonbaseline programs, the PAC or billet structure must include all program execution, management overview, and oversight positions.

h. Modifications. Within a 12-month period, each PD/PM, on his or her own authority, may make modifications to the PAC or billet structure that equate to 5 percent of the personnel accessed to the program or 100 positions/billets, whichever is less. If a PD/PM requires more than a 5-percent or 100-position/billet modification during a 12-month period, the Chief, TMO must approve the modification. PDs/PMs summarize changes to their PAC or billet structure during SAPOC revalidation briefings. While not as rigidly structured as billet plans, PACs still require a significant amount of management planning on the part of the PD/PM and the PSM. PAC plans provided to the TMO for review and approval will include a deliberate process for identifying the minimum numbers of Government, contractor, and other support personnel necessary to effectively execute the program.

i. Updates. As PAC or billet structure changes occur, PDs/PMs forward updated pages to the appropriate access approval authorities. The PAC or billet structure will be reviewed during the Working SAPOC. Changes to the PAC or billet structure will be approved during the executive SAPOC. After each SAPOC revalidation, PDs/PMs provide the TMO with an updated PAC or billet structure.

6-4. Rosters

a. Using ASATS software, SAP PDs/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, and date access granted, if appropriate. For personnel holding TOP SECRET clearances, PSMs will also maintain the date each employee's periodic reinvestigation is due to ensure accurate tracking of periodic reinvestigation status and to avoid late periodic reinvestigation submission. Additionally, PDs/PMs maintain an inactive roster listing all personnel debriefed from their program, recording the date of debriefing.

b. PDs/PMs notify access roster holders when individuals are debriefed and provide real-time or quarterly updates of ASATS data to the TMO.

c. PDs/PMs must address disposition of program access rosters in the disestablishment concept plan.

d. An individual's access to Army SAP information may be verified 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 (provided by a security staff member).
- (4) Checking ASATS (through an authorized user).

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 and approval from the program ACA or designated access approval authority for access to a SAP (see para 5-4). SCI will not be a prerequisite for access to Army SAPs.

b. All PDs/PMs must comply with the OSD SAP access matrix that requires specific access requests be forwarded through the OSD SAPCO. A current copy of the matrix should be requested from the TMO.

c. Individuals nominating personnel for access to a SAP submit a DD Form 2835 (Program Access Request) to the program access approval authority. An authorized security official (for example, the security manager) verifies the individual's clearance data (accomplished through the use of Defense Central Index of Investigations or Joint Personnel Adjudication System) before signing and submitting the DD Form 2835 to commander or PD/PM for signature concurrence. Final approval for access rests with the ACA or designated access approval authority. The SAP PD/PM maintains DD form 2835 (RCS exempt, AR 335-15, para 5-2b(4)) for 2 years after debriefing an individual, after which it is destroyed. Upon disestablishment of the SAP, the program disestablishment concept plan must address disposition of DD forms 2835 less than 2 years old at the time of disestablishment.

6-6. Indoctrination

a. Once an access approval authority has determined that an individual requires access to a SAP, the access approval authority indicates approval on the DD Form 2835 and signs the form.

b. Access approval authorities can limit the duration of an individual's access. In these cases, the access approval authority or person conducting the read-on notifies the individual of the date when their access will end. This expiration date is annotated on DD Form 2836 (Special Access Program Indoctrination Agreement) (RCS exempt, AR 335-15, para 5-2b(4)). The expiration date (if any) is included as an entry in the ASATS database. When the expiration date arrives, 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 will—

(1) Verify the information on the DD Form 2836, 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) Utilize the program's approved standard indoctrination briefing package.

(3) Require individuals to read, agree to, and sign DD Form 2836 before being indoctrinated.

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

(5) Include in the briefing program specific security requirements (for example, what is sensitive about the program and why), procedures for OPSEC and communications security, critical elements, classification guidelines, subversion and espionage directed against the army reporting, and how to report fraud, waste, and abuse without compromising security.

(6) Sign DD Form 2836 as the witness.

6-7. Termination of access

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, access approval authorities, or their designated representatives will use DD Form 2836 (Back) (RCS exempt, AR 335-15, para 5-2b(4)) for termination briefings.

Note. It is not recommended to fill in the electronic forms on the unclassified AIS connected to the Internet. Print or download these forms to your classified AIS for program use.

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 DD Form 2836 (Back) (except for the individual's signature) and forward it to the office of record.

c. PDs/PMs and access approval authorities continually review rosters, deleting individuals no longer requiring access to the SAP. The PDs/PMs retain 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. Army Special Access Tracking System

a. ASATS is an automated system for maintaining access and billet roster information for Army SAPs. ASATS will not be used to verify SCI access.

b. PDs/PMs will—

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

(2) Provide real-time ASATS data updates to the central ASATS database (contact the TMO).

(3) Perform a comprehensive review and reconciliation of ASATS data at least annually, prior to the annual SAPOC.

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 and the program security guide

a. DOD 5220.22-M specifies baseline security procedures for contractors working on Federal Government projects. The DOD 5220.22-M Supplement specifies additional procedures that apply to SAPs.

b. The NISPOM Supplement Overprint specifies required security enhancements for use by SAPs. The SAP PSG and DD 254 are the primary documents used to convey security requirements to Army SAP contractors. In cases of conflict between the NISPOM Supplement Overprint and the PSG and DD Form 254, the contractor will adhere to the more restrictive rule until the PSM can resolve the conflict. In cases requiring IT policy interpretation, the PSM will contact TMO Security, who will coordinate with CIO/G-6, for final resolution. Any security enhancements above those specified by the NISPOM Supplement Overprint for Army Government facilities must be approved by the TMO. Security enhancements above those specified by the NISPOM Supplement Overprint for contractor facilities must be forwarded for approval through the TMO to OSD.

7-3. Contractor personnel security

a. The basic personnel security requirements of DOD 5220.22-M 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 urinalysis and CI scope polygraph tests/examinations. The PD/PM must remove contractor personnel who withdraw their consent to undergo a polygraph from the program and report this action to the contracting officer.

7-4. Physical security

a. DSS industrial security representatives accredit SAPFs for Army SAPs under their inspection cognizance. The 902d MI Group accredits Army SAPFs for SAPs that have been carved out of DSS cognizance. In both cases, the accrediting agency will adhere to the SAPF standards described in this regulation (chap 5). Each SAP's PSG clarifies this basic guidance. After DSS or 902d accreditation, the PSM issues a letter to the contractor (within 14 days) referencing the accreditation and authorizing the contractor to store SAP material based upon the accreditation.

b. DSS (or 902nd) coordinates exceptions to contractor facility construction standards to ensure standards do not conflict with DOD 5220.22-M requirements.

c. DCID 6/9 and the provisions of paragraph 5-2 of this regulation apply to SAPs containing SCI.

7-5. Industrial security inspections

a. It is Army policy that the DSS conducts security inspections of contractors to eliminate the potential for the appearance of impropriety between the Army program office and the contractor.

b. SAPs require fully documented comprehensive security inspections of contractors by qualified Government industrial security specialists. 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 follow contract security inspection standards set by DOD 5220.22-M, the NISPOM Supplement Overprint, and the PSG.

c. SAP Government offices or proponents coordinate DSS inspections with the contractor and/or subcontractor. The SAP Government security office extracts appropriate security procedures from the NISPOM Supplement Overprint, highlights these in the SAP PSG, and provides them to the appropriately cleared DSS inspectors. SAP Government offices may attend DSS inspections only in the following cases: Initial industrial security inspection of a facility, a new contractor/subcontractor, a new industrial security representative, a new contract security officer, or a significant anticipated or unanticipated security problem. In all other cases, SAP Government offices conducting visits to contractor/subcontractor sites will conduct these visits separately from DSS inspections. SAP Government offices may conduct announced/unannounced security assistance visits with a frequency determined by the PD/PM. The SAP Government office will not conduct SAP inspections. Exceptions authorizing concurrent visits to contractor/subcontractor facilities by the SAP Government office and DSS representative will be approved/disapproved case by case by the TMO. In cases where DSS has been carved out (see 7-5*d*), the concurrent visit policy will be applied in the same manner to the alternate inspection authority.

d. Army contracts excluding DSS are carve-out contracts and must be based on compelling reasons. 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 the TMO for SA review and Deputy Secretary of Defense approval. Carve-out procedures must comply with the NISPOM Supplement Overprint, AR 380-49, and the Federal, Defense, and Army acquisition regulations. Normally, the Army does not approve carve-out requests.

(1) USAINSCOM will conduct industrial security inspections 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 USAINSCOM.

(3) When contracts no longer require carve-out status, proponents transfer the industrial security inspection responsibility to DSS and update the DD Form 254 to reflect this change. The proponent will provide a copy of the updated DD Form 254 to the TMO.

e. If it is anticipated that Army SAP material will be used or generated under a contract by a non-Army activity or at a non-Army facility, and that activity will not allow DSS to conduct the industrial security inspections, then the MOA/terms of reference must state which organization will conduct the industrial security inspections, and this must be approved by the TMO prior to entering into the arrangement. In cases where such an arrangement already exists prior to the date of this guidance, then the MOA/terms of reference must be modified to reflect the industrial security arrangements, and be submitted to the TMO for review and approval.

7-6. Contract management

a. Any contract for a SAP requiring a DD Form 254 to be completed must use secure environment contracting procedures.

b. The DCAA Field Detachment 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.

d. SAP research and development contracts and materials/supplies and services contracts will be assigned to the Defense Contract Management Agency for secure environment contract administration under the Federal Acquisition Regulation System (FARS) (48 CFR 42.2), the Defense Federal Acquisition Regulations Supplement (DFARS), and the Army Federal Acquisition Regulation Supplement (AFARS).

e. PSMs will complete and forward DD Form 254 to the contracting officer, who will then determine whether or not a contract modification will need to be accomplished in consultation with the PSM. The contracting officer forwards a copy of each completed DD Form 254, including all revisions, to the 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 incidents involving SAP information to the contractor security manager (for the SAP), who, in turn, within 24 hours reports to the DSS industrial security representative (or 902nd POC in case of carve-out status) and the PD/PM who, in turn, 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 to the program office and DSS. Contractors will report all security incidents that involve classified information, regardless of level of severity, to DSS. DSS will conduct an administrative inquiry if they determine further action is necessary, or at the request of the program office. The PSM will follow the reporting procedures in paragraph 5-9.

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 because of 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 PD/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) PSGs and SCGs outline security and classification guidance.

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

(3) SAP PSMs will prepare a DD Form 254 for each SAP-related contract. The PSM will annotate block 16 of DD Form 254, adding the TMO to the distribution, and either the PSM or the SAP PD/PM will sign the form. The PSM will then forward the completed DD Form 254 to the contracting officer who will, in consultation with the PSM, determine whether or not a contract modification is necessary.

(4) For carve-out contracts, 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 DD Form 254 stating the contract contains certain carve-out information and provides a copy of the DD Form 254 to the responsible identified USAINSCOM inspection authority and the TMO.

(5) Army SAP contracts list AR 25-2, the NISPOM Supplement Overprint, and this regulation in block 15 of DD Form 254 as documents governing accreditation of contractor's AIS.

(6) The program office conducts a review of DD Forms 254 in the following circumstances (not an inclusive list): every 2 years; a change to the SCG; a change to Army or DOD security guidance that impacts upon the guidance provided in the 254; or other reviews specified in contracting regulations. Re-issue of DD Forms 254 is not necessary

after the biennial review unless changes to any of the DD Forms 254 are required. The PSM will document the fact that the review was conducted and complete a Memorandum for the Record (retain until next review conducted). A copy of the Memorandum for the Record will be provided to all relevant contractors. In all cases of DD Form 254 revisions, the PSM provides an information copy of revisions to the TMO.

(7) The SAP PD/PM is responsible for resolving questions or issues regarding the PSG, DD Form 254, or the classification guide.

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

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

(2) Processes contractor requests for postcontract retention of classified material. Only the VCSCA can approve such requests for contractor retention of documents other than that mandated by the FAR.

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

(4) Ensures that the procedures provided in appendix H are followed.

7–9. Automated information systems

a. DSS is the DAA for contractor AIS. Contractors will prepare an accreditation package (using a format prescribed by DSS) for each AIS (to include networks) used to support Army SAP. After DSS grants accreditation for the system or network to be used to process classified information, the Government PSM must issue a SAP use authorization letter to the contractor for each system or network. The contractor is not permitted to process SAP information on any SAP AIS unless specifically authorized to do so by the PSM.

b. If conflict exists between the published guidance provided by DSS and the PSM, the TMO (through CIO/G–6) will resolve the conflict (see para 7–2*b* for additional guidance).

c. Contractor AIS connected to a Government network must be approved by both the DAA for the CIO/G–6 and the DSS. For the purpose of this paragraph, contractor AIS include workstations or contractor owned networks that are connected to any Government-owned AIS or IT network that processes SAP or sensitive data.

Chapter 8 Information Management Area

8–1. General

a. This chapter describes the essential parameters and procedures to follow to ensure the IT support provided to SAPs, sensitive activities, and agencies processing SAR information on their IT systems is secure. The IT encompasses communications, AIS, audio/visual support, records management, printing, and publications.

b. The CIO/G–6 is the Army’s executive agent for information systems support and serves as the DAA for all Army SAP AIS (excluding contractor AIS—see 7–9). The CIO/G–6 will coordinate with the DCS, G–2 on all AIS simultaneously processing SAP and SCI. Additionally, the CIO/G–6 is the DA focal point for staff management and is responsible for oversight of IT.

c. The PEO EIS–TAO provides IT support to SAPs and sensitive activities and all other agencies processing Army SAR information on their IT systems as directed by official tasking of the CIO/G–6. This support includes engineering, fabrication, installation, operation and maintenance, and life-cycle support of IT systems and components.

d. The TMO and CIO/G–6 establish SAP-specific IT policy and validate new requests for IT support. Validation of new IT support requests will include—

(1) Verification that SAP or sensitive activity is active and approved by the TMO.

(2) Assurance that an ISRP or IMSP was submitted by the requestor prior to initiating the request for IT support or the request is for development of an ISRP or IMSP.

e. CIO/G–6 approves all requests for IT support by the PEO EIS–TAO to SAPs, sensitive activities, and all other agencies processing SAR information on their IT systems.

f. All IT systems and components purchased to support SAP IT systems requirements will be approved by CIO/G–6 via the IMSP (para 8–3), the ISRP (para 8–2), or an addendum to the IMSP (para 8–3*g*).

g. Requests for IT support from PEO EIS–TAO will be sent to CIO/G–6 for approval through the TMO for validation of SAP/SA status.

h. For approved IT support requests, the PEO EIS–TAO will provide the following support:

(1) Assist PDs/PMs, commanders, or directors with development of their ISRP and/or IMSP.

(2) Provide PDs/PMs to perform or assist in acquisition and implementation of approved ISRP or IMSP IT projects.

(3) Assist PDs/PMs with identification of Information Assurance requirements and implementation of IT solutions necessary to protect SAP or sensitive activities AIS and data.

(4) Assist PDs/PMs with development of the AIS system accreditation packages.

8-2. Information systems requirements package

a. SAP activities must document initial information management support requirements (for example, secure voice, data, and facsimile systems) in an ISRP and submit it as an enclosure to the initial request for PSAP status. A suggested format for an ISRP is shown in appendix L.

b. The ISRP will be reviewed by the Chief, TMO and approved by CIO/G-6.

8-3. Information management support plan

a. Following SAP establishment, listing as a sensitive activity, or determining the requirement to process SAR information on an agency's IT systems, PDs/PMs, commanders, or agency directors will prepare a detailed IMSP. This plan should be initiated within 90 days of SAP establishment, listing as a sensitive activity, or beginning to process SAR information on an agency's IT system and should identify IT resources necessary to accomplish the assigned information mission of the program, activity, or agency for the next 5 years or throughout its anticipated life cycle if it is fewer than 5 years. The IMSP is comparable to information resource management (IRM) planning accomplished in other organizations. It provides a framework for the management, coordination, and support of IT used by a program, activity, or agency over time. It identifies challenges and opportunities for furthering the program, activity, or agency goals and objectives and charts the overall direction of IRM during the life of the program. The IMSP development process should guide IRM planning by integrating the program's activities or the agency's IRM plans, performance plans, financial management plans, and budget processes. Appendix M outlines the suggested format for the IMSP.

b. The IMSP will be formatted as two stand-alone documents. It will consist of a SAR classified document that contains an executive summary (IMSP executive summary) of the IMSP main body. The two documents will allow separation of the SAR and non-SAR data. These documents will be structured as follows:

(1) The IMSP executive summary will contain executive summaries of all the paragraphs in the main body plus any classified IT projects and the Letter of Agreement, Letter of Understanding, MOA, and/or MOUs for the SAP.

(2) The IMSP main body will contain all the detailed information of the required IT projects but will not contain any SAR information. If a SAP PDs/PM has an IT project(s) that must be classified SAR, these projects will be put in the IMSP executive summary as an appendix.

c. The IMSP will be reviewed annually to validate the appropriateness of the IT requirements based on present requirements and impacts of industry technology advances. Annual review is a process that will help PDs/PMs, commanders, or directors link IT investments directly to their missions, to achieve measurable improvements to their mission outcomes. It consists of prioritizing a list of projects by specified capital planning criteria (compliance with IT architecture, benefits, costs, performance measures, and so on) and then selecting the best mix of projects in the IMSP that maximizes the return based on the decision criteria. The process should not only give PDs/PMs, commanders, or directors a view of a particular IMSP project for a system or IRM investment, but also provide a view of systems and IRM investments that are interdependent or codependent on each other. By preparing and maintaining currency of the IMSP projects for major information systems, the PD/PM is able to monitor investments and prevent redundancy of existing or shared systems. The IMSP projects should provide information demonstrating the impact of alternative IRM investment strategies and funding levels, identify opportunities for sharing resources, and consider the program's inventory of information resources. The annual reviews will be documented and a copy provided to CIO/G-6.

d. Failure to perform annual reviews will result in the IMSP being invalidated and require the PD/PM, commander, or director to initiate a new IMSP.

e. The IMSP should draw from the ISRP (if applicable) and document present IT assets and objective IT requirements of the PDs/PMs, commanders, or directors. The IMSP will document—

(1) Present and proposed IT system architecture.

(2) Estimated cost of proposed IT projects.

(3) Management, command and control structure, personnel, and organizations.

(4) Financial management, resource management, and property accountability procedures and requirements.

(5) Information security plan.

(6) Information assurance requirements.

(7) Recommended implementation schedules for the life of the IMSP.

(8) Operations and maintenance, and integrated logistics support requirements

(9) All program support provided by external sources by listing all MOUs, Letters of Agreement, and so on.

f. The PD/PM, commander, or director is responsible for formulation and promulgation of the IMSP. Upon request and approval by CIO/G-6, in accordance with procedures contained in paragraph 8-1, the PEO EIS-TAO will provide technical advice and support to a PD/PM, commander, or director in preparing and implementing the IMSP.

g. PDs/PMs, commanders, or directors will submit the IMSP through the TMO to CIO/G-6, for validation and approval. Upon approval, the PD/PM, commander, or director will provide a final copy of the IMSP to the TMO who retains the record copy of the plan to facilitate oversight by HQDA. The TMO and CIO/G-6 will ensure that IT procured and utilized by the program, activity, or agency is reflected in the approved IMSP.

h. PDs/PMs, commanders, or directors who find it necessary to procure IT to support mission requirements not contained in their approved IMSP, will document such supplemental requirements as an addendum to their IMSP as

reflected in appendix M and provide a copy through the TMO to CIO/G-6 for approval. CIO/G-6 will return the approved addendum to the PD/PM, commander, or director for inclusion in their IMSP and provide a copy to the TMO for posting in the record copy of the IMSP.

8-4. Accreditation

a. PDs/PMs are required to have all IT that processes SAP information accredited under AR 25-2 using the Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Additionally—

(1) SAPs, sensitive activities, or other agencies processing SAR information on their IT systems will operate them in accordance with the NISPOM Supplement Overprint, chapter 8.

(2) PDs/PMs, commanders, or directors will request accreditation at the sensitivity level appropriate to the classification of the material involved. The accreditation authority for systems processing SAR information is the CIO/G-6. PDs/PMs, commanders, or directors whose IT systems simultaneously process SAR and SCI information must accredit their IT systems in accordance with DCID 6/3 using the DITSCAP. The CIO/G-6 and the DCS, G-2 are the accreditation authorities for SAR/SCI systems. All initial and revision requests should be forwarded to the CIO/G-6, who will ensure the required coordination with the DCS, G-2.

b. PDs/PMs, commanders, or directors provide a coordinated accreditation package, any coordination reports, and their recommendations to the accrediting authority, who then determines if the automated system may process SAR information. In accordance with the DITSCAP the primary accreditation authority is CIO/G-6 and the designated accreditation authority is CIO/G-6.

(1) Accreditation packages will be prepared without including SAP information and then processed through the program, activity, or agency security office to the appropriate accreditation authority. Security personnel need not be in an approved SAP billet to process this documentation.

(2) The main body of the accreditation package will be unclassified. If SAR information must be included, a SAR annex to the plan will be created and staffed through the program's normal SAR distribution channels (for example, mail).

8-5. System maintenance

a. When maintenance or programming must be performed on AIS that process SAP information, only the information assurance manager or information assurance officer for the SAP, activity, or agency may authorize the removal of system components from the automation site, to include magnetic media. Systems components that cannot be declassified will not be removed from the automation site for maintenance.

b. Programmers and maintenance personnel must have at minimum a SECRET security clearance based upon a national agency check/local agency check/credit investigation and be current within the last 5 years (see para 5-4 for requirements).

c. Programmers and maintenance personnel must—

(1) Be escorted by a program-cleared person with reasonable knowledge of the technical requirement to repair the system and oversee the nonprogram cleared technician at all times.

(2) Be a program-briefed technician from TAO; or be program briefed for the information being processed on the AIS.

(3) Be escorted by an individual defined in 8-5c when installing, performing maintenance on, and programming internal telephone switches and other devices used for signal isolation.

8-6. Information management support

a. Army SAPs, sensitive activities, and other agencies processing SAR information on their IT systems requiring IT support (as authorized in an approved ISRP or IMSP) should submit their request to the PEO EIS-TAO through the TMO and CIO/G-6. The TMO will review IT support requests to ensure that the requestor is a valid SAP or sensitive activity. The CIO/G-6 will check the IT request for conformity with an approved program IMSP/ISRP or, if appropriate, approve the use of special procedures in lieu of normal/routine support procedures. PEO EIS-TAO will redirect all tasks that are beyond the scope of an approved IMSP/ISRP to CIO/G-6 for validation and approval with information copy to the TMO.

b. Army SAPs, sensitive activities, and other agencies processing SAR information on their IT systems requiring IM support and not reflected in an approved IMSP will submit requests through the TMO for review and concurrence, to CIO/G-6 for validation and approval. Approved requests will be posted to the approved IMSP/ISRP as an appendix.

8-7. Information assurance

a. Information assurance must be addressed in each IMSP project. The SAP PD/PM must ensure that all reasonable procedures are taken to ensure the integrity of any SAR data stored on AIS. Vendors are marketing computers that include removable media devices such as CD-R, CD-RW, DVD-R, and zip drives that cost less than special-order computers without these removable storage devices; however, these devices will be disabled at the basic input/output system and operating system level on all workstations except for the minimum essential number of positions. The

number of workstations that have the ability to produce removable media containing SAR data should be limited to the maximum extent possible by the PD/PM and PSM. Additional workstations may be provided the capability to produce removable media only on a valid, justifiable mission need. The justification for additional workstations with write capability to a removable media will be included in the data IT security certification and accreditation process package for review and validation by the designated accreditation authority. Standard operating procedures will provide for other physical controls to restrict the use of removable media. The AIS standard operating procedure will provide audit procedures to document storage of all SAP data on removable media. These procedures will require at least a two-level approval before the data can be stored and removed from the SAP facility. The using organization of the IT will be required to certify in their data IT security certification and accreditation process accreditation package that these devices have been disabled on all computers except for those with an approved mission requirement. The mission requirement/justification must be included in the accreditation package. They must also have and properly implement training for personnel authorized to create removable media containing SAR data.

b. All infrared ports must be disabled and no wireless keyboards, mice, or other wireless devices will be used in the SAPF.

c. Personal data assistants, cellular telephones, data diaries, long-range cordless telephones, personally owned automated information systems, two-way pagers, two-way radios, watches with communications software, and wireless network devices will not be used in SAPFs.

d. Audit procedures must be enforced for all IT systems that process SAP data. This requirement includes stand-alone workstations as well as workstations connected to a network. The audit procedures include a requirement for review of the automated and manual audit reports for IT processing SAP data. The review procedures must be included in the DITSCAP accreditation package. These procedures will document the validation process used to ensure the audit is implemented and properly reviewed.

e. Password procedures must be established to meet length requirements. Operators will not share passwords; must use a password with two or more numbers in it; and meet all the requirements defined in AR 380-19, paragraph 2-14. These password controls will be implemented on all AIS to include standalone workstations. Systems administrators will not use a systems administration password; instead, a unique logon name and password that will reflect their action in the system audit as required above will be used.

f. Training of personnel operating and or maintaining IT that processes SAR information is critical. The SAP PD/PM is responsible for ensuring that all personnel operating and or maintaining AIS have attended all required IT training. The requirements for IT training can be found on Army Knowledge Online or <https://informationassurance.us.army.mil>.

8-8. Continuity of operations planning and business continuance planning

a. All SAP PDs/PMs will develop a continuity of operations plan that addresses protecting the SAR data stored on their AIS. The plan will address creation of backup data on removable media. The removable media must be stored at another facility that does not have a probable chance of being destroyed by the same event that could destroy the original AIS data. This requirement precludes using another building on the same post, camp, or station. The data must be stored in a facility approved and authorized to store the SAR data.

b. All SAP PDs/PMs will develop a business continuance plan that addresses how they would restore operations after a event that destroys or prevents use of their AIS. At a minimum, the plan should provide procedures for restoring the operating system of the AIS, then restoring the SAR data from the removable media stored offsite in accordance with the continuity of operations plan. It should, if appropriate, address relocation of their operation to another approved facility.

8-9. Removal of non-SAR data from systems approved to process SAR data

a. Understandably, many SAP PDs/PMs process unclassified data on their SAR AIS because they do not have both unclassified and SAR AIS. This practice is problematic in many situations to include when a SAP is disestablished and the unclassified/non-SAR information is still required. The PD/PM must request a waiver to allow removal of the unclassified/non-SAR data from the AIS before the SAR data are destroyed or archived. In cases where SAR and SCI are processed simultaneously, the CIO/G-6 will coordinate the waiver request with the DCS, G-2.

b. The waiver to remove non-SAR data from approved AIS processing SAR data must be submitted to the TMO through CIO/G-6 (the CIO/G-6 will coordinate with the DCS, G-2 in cases involving SCI). The waiver must include the formal procedures that will be used to ensure SAR data are not removed along with the non-SAR data. The CIO/G-6 will provide removal procedures and software that are technically sound and that minimize the risk of SAR data being removed along with the non-SAR data.

c. The Chief, TMO is the only approval authority for this waiver and will sign the waiver based only on assurances by the CIO/G-6 (and in cases involving SCI, the DCS, G-2) that the procedures are appropriate to minimize the risk to SAR data.

8-10. Records management

a. The PD/PM, commander, or director will determine the records that are necessary to maintain "adequate and

proper documentation" of the program, activity, or agency and its operations. PDs/PMs, commanders, or directors 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. PDs/PMs, commanders, or directors must ensure that needed records are recorded and maintained in official files. PDs/PMs, commanders, or directors 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. Design of electronic file systems will satisfy records management requirements contained in this paragraph and must be included in the approved IMSP for the program, activity, or agency. Network file servers as well as stand-alone computers should have a file directory structure that supports easy identification of the categories of records identified in paragraph 8–1c.

c. PDs/PMs, commanders, or directors will maintain their record files in accordance with AR 25–400–2. As a minimum, the SAP record file will include—

- (1) Written program approval(s) from the authority initially establishing the SAP.
- (2) Written approval for special management and special delegation procedures when they exist.
- (3) The program's annual SAP report to the SAPOC, to include both parts 1 and 2 completed in accordance with the last-issued SAPOC informational and format requirements.
- (4) The POM and the president's budget decision review of issue papers.
- (5) Budget exhibits as required under DOD 7000.14–R, vol. 2A–B.
- (6) Legislative language history on the SAP.
- (7) Identification of associated programs, if SAP is, or under an umbrella SAP.
- (8) Identification and location of prime contractor(s) and subcontractor(s) performing classified work under the SAP.
- (9) SAP access rosters (current and historical) and records of inadvertent disclosure.
- (10) Foreign disclosure case files.
- (11) Current and historical security classification guides and program security guides.
- (12) Documented inspection reports of the results of the review of each SAP under the cognizance of the Army SAPCO.

d. Archiving of SAP material is required upon disestablishment of a SAP program. When a PD/PM is preparing a SAP for disestablishment, the PD/PM must contact the TMO before developing a disestablishment concept to coordinate disposition of historical files. In addition, there are two further conditions under which a program will archive SAP material:

(1) During the life cycle of the program, when material holdings become too excessive to maintain on site. Programs should review material at least every 3 years to determine if material needs archiving.

(2) When a program is instructed to merge with another program.

e. Program will contact the TMO in any of these situations for detailed guidance on proper archiving procedures.

Chapter 9 Funding

9–1. SAP funding

a. The Army will fund only properly registered and approved SAPs. A new start is a term used when the Army is pursuing a new effort (classified or unclassified) that has not yet been appropriated by Congress. A new start may be created under the protection of an existing SAP, or may require the establishment of a new SAP. A new SAP is established when funds are placed against a program that is not new work, but requires its own security structure, has gone through the PSAP process, and has been approved by OSD as a SAP. The new SAP will be a parent program and can have additional subcompartments.

b. Before providing resources to or in support of or receiving resources from another DOD or Federal agency SAP, the Army program office must establish an MOA which meets the requirements of paragraph 4–7c and 4–7d of this regulation.

c. All Army resource documents for SAPs will be coordinated with the TMO prior to submission to OSD.

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, RDT&E, procurement, and Operation and Maintenance, Army (OMA) funds), by year, through the Future Years Defense Plan.

b. The Army Staff proponent, ASA (ALT), DCS, G–8, Army Budget Office, and ASA(FM&C) evaluate the proposed funding and management structure. The management structure must specify distinct program elements,

project codes and standard study numbers. The Army Staff proponent also assigns the program to the appropriate management decision package.

c. MACOM/PEO/PDs/PMs are prohibited from providing funds to PSAP requirements without prior written authorization of the Chief, TMO. The 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. *Annual POM/budget estimate submission.* PDs/PMs justify a continuing need to fund a program by submitting a budget estimate submission every August. The budget estimate submission identifies resources necessary to maintain the program and provides information on the prior year, current year, and the two budget years. OSD publishes guidance annually regarding the format and suspense dates for budget exhibits. The ASA (FM&C) appointed personnel will collect the information submitted from the MACOMs/PEOs. Once ASA (FM&C) has collected and assembled this data, it will be reviewed by the TMO before submission to OSD.

b. *Program budget decision.* Program budget decisions and program decision memorandums are issued between October and December, after the OSD review of the POM (budget estimate submission and Future Years Defense Plan). Using the program budget decisions, OSD proposes changes to the Army POM submission. All program budget decisions and program decision memorandums will be routed through the ASA (FM&C), DCS, G-8, and TMO. The Army then has the opportunity to submit reclaims (counterarguments) to OSD. To facilitate the preparation of these reclaims, MACOMs/PEOs provide input to appropriate Army Staff proponents who validate the input and forward reclaims through the DCS, G-8, the TMO for all funding areas, and the ASA(FM&C).

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

(1) Reprogramming requests must be evaluated in terms of DOD guidance provided in DOD 7000.14-R, vol. 3, on requirements for congressional notification and/or prior approval. If congressional notification or prior approval is required, the Undersecretary of Army will be the Army's approval authority for reprogramming. Requests en route to the Undersecretary of Army will also be reviewed by the VCSA.

(2) When Undersecretary of Army approval is not required, the Army Staff proponent can approve SAP reprogramming requests after review by the offices listed in 9-3c(3). Army Staff proponents for SAPs at HQDA are: the ASA(ALT) for acquisition SAPs, the DCS, G-2 for intelligence SAPs, and the DCS, G-3 for operations and support SAPs (reprogramming format is shown in app N.)

(3) Regardless of the approving official, all requests to reprogram SAP funds must be reviewed by: the ASA (ALT), ASA(FM&C), TMO, OTJAG, OGC, and DCS, G-8. ASA (FM&C) will ensure the reprogramming action complies with HQDA directives and DOD guidance. During the final 3 days of the fiscal year, each MACOM or PEO may reprogram up to a cumulative of \$100K of expiring SAP funds without prior coordination with the ASA (ALT), ASA(FM&C), TMO, OTJAG, OGC, and DCS, G-8. By 15 October of the following fiscal year, the MACOM and/or PEO must report all reprogrammings executed under the special \$100K provision to the Chief, TMO.

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

d. *Congressional notification.* Congressional notification is required if a reprogramming action exceeds the appropriation thresholds as stated in DOD 7000.14-R, volume 3, chapter 6, or if a project meets the definition of a "new start." All reprogramming actions or new starts requiring congressional notification must be approved by the Undersecretary of the Army. The TMO will provide the notification letter to OSD Special Programs Coordination Office, which will then notify the appropriate congressional subcommittees.

9-4. Disestablishment

When disestablishing a SAP, the MACOM/PEO prepares a disestablishment concept plan that addresses fiscal control (app H) and submits it to the TMO for approval. 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 Army Staff proponent to the TMO. The OPDUSD(A&T) provides the report format and preparation instructions in a memorandum to the Services. SAP reports cover program activities and funding requirements, and justification for continued SAP status. The TMO consolidates these SAP reports and submits them to the OPDUSD(A&T), which 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.

Chapter 10 International Special Access Programs

10-1. Purpose

This chapter provides management guidance and uniform procedures to be followed when Army SAPs participate in international sharing and functional agreements with partner nations.

10-2. International characteristics

a. International efforts. International efforts with allied or other friendly countries are an increasingly important part of U.S. national security and defense acquisition strategies. Upon approval by the SA and Secretary of Defense, Army acquisition SAPs may release SAP information as part of approved international or functional agreements with specified foreign governments or international organizations (see AR 550-51).

b. Classified military information. The disclosure or release of DA classified military information, to include SAP information, to foreign governments or international organizations may be the result of DA participation in activities stemming from international and functional agreements negotiated and concluded in accordance with applicable DOD and Army regulations (see AR 550-51).

c. Information sharing. Information sharing characterizes an association or agreement with an ally or allies in that selected U.S. SAP information is exchanged (see AR 550-51 and DODD 2040.2).

d. Cooperative programs. A cooperative program characterizes an international agreement between the United States and a foreign government for RDT&E within a specified technology area(s) or for RDT&E to develop a weapon system or component to achieve a jointly desired goal. In such a cooperative effort, some, but not all, U.S. SAP information pertaining to the technology area(s) or RDT&E development may be approved for disclosure or release to the specified government(s). All information and material jointly generated and funded pertaining to the cooperative program becomes foreground information and is available for use by all participating governments in accordance with the terms of the MOA (see AR 550-51 and DODD 2040.2).

e. Co-production programs. A co-production program is characterized by an international production agreement in which items intended for military application are jointly (between U.S. SAP and allies) produced or assembled under provisions of a formal agreement. The formal agreement will provide for transfer of build-to-print and assembly information from the U.S. SAP to a foreign government(s). In a co-production program, all U.S. SAP information pertaining to the production or assembly may be approved for disclosure or release to a specified government. All information and material jointly generated and funded pertaining to the co-production program becomes foreground information and is available for use by all participating governments in accordance with the terms of the MOA (see DODD 2040.2).

10-3. International SAP architectures

a. To facilitate the U.S. Army SAP oversight process, the following SAP architectures will be used for all information sharing, cooperative programs, and production efforts.

b. The security architecture to protect SAP data under information sharing agreements and cooperative programs will generally be protected under a subcompartment to an existing U.S. parent SAP. Under this architecture, the U.S. subcompartment will contain only the shared information and the nickname will generally be the same nickname used by the ally. The ally will not be made knowledgeable of the existence of or have access to SAP information protected by the U.S. parent SAP, other subcompartments of the SAP, or any other contributing SAPs. The security architecture will allow for the leverage of classified collateral and SAP information (background information) from other programs for use in the international effort. The architecture must also allow for the development of collateral and SAP classified information within the international effort (foreground information).

c. The security architecture to protect SAP data during co-production efforts will generally be a stand-alone U.S. SAP under which all SAP data provided to, or generated by, the co-production SAP is jointly owned, releasable, or shared with the ally or allies. The nickname assigned to this SAP will be the same nickname used by the ally or allies in accordance with the jointly developed and approved procedures for the effort. The information review team must approve data for release because the stand-alone U.S. SAP protecting the co-production may receive feeder information from other U.S. SAPs.

10-4. Information review team

As the office of primary responsibility for the project, each sponsoring U.S. SAP program office will establish an information review team. This team will consist of technical and security experts indoctrinated to all SAP information involved to review SAP information proposed for release to the allied partner(s). The information review team will perform technical and security reviews of information proposed for release, ensuring that it meets the release criteria of the applicable MOA, any executive committee guidance and the approved delegation of disclosure authority letter. The TMO will review the proposed delegation of disclosure authority letter prior to approval by the DCS, G-2. Prior to approval, the DCS, G-2 will review all proposed releases to ensure compliance with existing delegation of disclosure authority letters and executive committee guidance. The U.S. office designated as the office of primary responsibility

will develop written procedures, consistent with this regulation, providing specific instructions, guidance and security procedures to be followed by the command or agency during the information review team and foreign disclosure office review and approval process. Once developed, these procedures will be reviewed and approved by the DCS, G-2 and the TMO prior to implementation and will not be released to the allied partner(s). The allied partners will not be made aware of any contributing U.S. SAP(s) to the effort or project.

10-5. Document marking and control procedures

a. Documents submitted to the information review team for a final release determination. These will be marked in such a manner as to preclude the inadvertent or premature release of information to the ally before it is approved by the foreign disclosure office. Documents that have been reviewed and approved for release to a foreign government(s) will be clearly marked by PSMs to distinguish them from documents that have not been reviewed and/or approved for release.

b. Approval and disapproval statements. The program office will maintain records of documents that have been approved or disapproved for release; these will clearly indicate the name of the person who made the decision and the date of the decision. Documents provided to an ally will NOT display this approval/disapproval statement and signature.

c. Receipts. All documents, media, or other classified material transferred in support of an approved project will be documented on an accountability record or other form as specified in the program security instructions or MOA. Copies of signed receipts for classified material will be maintained in the office of primary responsibility local file area for a minimum of 5 years after the date of the transfer, or longer if specified by the joint program security instructions or MOA. If not otherwise specified in the program security instructions or MOA, DA Form 3964 may be used to document transfers of classified information. If another form is used it will provide—

(1) Identification of the date and the name of the individual by name and office to whom the information was provided.

(2) An unclassified description of the material, to include the control number assigned by the office of primary responsibility to the material and the format of the media used—document, 3.5-inch disk, CD, and so on.

(3) Classification of the material released.

(4) Record copies of all information and material transferred to allied partners and all documents considered but disapproved for release will be maintained in the sponsoring U.S. SAP program office. The TMO has the responsibility to maintain oversight of all SAP related foreign disclosure decisions. These files will be filed, retained, and archived in accordance with AR 25-40-2 and are subject to review during inspections and audits.

d. Classified project foreground information. Each document will be conspicuously marked or stamped at the top and bottom of the front cover and the first page and the back side of the last sheet/back cover and last page (for example, "SECRET/BIG TREE" with the following added directly under the classification marking: "BIG TREE Special Control and Access Required (SCAR) Use Only," or as directed in the program security instructions or MOA.

10-6. Classified information categories

a. As an example, the classification categories and markings used by the BIG TREE SCAR program are as follows:

(1) SECRET/BIG TREE (Equivalent country classification/BIG TREE).

(2) CONFIDENTIAL/BIG TREE (Equivalent country classification/BIG TREE).

b. As appropriate, only the first classification marking for each category (that is, SECRET and CONFIDENTIAL) will be used in the narrative portion of this annex when referring to the BIG TREE SCAR classification categories and markings outlined above.

10-7. Accessing procedures

International SAP and associated subcompartment accesses will be granted in accordance with the procedures directed by the governing program security instructions. The sponsoring U.S. Army SAP program office is responsible for recording, entering, and maintaining these accesses in the current version of the ASATS. Access to classified information under information sharing, cooperative programs, and production efforts are normally detailed in the program security instructions and governed by an approved ceiling or maximum number of individuals representing each participating country authorized to have access to SAP information under the project. The U.S. SAP office of primary responsibility, in coordination with the DCS, G-2, TMO, and SAAL-SSP (if the project is an acquisition effort), will assist the U.S. office of primary responsibility in jointly developing the U.S. access ceiling base on programmatic, security, and oversight requirements for the effort. The access ceiling is independent of the Army baseline billet structure and will account for that fact. Requests for formal billet structures will be submitted to the Chief, TMO for approval.

10-8. Project reviews, SAPOCs, inspections, and audits

U.S. Army cooperative programs, co-production, and information-sharing efforts are subject to recurring and special

inspections, audits, and reviews. Contractor facilities located in the United States involved in cooperative programs, co-production, and information-sharing possessing SAP information or material under joint efforts must possess the required DOD facility and personnel clearances. Contractor facilities in support of U.S. Army international and cooperative efforts will undergo routine, annual, and, if necessary, followup or special industrial security reviews by the DSS. DSS security review carve outs must be approved by the TMO prior to the contract award of SAP classified work at a contractor facility. The U.S. Army Program Office is required to brief information on the international efforts involving SAP data as part of the annual SAPOC process.

Appendix A References

Section I Required Publications

DOD publications are available at www.dtic.mil/whs/directives.

AR 11-2

Management Control. (Cited in para 4-5a.)

AR 25-400-2

Army Records Information Management System (ARIMS). (Cited in paras 2-22cc; 2-31f; 5-3g and l; 8-10d; and 10-5c(4).)

AR 380-5

Department of the Army Information Security Program. (Cited in paras 1-4a; 4-5f(4); 4-5j; 5-2a and d; 5-3b, g, l, j, k, and i; 5-4a; 5-9a; B-2b(3)(a); B-3d(1); and H-2c.)

AR 25-2

Information Assurance. (Cited in paras 7-8a(5) and 8-7e.)

AR 380-67

The Department of the Army Personnel Security Program. (Cited in para 5-4c.)

AR 381-2

Subversion and Espionage Directed Against US Army (SAEDA). (Cited in para 4-5f(4).)

(U) AR 381-14

Technical Counterintelligence (TCI) (S). (Cited in para 5-5a(1), 5-5b, c(3).) (Available at [/www.us.army.mil/portal/portal_home.jhtml](http://www.us.army.mil/portal/portal_home.jhtml).)

AR 530-1

Operations Security (OPSEC). (Cited in paras 4-5f(6)(d), 5-8c.)

AR 550-51

International Agreements. (Cited in 5-7 and 10-2.)

AR 715-30

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

DOD 5220.22-M

National Industrial Security Program Operating Manual. (Cited in paras 4-2a; 4-3c; 4-7j; 5-1a; 5-2c and d; 5-3b, d, g, l, and k; 5-4a; 7-2a and b; 7-3a; 7-4b; 7-5b, c, and d; 7-8a(5); and 8-4a(1).)

DOD 5220.22-M Supplement

National Industrial Security Program Operating Manual Supplement. (Cited in paras 5-7b and 7-5b and d.)

DODD 2040.2

International Transfers of Technology, Goods, Services, and Munitions, 17 January 1984. (Cited in para 10-2a and d.)

DODD 5230.20

Visits, Assignments, and Exchange of Foreign Nationals, 24 April 1992. (Cited in para 5-7b.)

(U) DODD C-5230.23

Intelligence Disclosure Policy (C). (Cited in para 5-7b.)

DODD 5530.3

International Agreements, 11 June 1987. (Cited in para 5-7b.)

DODI 4000.19

Interservice and Intergovernmental Support, 09 August 1995. (Cited in para 4-7g.)

DCID 6/3

Protecting Sensitive Compartmented Information within Information Systems. (Cited in para 8-4.) (Available at www.us.army.mil/portal/portal_home.jhtml.)

DCID 6/9

Physical Security Standards for Sensitive Compartmented Information Facilities. (Cited in paras 5-2, 5-5a(4), 7-4c, and 8-4a(2).) (Available at [/www.us.army.mil/portal/portal_home.jhtml](http://www.us.army.mil/portal/portal_home.jhtml).)

EO 12958

Classified National Security Information. (Cited in 4-1a.) (Available at www.archives.gov/federal_register/exec_orders/1995.html.)

(U) NDP-1

National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (S), October 1988, as amended. (Cited in para 5-7b.) (Available on the SIPRNET.)

National Security Agency Quarterly Publication

Information Systems Security Products and Services Catalog. (Cited in para 5-5a(1).) (Available from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC.)

NISPOM Supplement (NISPOMSUP) Overprint

DOD Overprint to the National Industrial Security Program Operating Manual Supplement (FOUO). (Cited in paras 4-3c, 4-7j, 5-1a, 5-2c, 5-3b, d, g, l(2), and k, 5-4a and b, 7-3a and b, 7-5b and d, 7-8a(5), and 8-4a(1).) (Available through the Technology Management Office, Special Access Program Central Office, 200 Army Pentagon, Rm. 2A-28, Washington, DC 20310-0200.)

40 USC 1401

Public Buildings, Property, and Works: Definitions. (Cited in para 2-17e.) (Available at <http://www.gpoaccess.gov/uscode/index.html>.)

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. DOD publications are available at www.dtic.mil/whs/directives.

AFARS

Army Federal Acquisition Regulation Supplement. (Available at http://dasapp.saalt.army.mil/Ind_base_policy/AFARS%20conformed.htm.)

AR 1-1

Planning, Programming, Budgeting and Execution System

AR 11-7

Internal Review and Audit Compliance Program

AR 20-1

Inspector General Activities and Procedures

AR 25-1

The Army Information Management

AR 25-55

The Department of the Army Freedom of Information Act Program

AR 37-47

Representation Funds of the Secretary of the Army

(U) AR 37-64

Finance and Accounting for Sensitive Mission Funding (C). (Available at www.us.army.mil/portal/portal_home.jhtml.)

AR 70-1

Acquisition Policy

AR 70-6

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

AR 70-9

Army Research Information Systems and Report

AR 71-9

Materiel Requirements

AR 195-2

Criminal Investigation Activities

AR 195-6

Department of the Army Polygraph Activities

AR 335-15

Management Information Control System

AR 380-10

Foreign Disclosure of Information and Contacts with Foreign Representatives

(U) AR 380-28

Department of the Army Special Security System (C). (Available at www.us.army.mil/portal/portal_home.jhtml.)

AR 380-40

Policy for Safeguarding and Controlling Communication Security Materiel

AR 380-49

Industrial Security Program

AR 380-53

Information Systems Security Monitoring

AR 381-10

U.S. Army Intelligence Activities

AR 381-11

Production Requirements and Threat Intelligence Support to the U.S. Army

AR 381-20

The Army Counterintelligence Program

(U) AR 381-26

Foreign Materiel Exploitation Program (S). (Available at www.us.army.mil/portal/portal_home.jhtml.)

(U) AR 381-47

U.S. Army Offensive Counterespionage Activities (S). (Available at www.us.army.mil/portal/portal_home.jhtml.)

(U) AR 381-100

Army Human Intelligence Collections Programs (S). (Available at www.us.army.mil/portal/portal_home.jhtml.)

(U) AR 381-102

U.S. Army Cover Program (S). (Available at www.us.army.mil/portal/portal_home.jhtml.)

(U) AR 381-141

Intelligence Contingency Funds (ICF) (C). (Available at www.us.army.mil/portal/portal_home.jhtml.)

(U) AR 381-143

Logistics Policies and Procedures (C). (Available at www.us.army.mil/portal/portal_home.jhtml.)

DA Pam 70-3

Army Acquisition Procedures

CJCSM 3150.29B

Codeword, Nickname, and Exercise Terms (NICKA) Systems. (Available from DOD J-2 (JS/J33/CJOD).)

DFARS

Defense Federal Acquisition Regulations Supplement. (Available at www.acq.osd.mil/dp/dars/dfars.html.)

DFAS 37-1

Finance and Accounting Policy Implementation. (Available at www.asafm.army.mil/budget/di/di.asp.)

DFAS IN Manual 37-100-FY

(Available at www.asafm.army.mil/budget/di/di.asp.)

(U) DOD S-5105.21-M-1

Sensitive Compartmented Information Administrative Security Manual (C). (Available from the Defense Intelligence Agency (DIA/DAC-2B).)

DOD 7000.14-R , vols. 2a, 2b 3, 5, and 11 (chap 1)

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

DOD 7600.7-M

Internal Audit Manual

DODD 5200.1-R

Information Security Program

DODD 5200.2-R

Personnel Security Program

DODD O-5205.7

Special Access Programs

(U) DODD S-5210.36

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

DODD 5210.48-R

DOD Polygraph Program

DODD 5230.11

Disclosure of Classified Military Information to Foreign Governments and International Organizations

DODD 5500.7

Standards of Conduct

DODI O-5205.11

Management, Administration, Oversight of DOD Special Access Programs (SAPs)

DODI 5210.74

Security of Defense Contractor Telecommunications

DODI 5505.2

Criminal Investigations of Fraud Offenses

FARS (48 CFR 52.227–10)

Filing of Patent Applications—Classified Subject Matter (Available at www.gpoaccess.gov/ecfr.)

FARS (48 CFR 200–299, Subpart 42.2)

Contract Administration. (Available at www.gpoaccess.gov/ecfr.)

Section III**Prescribed Forms**

The following forms are available on the Army Electronic Library CD-ROM and the APD Web site (www.apd.army.mil) unless otherwise stated. DD forms are available from the Office of Secretary of Defense Web site (www.dir.whs.mil).

DA Form 5750

Inadvertent Disclosure Oath. (Cited in para 5–9*d*.)

DD Form 2835

Program Access Request. (Cited in paras 6–5*c* and 6–6*a*.)

DD Form 2836

Special Access Program Indoctrination Agreement. (Cited in paras 6–6*b*, 6–6*c*(1), 6–6*c*(3), 6–6*c*(6), and 6–7*a* and *b*.)

Section IV**Referenced Forms****DA Form 11–2–R**

Management Control Evaluation Certification Statement

DA Form 3964

Classified Document Accountability Record

DD Form 254

Department of Defense Contract Security Classification Specification

DD Form 350

Individual Contracting Action Report

SF 86

Questionnaire for National Security Positions. (Available at <http://contacts.gsa.gov/webforms.nsf>.)

Appendix B

Reporting of Army Sensitive Activities—Data Call Sheets

B-1. Headers for the data call sheet part 1 chart:

- a.* Program nickname.
- b.* Codeword.
- c.* Army or Non-Army Sponsor.
- d.* Army POC (name, title, phone number, nonsecure internet protocol network and secure internet protocol network (if available), e-mail).
- e.* Nondisclosure forms required?
- f.* Central billet or knowledgeability roster maintained?
- g.* Army \$ or man-years spent on program (previous FY).
- h.* MOA or TOR?
- i.* Date of MOA or TOR.
- j.* MOA or TOR review authority?
- k.* Foreign material acquisition?
- l.* Current estimated FMA \$ values.
- m.* Type of sensitive activity if not SAP.
- n.* Type of Army involvement if not SAP.

B-2. Headers for the data call sheet part 2 chart:

- a.* Program nickname.
- b.* Secure environment contracting office.
- c.* Contract number.
- d.* Contractor name and address.
- e.* Date of contract award.
- f.* Contract length (base year + option years).
- g.* Total estimated contract amount.
- h.* Total \$ obligated to date.
- i.* DCMA utilized?
 - (1) Yes.
 - (2) No.
- j.* If DCMA utilized, preaward, postaward, or both?
- k.* DSSN & location of paying office.
- l.* Access to SCI on DD 254?
 - (1) Yes.
 - (2) No.
- m.* NISPOM options issued in the DD 254?
 - (1) Yes.
 - (2) No.
- n.* DD 254 sent to the TMO?
 - (1) Yes.
 - (2) No.
- o.* PCO, ACO, and DCAA auditor names, phone numbers, and e-mail.
- p.* Brief narrative of SAP leases.

Appendix C Program Performance and Budget Execution Review System Charts

Use the following instructions to complete the PPBERS charts (figs C-1 and C-2).

C-1. Program appropriation

Prepare a PPBERS 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 C-1).

a. Fiscal year and quarter. In the upper left-hand side of second row labeled "FY" and "QTR," enter the fiscal year and quarter under review.

b. Program nickname. In the middle of the second row, after "PGM", enter actual program nicknames. Do not use funding nicknames.

c. Program office. In the upper right-hand side of the second row labeled PROPONENT, enter the name of the program office, POC, and telephone number.

d. Current year. Directly under OVERALL PROGRAM OBJECTIVES, display bar graphs of planned and actual obligations and disbursements for current fiscal year funding. Enter the type of appropriation (that is, RDT&E, OMA, or procurement) 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.

e. Obligations and disbursements. The block directly under the bar graph labeled RESOURCE DETAILS contains cumulative amounts of OBLIGATIONS and DISBURSEMENTS, with each divided as follows:

(1) 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.

(2) PLAN (\$M). Equals the cumulative amount of funds planned for obligation. This figure does not include prior year funding carried over.

(3) ACTUAL (\$M). Reflects actual cumulative obligations and disbursements shown at the end of quarter in official accounting reports.

(4) DA GOAL (% PROG). Shows the DA goal percentage.

(5) ACTUAL (% PROG). Shows the percentage derived by dividing the actual obligations/disbursements by the total programmed amount for that fiscal year (that is, the amount shown in the resource summary block). Address all deviations as less than 10 percent in the analysis section.

f. Deviation. In the top upper right-hand corner of the chart, rate the program RED if deviation is greater than 15 percent), AMBER (deviation 10 to 15 percent), or GREEN (deviation less than 10 percent).

g. 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, closed account, and approved reprogrammings. In the upper right corner of the block, after PE, enter the appropriate number.

h. Discussion. In the ANALYSIS block, discuss—

(1) Plans for funds carried over from the previous fiscal year.

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

(a) Disbursements. Brief comments to support issues:

1. Disbursements not reported by DFAS: \$

2. Not recorded or erroneously posted disbursements DFAS: \$

3. Invoices and billings not yet paid by DFAS: \$

4. Unit has not submitted acceptance/receiving report to DFAS: \$

5. Work performed or goods received but not yet billed: \$

6. Total unreported disbursements and accruals: \$

(b) Combined disbursements and accruals. \$

(3) What unresolved issues remain.

(4) Difference between appropriated and programmed amounts (that is, small business innovation research, closed account, and reprogrammings).

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

(6) Date of the last audit (DAIG, DOD IG, AAA, and so forth).

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

C-2. Procurement funds

Prepare a separate PBBERS chart for procurement funds. Enter the same data as shown on the RDT&E sample PBBERS chart (figure C-1). Because 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.

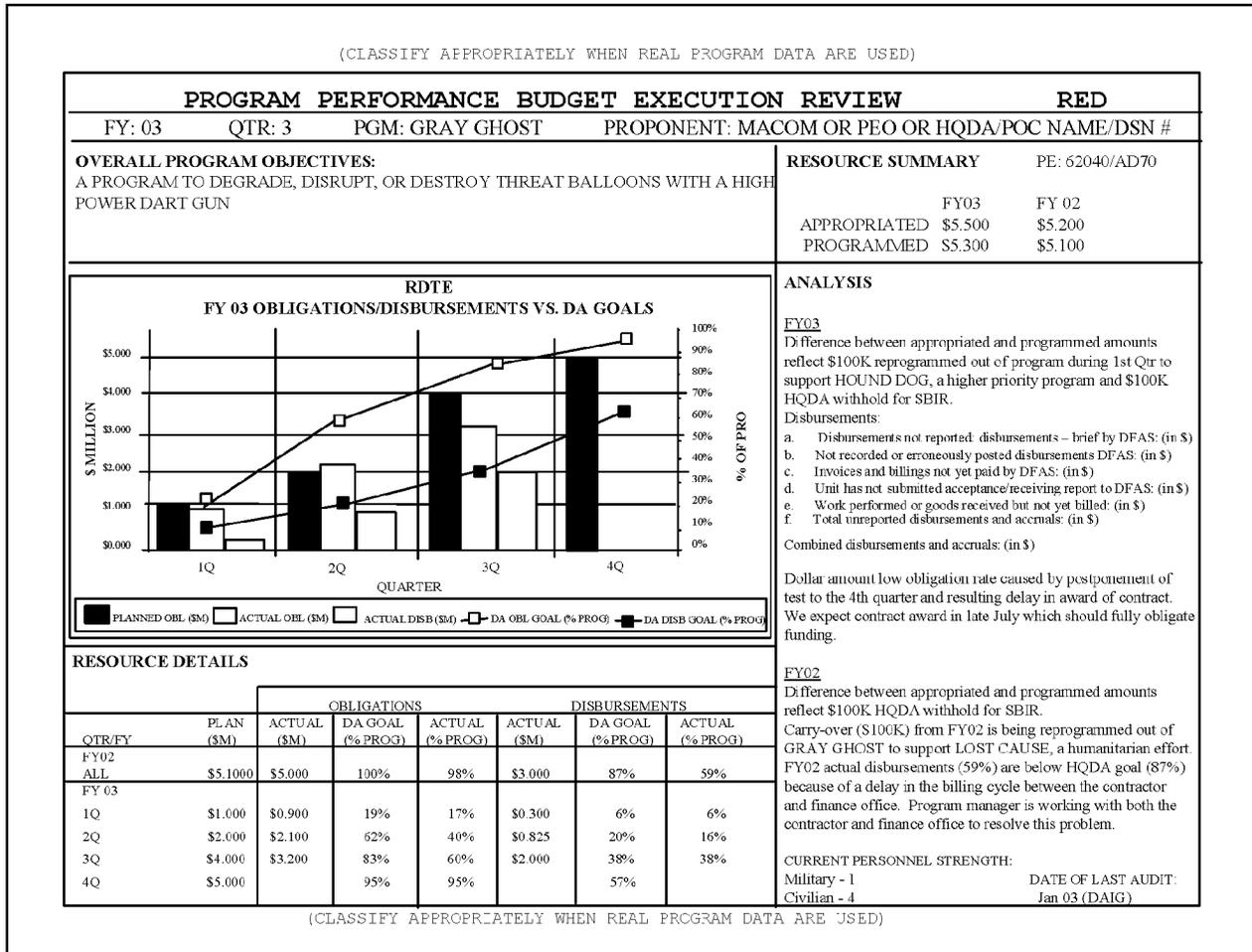
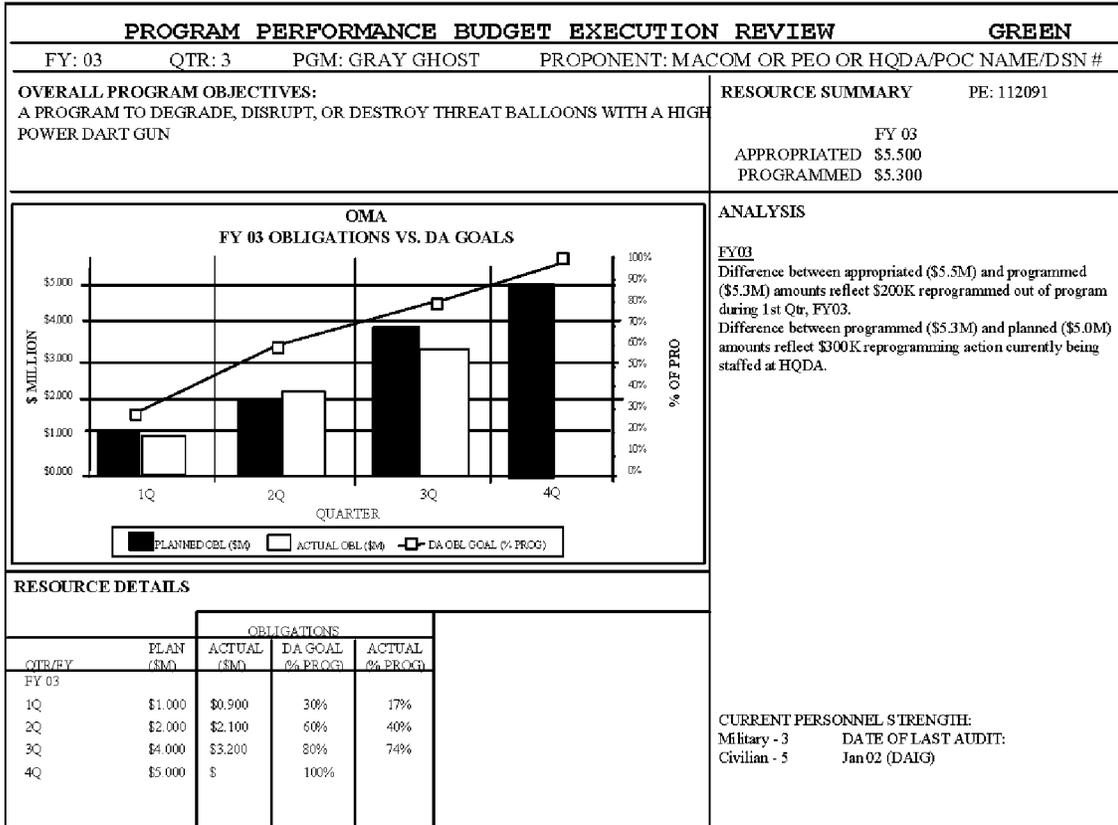


Figure C-1. RDT&E PBBERS chart

(CLASSIFY APPROPRIATELY WHEN REAL PROGRAM DATA ARE USED)



(CLASSIFY APPROPRIATELY WHEN REAL PROGRAM DATA ARE USED)

Figure C-2. PBBERS chart for procurement fund

Appendix D

Guidance on Preparing the Standard QUAD Chart Slide

The following is guidance to be used to prepare the standard QUAD Chart Slide for the POM/budget estimate submission and the annual SAP report (the TMO maintains the most current format).

D-1. Upper left-hand side

a. This should show photo/line drawing/artist sketch of the item being developed. If a technology, provide an illustration of the technology application. An explanatory caption may be included.

b. "A picture is worth a thousand words."

D-2. Upper right-hand side

a. Insert program status.

b. Show important issues affecting program status or progress.

D-3. Lower left-hand side

a. Insert brief program description. What is it? Where is the program going? What need does it fill? Why is it a SAP?

b. List the major points and successes or problems.

D-4. Lower right-hand side

a. At a minimum, include the current fiscal year and the next two fiscal years.

b. Include most recent or next (whichever is closer) milestone or Defense Acquisition Board level review.

c. Fiscal year total includes all types of funds (research and development, procurement, operations and maintenance, and so forth).

d. Schedule bars should be accurate to the month if possible.

D-5. Format instructions

a. Generate a slide using PowerPoint (or other presentation) software.

b. Slide should be formatted using the SAPOC slide format as a guide (see fig D-1).

ENTER CLASSIFICATION HERE (18PT ARIAL BOLD RED)

<p>PICTURE</p>	<p>STATUS - ISSUES (ARIAL 14 PT BOLD)</p> <ul style="list-style-type: none"> * BULLETS FORMAT (ARIAL 12 PT NORMAL) * BRIEF STATUS SUMMARY * IMPORTANT ISSUES * BULLETS IN YELLOW 																																								
<p>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) * ITEM1 * ITEM2 * BULETS IN YELLOW 	<p>BUDGET AND SCHEDULE (ARIAL 14PT BOLD RED)</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="text-align: left;">TASK</th> <th>FY XX</th> <th>FY XX</th> <th>FY XX</th> </tr> </thead> <tbody> <tr> <td>GO AHEAD</td> <td colspan="3">▲</td> </tr> <tr> <td>DESIGN/FAB</td> <td colspan="3">■</td> </tr> <tr> <td>INTEG/TEST</td> <td colspan="3">■</td> </tr> <tr> <td>DEPLOY</td> <td colspan="2">■</td> <td>▲</td> </tr> <tr> <td>COMPLETE</td> <td colspan="3">▲</td> </tr> <tr> <td>R/D/E</td> <td></td> <td></td> <td></td> </tr> <tr> <td>CPA</td> <td></td> <td></td> <td></td> </tr> <tr> <td>OMA</td> <td></td> <td></td> <td></td> </tr> <tr> <td>TOTAL</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	TASK	FY XX	FY XX	FY XX	GO AHEAD	▲			DESIGN/FAB	■			INTEG/TEST	■			DEPLOY	■		▲	COMPLETE	▲			R/D/E				CPA				OMA				TOTAL			
TASK	FY XX	FY XX	FY XX																																						
GO AHEAD	▲																																								
DESIGN/FAB	■																																								
INTEG/TEST	■																																								
DEPLOY	■		▲																																						
COMPLETE	▲																																								
R/D/E																																									
CPA																																									
OMA																																									
TOTAL																																									

ENTER CLASSIFICATION HERE (18PT ARIAL BOLD RED)

Figure D-1. Sample slide format for Standard QUAD chart slide

Appendix E Establishment

E-1. Establishment of checklist/timeline

Table E-1 is a list of the major events required to establish a SAP.

Table E-1 SAP establishment timeline	
Day	Event
0	Memo requesting PSAP status and draft security plan sent to TMO
15	PSAP memo staffed within HQDA
40	TMO approves PSAP and dispatches PSAP approval memo request for SAP establishment memo given. Knowledgeability roster started
60	Proponent submission of proposed structure and manning proposal to USAFMSA for preliminary validation
100	Final security plan, billet structure (waived programs), draft SAPOC briefing slides, and request to establish SAP memo to TMO
120	USAFMSA manpower report submitted
130	TMO conducts working SAPOC
160	HQDA SAPOC meets
180	TMO submits SAPOC paperwork to OSD
220	Deputy Secretary of Defense approves SAP
TBD	OSD submits notification letters to Congress
TBD+30	SAP can obligate funds

E-2. Format for requesting establishment of a prospective SAP

a. The proponent submits a request to establish a PSAP in the format shown below through the chain of command to the 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) of the program that 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) PD/PM (address and phone).

(c) PSM (address and phone).

E-3. Format for requesting establishment of a SAP

The proponent submits a request to establish a SAP to the TMO in the format 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 that cannot be adequately protected under the provisions of AR 380-5 and reasons why collateral measures are inadequate.

(2) Multidiscipline CI 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 SCG, security procedures guide, OPSEC Plan, billet structure, and program indoctrination briefing).
- g.* Key program personnel (include address and phone numbers).
 - (1) PD/PM.
 - (2) PSM.
 - (3) Contracting office and its location.
- h.* ISRP.
- i.* Any MOAs (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 military occupational specialty/job series.
- m.* Agency POC (position or title, address, and telephone number).

Appendix F Format for Working SAPOC Slides

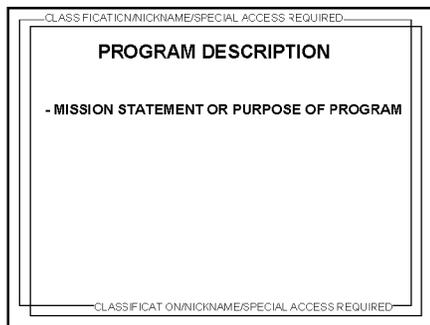
Working SAPOC charts will be submitted in the following format (fig F-1, slides 1-37). Programs will not modify the format. SAPOC charts will be created from slides submitted from WSAPOC. WSAPOC slides will be submitted to the TMO on electronic media a minimum of 5 working days prior to the scheduled Working SAPOC date.

Slide 1



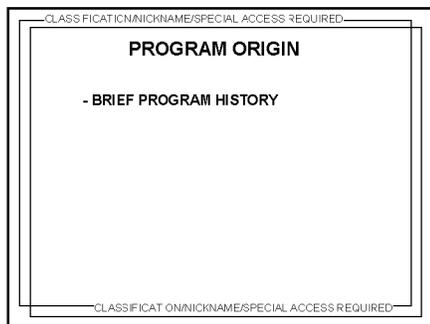
Example cover slide indicating program name. Insert applicable “Derived from” and “Declass” instruction information in bottom left corner. Ensure all slides are properly marked with security classification. Applies to all SAPs.

Slide 2



Applies to all SAPs. Insert applicable mission/purpose information.

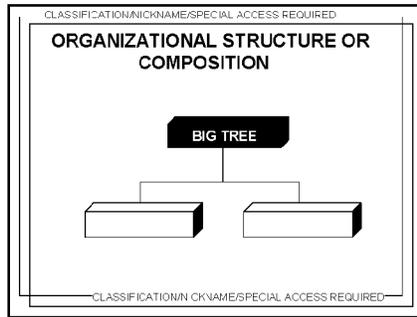
Slide 3



Applies to all SAPs. Insert applicable information regarding history. Acquisition SAPs may include *significant* recent program accomplishments.

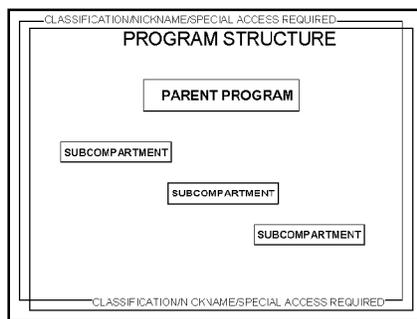
Figure F-1. Formats for Working SAPOC charts, slides 1-37

Slide 4



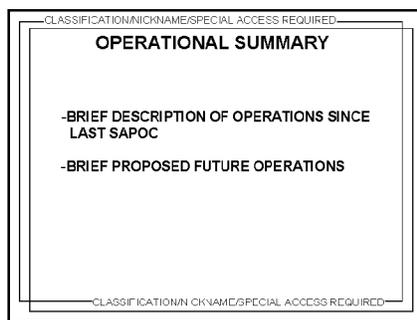
Example slide. Applies to operations and intelligence SAPs only. Provide applicable program and subcompartment names.

Slide 5



Applies to acquisition SAPs only. A follow-on slide for each subcompartment will follow. On each subcompartment slide include a description of the technology and content. Include photo/concept sketch of technology or embedded video on each subcompartment slide, as appropriate.

Slide 6



Applies to operations and intelligence SAPs only. Multiple slides may be required with pictures to convey the message.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 7

—CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED—

JUSTIFICATION FOR SAP PROTECTION

- WHAT REQUIRES PROTECTION
- SECURITY OBJECTIVE

—CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED—

Applies to all SAPs. Insert applicable justification information.

Slide 8

—CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED—

CRITICAL ELEMENTS

—CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED—

Applies to all SAPs. Should include bulletized comments discussing critical elements of SAP. Majority (not necessarily all) information should come from program SCG (not a duplicate of previous slide—ensure discrimination is made between critical elements and justification for SAP protection).

Slide 9

—CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED—

RELATIONSHIP TO OTHER PROGRAMS

- RELATIONSHIP WITH OTHER DOD AND FEDERAL AGENCIES CONDUCTING SAP OR SAP-LIKE WORK
- TYPE OF WORK BEING CONDUCTED AND/OR SHARED

—CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED—

Applies to all SAPs. Insert applicable information and/or organizational diagram reflecting relationship(s).

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 10

CLASSIFICATION/NAME/SPECIAL ACCESS REQ. REF.

FOREIGN TARGETS & TECHNOLOGY

- WHAT ADVERSARY SYSTEMS THE PROGRAM IS DESIGNED TO ATTACK
- ANY FOREIGN INTEREST/PROGRESS IN SIMILAR TECHNOLOGY
- WHAT ADVERSARY SYSTEMS WOULD ATTACK THE U.S. SYSTEM
- WHAT COUNTERMEASURES THE ADVERSARY WOULD USE AGAINST THE U.S. SYSTEM

CLASS F. CAT. OMNICKNAME/SPECIAL ACCESS REQUIRED

To be completed by DCS, G-2. Insert applicable information.

Slide 11

CLASSIFICATION/NAME/SPECIAL ACCESS REQ. REF.

CI SUPPORT HIGHLIGHTS

CLASS F. CAT. OMNICKNAME/SPECIAL ACCESS REQUIRED

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information regarding events that occurred since last SAPOC.

Slide 12

CLASSIFICATION/NAME/SPECIAL ACCESS REQ. REF.

PROGRAM VULNERABILITIES

CLASS F. CAT. OMNICKNAME/SPECIAL ACCESS REQUIRED

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 13

A rectangular chart template with a double-line border. At the top center, it reads "FIS THREAT". At the top and bottom edges, there is a small text label: "CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED".

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information.

Slide 14

A rectangular chart template with a double-line border. At the top center, it reads "EXTERNAL THREATS". Below this, there is a list of categories: "- HUMINT", "- SIGINT", "- IMINT", "- MASINT", and "- OTHER". At the top and bottom edges, there is a small text label: "CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED".

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information.

Slide 15

A rectangular chart template with a double-line border. At the top center, it reads "SECURITY INCIDENTS". At the top and bottom edges, there is a small text label: "CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED".

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information regarding events that occurred since last SAPOC.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 16

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

G-2 ASSESSMENT

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

This slide template features a double-line border. The top border contains the text 'CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED'. The center of the slide is dominated by the bolded title 'G-2 ASSESSMENT'. The bottom border also contains the text 'CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED'.

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information.

Slide 17

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

G-2 RECOMMENDATION

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

This slide template features a double-line border. The top border contains the text 'CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED'. The center of the slide is dominated by the bolded title 'G-2 RECOMMENDATION'. The bottom border also contains the text 'CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED'.

Example slide to be completed by HQDA, DCS, G-2. Applies to all SAPs. Input applicable information.

Slide 18

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

CONTRACTOR TRENDS

- AIS
- INFORMATION
- PHYSICAL
- CONTRACT

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

This slide template features a double-line border. The top border contains the text 'CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED'. The center of the slide is dominated by the bolded title 'CONTRACTOR TRENDS'. Below the title is a bulleted list with four items: '- AIS', '- INFORMATION', '- PHYSICAL', and '- CONTRACT'. The bottom border also contains the text 'CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED'.

The following three example slides are to be completed by DSS. They apply to all SAPs. Use one slide (with continuation slide if necessary) to input applicable information. Consolidate slides if possible.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 19

CLASSIFICATION/CRNAME/SPECIAL ACCESS REQUIRED

FUNCTIONAL & POLICY ISSUES

CLASSIFICATION/CRNAME/SPECIAL ACCESS REQUIRED

Example slide to be completed by DSS. Applies to all SAPs. Input applicable information.

Slide 20

CLASSIFICATION/CRNAME/SPECIAL ACCESS REQUIRED

RECOMMENDATIONS/SOLUTIONS

CLASSIFICATION/CRNAME/SPECIAL ACCESS REQUIRED

Example slide to be completed by DSS. Applies to all SAPs. Input applicable information.

Slide 21

CLASSIFICATION/CRNAME/SPECIAL ACCESS REQUIRED

SECURITY MANAGEMENT

PROGRAM SECURITY GUIDANCE

	<u>Effective Date</u>	<u>Review Date</u>
Security Class Guides	06 Jul 00	Jul 02
Security Procedures Guide	17 Aug 00	Aug 02
OPSEC Annex/Treaty Plan	18 Aug 00	Aug 02

WAIVERS TO ARMY/DOD POLICIES AND REGULATIONS:
NONE

CLASSIFICATION/CRNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Input appropriate dates as applicable. List waivers to all Army/DOD policies and regulations if appropriate. If none, so state.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 22

ACCESS AND SECURITY STATUS	
Total Personnel Access Ceiling (PAC)	
• Approved Structure (Mar 01)	500
Total Number with Access – (Not including baseline)	
• Previous Year	450
• This Year	475
• Percent +/-	+ 5.55%
ACA: MG Smith, Command Name	
Access Approval Authorities: PEO AMD: MG Jones	

Example slide. Applies to all SAPs. Input appropriate numbers and information as applicable. Ensure all access approval authorities are listed by command name.

Slide 23

SAP INSPECTIONS, AUDITS & REVIEWS		
AGENCY	DATE	RESULTS
AAA	May 00	SAT – 1 Finding
DAIG (Fin Mgmt)	May 01	SAT – 5 Recommendations
CIP Program	Jul 01	SAT – No findings
Monthly 10% Inventories	Jun 00 - Present	No discrepancies
Program 100% TS Inventory	May 00	No discrepancies

Example slide. Applies to all SAPs. Fill in dates and results of inspections as applicable.

Slide 24

SECURITY MANAGEMENT		
ASATS DATABASE RECONCILIATION		
Total # accessed to program	# Debriefed since last SAPOC	% Change since last SAPOC
800	92/14	.4%
SAP DEBRIEFINGS		
# Debriefings concluded since last SAPOC	# Of admin debriefs executed since last SAPOC	% Of admin debriefings to total # of debriefings
600	100	6.0%

Example slide. Applies to all SAPs. Input all numbers as applicable.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 25

CLASSIFICATION: (U) (N) (C) (S) (P) (A) (S) (R) (D) (J) (R) (D)

FUNDING PROFILE

Funding (FY03 BES - \$ in Millions)

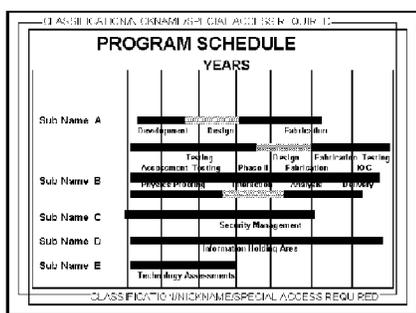
Program Line	Prior	01	02	03	04	05	06	07
511111DC11 (6.3)	50.0	0.0						
511101A01 (5.4)	20.0	0.0	1.0					
300000V530 (6.5)	20.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
300000PA	0.0	0.0	0.0	1.0	1.0	1.0	1.5	1.0
Other	100.0							
TOTAL	400.0	1.0	2.0	2.0	2.0	2.0	2.5	2.0

• DERF Funding FY02
• RAPT Funding FY02

CLASSIFICATION: (U) (N) (C) (S) (P) (A) (S) (R) (D) (J) (R) (D)

Example slide. Applies to all SAPs. List all cumulative prior year funding, funding in year prior to current year, current year funding, and funding for current year plus one, current year plus two, and so on, through current year plus six. Include other funding sources as applicable. List all reimbursable dollars from other programs or activities.

Slide 26



Example slide. Applies to all SAPs. List significant events, milestones, transitions by subcompartment across current POM cycle. Format does not have to fit this exact template, but should include required information.

Slide 27

CLASSIFICATION: (U) (N) (C) (S) (P) (A) (S) (R) (D) (J) (R) (D)

MANPOWER PROFILE

Officers	3
Warrant Officers	1
Enlisted	0
DA Civilians	4
<u>Contractor (On-Site)</u>	<u>15</u>
Total	23

NOTE

- USAFMER Manpower Survey - Dec 00
- USAFMER Manpower Revisited - Mar 01 & Jan 02
- No change in FY 00 authorizations
- USAFMER Manpower Review - 21 Feb 02

CLASSIFICATION: (U) (N) (C) (S) (P) (A) (S) (R) (D) (J) (R) (D)

Example slide. Applies to all SAPs. Includes personnel assigned and matrixed in support. List date and results of last manpower survey/review in note section as applicable. List in notes section how many positions are reimbursable from any other activity.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 28

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

CONTRACTING

<u>Contracting Offices</u>	<u>Officers</u>
• Command, Installation	Ms. Smith
<u>Contractors</u>	
• Raytheon	
• General Dynamics	
• Lockheed-Martin	
• Rockwell Collins	
There are no carve out contracts	

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. List supporting contracting office(s), contracting officer(s), and contractors. State if there are carve out contracts (or not).

Slide 29

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

SECURITY COMPLIANCE INSPECTIONS

<u>SAP Contractor Facilities</u>	<u>Last DSS Review/Status</u>	<u>DSS Cognizance</u>
SAE-Fairfax, VA (00000-000-00)	Nov 01/SAT	Yes
Lockheed - Wash D.C. 0000-00-00	Jan 00/SAT	No

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. List contractor facilities, last DSS review/status, and DSS cognizance as applicable.

Slide 30

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

INSPECTIONS, AUDITS & REVIEWS

SAP Inspections and Audits (Gov't)

<u>Most Recent</u>	<u>Date/Results</u>	<u>Next Inspection</u>
DAIG	Apr 00 / FIX-IT	May 02
AAA (Fin Mgmt)	Jan 01 / Pending	Unknown

Fix-it Status

<u>Finding #</u>	<u>Status</u>	<u>Est Closure Date</u>
IG 3111	Closed	
IG 3113	Open	1 st Qtr FY 02
IG 3114	Closed	
IG 3115	Closed	
IG 3119	Closed	

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Insert applicable information. Use continuation page(s) as required.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 31

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

**INSPECTIONS, AUDITS
& REVIEWS - Cont**

Agreements

TYPE	AGENCY	Date Signed	Last Review
MOA	NSA	10 Jul 98	Jan 02
MOA	DOS	27 Jul 99	26 Jan 00
MOA	USAF	2 Oct 98	Draft
MOA	DOE	10 Feb 00	Feb 02
CUA	USAF Program A	17 Feb 98	24 Mar 01
CUA	Army Program N	6 Apr 00	24 Mar 01
CUA	DARPA	24 Jan 99	24 Mar 01

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Insert information pertaining to MOA and co-utilization agreements. Use continuation page(s) as required.

Slide 32

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

**AUTOMATED INFORMATION SYSTEM
(AIS) STATUS**

	DATE
• IMSP	
• Approval Date	13 Mar 98
• Review/Update	Feb 01 (Annually)
• AIS Accreditation – Re-Accredited	
• Unclass. System	11 Dec 01
• Secret Collateral Systems	11 Dec 01
• Secret SAR systems	11 Dec 01
• TS/SCI	N/A
• TS/SAR	N/A
• DASIS/ASATS Fielding	
• Conversion Date	N/A
• Point-to-Point VTC System	
• Interim Approval to Operate	N/A

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Insert applicable dates/information.

Slide 33

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

WEB SITE SECURITY REVIEW

• Is ref made, either directly or indirectly of your program on any web site?	Yes
• Date web-site created (ASA[AL T])	Undated
• Date last security review	11 Oct 01
• Key data added within the past 12 months	Web Site modification to the Mission Statement – Done Mar 00 – OP-SEC concerns

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Insert applicable information.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Slide 34

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

PROGRAM MANAGEMENT

• ARCHIVING STATUS

Archived Since Last SAPOC	Estimated Submission For Next Archive/Date	Estimated Archiving Completion Date
None	None	N/A

• PATENT / SUBMISSIONS & REVIEWS: None

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Insert applicable number(s) and date(s).

Slide 35

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

ISSUES / PROBLEMS

SECURITY:

PROGRAMATIC:

FUNDING:

LEGAL:

CONTRACTING:

TECHNICAL:

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example slide. Applies to all SAPs. Insert applicable information or NONE as applicable.

Slide 36

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

DECISION SOUGHT

Revalidate BIG TREE as an Acquisition SAP

CLASSIFICATION/NICKNAME/SPECIAL ACCESS REQUIRED

Example decision (final) slide. Input applicable program name and type (acquisition, intelligence, operations and support) of SAP.

Figure F-1. Formats for Working SAPOC charts, slides 1-37—Continued

Appendix G
Fix-It Status Sheet

Figure G-1 is an example of a fix-it status sheet.

UNCLASSIFIED

3189 CATEGORY: Financial Management LEAD: AMC

PROGRAM: WHITE CLOUD

INSPECTION DATE: May 2002

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 percent.

RECOMMENDATION (s): That the PM institute a joint review program with servicing DFAS center determine why disbursing rates are not meeting DA goals.

STATUS: 13-14 JUL 2002 UNRESOLVED. Narrative follows.

STATUS: 12 OCT 2002 UNRESOLVED. Narrative follows.

STATUS: 25 JAN 2003 RESOLVED. Narrative follows. (Closed working fix-it 25 Jan 03.)

NOTES:

1. DAIG will assign finding numbers for their findings; the TMO will assign numbers for all other findings.
2. The category will be one of the following choices:
 - a. Program management
 - b. Contract management
 - c. Command and control
 - d. Financial management
 - e. Security management
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.
5. Lead will be the action agency as identified by the inspecting/auditing organization.
6. Narrative will be a description of actions taken thus far to resolve the finding.

UNCLASSIFIED

Figure G-1. Sample fix-it status sheet

Appendix H Disestablishment Concept Plan

H-1. Format

There is no prescribed format for the disestablishment concept plan.

H-2. Content

Plans must provide detailed information with respect to timelines and suspense dates. Each disestablishment concept plan must address the following:

- a. What is the basis/rationale for disestablishment?
- b. What are the fiscal controls for contractor close out and termination costs? What are the fiscal controls for funds not obligated and funds obligated but not disbursed? What are the fiscal controls for transfer and control of prior year accounting records?
- c. What is the disposition of SAP records and files? What is the disposition of AIS media (both Government and Contract) will be in accordance with AR 380-5?
- d. What is the disposition of any Government-owned property, both Government-furnished equipment and equipment purchased by vendors?
- e. What is the recommendation on security level of remaining program, if any (collateral, incorporated into another SAP, unclassified, and so forth)?
- f. What are the legal considerations?
- g. How is coordination implemented with the appropriate Army Staff proponent, DCS, G-2, DSS, and TMO to ensure new security guidance is applied to any related DOD program?
- h. How are debriefings to be handled and the number of individuals to be debriefed along with a proposed timeline for those debriefings?
- i. How are documents to be remarked?
- j. What are the contracting considerations? How are close out and final contract payments reconciled with funds obligated in accounting records?

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

- k. What is the disestablishment timeline with critical events highlighted?
- l. What is the plan for all international program information, AIS, or equipment?
- m. What arrangements have been made for inspections by the DAIG, DSS/USAINSCOM, DCAA, and other applicable organizations (with TMO oversight assistance)?

H-3. Disestablishment timeline

This table shows the timeline for disestablishment of an Army SAP.

Table H-3
SAP component disestablishment timeline

Special access program		Subcompartment (individual)	
Day	Event	Day	Event
-90	MACOM/PEO sends memo requesting disestablishment to the TMO for staffing/approval.	-30 to -90 (see event comments)	MACOM/PEO sends memo requesting disestablishment to the TMO for staffing/approval. If closure of subcompartment will change the mission or scope of the parent, must follow timeline for SAP Parent.
-60	The TMO returns memo w/ approval to MACOM/PEO for execution with a no later than date.	0	The TMO returns memo w/ approval to MACOM/PEO for execution with a no later than date.
-30	Executive SAPOC requesting disestablishment. SAPOC (thru TMO) forwards recommendation to SA.	60	Program is closed out and inspected. MACOM/PEO sends certification letter to TMO that disestablishment actions specified in appendix I have been accomplished.
0	SA recommendation to OSD, Deputy Secretary of Defense for decision. Deputy Secretary of Defense forwards recommendation to Congress.		

Table H-3
SAP component disestablishment timeline—Continued

Special access program		Subcompartment (individual)	
Day	Event	Day	Event
14	If no objection from Congress, the TMO notifies Army Staff, MACOM, and PEO that disestablishment has been approved; program commences disestablishment.		
180	Program is closed out and inspected. MACOM/PEO sends certification letter to the TMO that disestablishment actions specified in appendix I have been accomplished.		

Appendix I Disestablishment Certification Checklist

I-1. Checklist

MACOMs/PEOs and PDs/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.* Letters of agreement and expenditure authorization documents for special mission funds or intelligence contingency funds 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/USAINSCOM notified and DSS/USAINSCOM has performed contractor closeout inspections in accordance with the disestablishment plan.
- 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.* CIO/G-6 contacted for IT disestablishment procedures.

I-2. Certification memorandum

In coordination with USAINSCOM, after the MACOM/PEO certifies that disestablishment is complete, the PDs/PMs will forward a memorandum through the chain of command to the TMO specifying all actions specified in the disestablishment plan are complete.

Appendix J

Format for Automated Information System Incident Checklist

J-1. Security incident checklist

Use the AIS security incident checklist to document each step taken by personnel discovering an AIS SAP related incident.

- a. Name of person reporting incident.
- b. Date.
- c. Type of incident (circle one):
 - (1) Data Spillage
 - (2) E-mail.
 - (3) Briefing.
 - (4) Memo.
 - (5) Spread Sheet.
- d. Date and time of incident.
- f. On what network did the incident occur (circle all that apply)?
 - (1) NIPERNET.
 - (2) SIPERNET.
 - (3) TS/SC.
 - (4) Wireless E-mail.
- g. What is the classification of the information?
- h. Who was the originator?
- i. What was the subject line?
- j. Who is the data owner?
- k. When was the PSM/PD/PM notified?
- l. Was a risk assessment conducted?
 - (1) Yes.
 - (2) No.
- m. When was the covering agent notified?
- n. Who is the covering agent?
- o. When was the DCS, G-2 notified?
- p. When was TMO security notified?
- q. When was SAP chain notified?
- r. When was the information system manager notified?
- s. Who were all the recipients of the document?
- t. When was the network taken offline?
- u. What tools were used to sanitize the system?
- v. Was backup material sanitized?
 - (1) Yes.
 - (2) No.
- w. Were infected hardware labeled and serial numbered for tracking purposes?
 - (1) Yes.
 - (2) No.
- x. List the hardware and associated serial numbers.

J-2. Completed report

PSM will maintain the completed report until the hardware has been degaussed in accordance with the NISPOM Supplement Overprint program is declassified.

Appendix K Procedures for Handling Security Incidents

When an Army AIS is inadvertently contaminated with SAP data, the following procedures will be taken.

K-1. Unauthorized access

Individuals not authorized access to SAP information who discover any documents, e-mails, briefings, and so on that contains information with SAP markings or is believed to be SAP information will contact their unit security manager immediately. Within 24 hours, the unit security manager will contact the DCS, G-2 and TMO security. The DCS, G-2 will notify the respective PD/PM and/or PSM who will ensure that the procedures outlined in this guidance are followed. Individuals within the SAP community will immediately notify the SAP PSM or the PD/PM of the incident. The PSM/PD/PM will review the data to validate that the information in question is SAP material. Do not delete e-mail or documents in question until directed by the PSM and do not allow access to the workstation or storage site to any non-SAP-briefed personnel. After an incident has occurred and a decision (see para 5-9c) has been made that a piece of hardware is permitted for continued use—

a. A unique sticker/label will be created and affixed in a conspicuous location that identifies the piece of hardware is permitted for use in its current environment and classification level but needs to receive special handling for disposal.

b. Immediately notify local information system managers to cease operation on affected systems until all SAP data has been removed from the network. The information system manager will take the following actions (documenting each step for later review by security personnel):

(1) Isolate affected hardware and label with appropriate classification marking until sanitizing efforts are complete. This will include both the workstation of the individual reporting the incident and all network servers associated with that workstation.

(2) Disable the exchange (or follow-on generation software package) accounts of the sender and all recipients of e-mail (and verify status of any blind courtesy copies sent) related information.

K-2. Level of compromise

a. Incident occurrence on unclassified net. The information system manager will—

(1) Immediately cease all operations on the network until source and destination of information is determined.

(2) Isolate affected hardware.

(3) Determine level of material sent over system. If material is TS or SCI caveated, remove hardware and control in accordance with DCID 6/9 procedures. If material level is collateral SECRET, run word search program for key words provided by the PSM.

(4) Sanitize the system in accordance with procedures listed in K-3 and K-4.

(5) Record the serial number of the cleaned hardware. Maintain internal log of hardware location to ensure hardware is never released outside of Army channels. Prior to release outside of Army channels, hardware must be degaussed in accordance with the NISPOM Supplement Overprint.

b. Incident occurrence on SECRET net (SIPERNET). The information security manager will—

(1) Immediately cease all operations on the network until source and destination of information is determined.

(2) Isolate affected hardware.

(3) Determine level of material sent over system and run word search program. If material is TS or SCI caveated, remove hardware and control in accordance with DCID 6/9 procedures.

(4) Sanitize the system in accordance with procedures listed in K-3 and K-4.

(5) Record serial number of cleaned hardware. Maintain internal log of hardware location to ensure hardware is never released outside of Army channels. Prior to release outside of Army channels, hardware must be degaussed in accordance with the NISPOM Supplement Overprint.

c. Incident occurrence on TS/SCI net. Follow procedures outlined in DCID 6/9.

K-3. Clean-up activities

These involve the inspection of each machine to determine if it has been contaminated, sanitization of each workstation and hardware involved, and re-inspecting each machine to verify effectiveness of the sanitization process. Procedures for sanitizing workstations:

a. The information security manager (timing is case specific) will—

(1) Visit the user(s) who discovered and received the SAP related document.

(2) Conduct a word search of the individual workstations C drive to ensure document is not resident on the individual workstation.

(3) Search any additional drives connected to the workstation for the relevant document(s).

(4) For e-mail violation search the individual workstations for the following:

(5) Check outlook profile for personal folders.

(6) Search for .PST files on all local drives. If personal folders exist, scan them and ensure that the offending message/data are not present. If the offending message/data are found, the hard drive needs to be pulled and sanitized.

b. Check to see if Auto Archive is enabled. If Auto Archive is enabled, document the location of the Auto Archive file and scan it for the offending message/data.

c. Check to see if work offline is enabled. If work offline is enabled, document the file location of .OST. Search local drives for .OST file. Document the modified date of all .OST files found. If the modify date of the .OST file is on or after the date of the incident the hard drive needs to be pulled and sanitized.

d. Ensure no rule exists to forward e-mail; from Outlook, click on the user's mailbox and go to Tools, Out of Office Assistant (search for rules).

e. Check mail forwarding on the server side; check for Alternate Recipients.

K-4. Action on affected servers

The following procedures will be accomplished on all affected servers. The tools listed are recommended, but are not the only tools available. Check with CIO/G-6 for the latest recommend tools. The information security manager will—

a. Process for sanitizing the server.

(1) Install On Track Power Controls 1.0 and Ultra Wipe on the exchange server where the receiving mailbox of the offending message/data resides.

(2) Search for the phrase of the offending message/data using Power Controls software. The exchange server must be stopped to search for the phrase.

(3) Stop unnecessary services to speed up the search process.

(4) If an instance of the message/data is found, start the exchange services and delete the message from its location.

(5) Defragment the information store of the exchange server by running the following command:
C:\exchsrvr\bin\eseutil/d/tE:\TempPriv.edb/ispriv.

(6) Run Ultra Wipe and delete all free space on the Server.

(7) Scan information store again for the phrase (if an instance of the message is found repeat preceding steps).

b. Process for sanitizing the backup media.

(1) Remove backup media from storage and wipe clean of all data.

(2) Reformat media and verify all previous information has been removed.

(3) Assign a serial number or other tracking number (for example, label) to the media and place back in service.

(4) When media is finally removed from service dispose of in accordance with national security requirements.

K-5. Wireless e-mail devices (Blackberry)

These are primarily used for processing information at the unclassified and FOUO level, therefore the recommended response to an incident involving classified information is to destroy the device in accordance with NISPOM Supplement Overprint procedures for hardware and software destruction. Any inadvertent processing of SAP information requires the following immediate action:

a. Immediately notify the PSM or the PD/PM of the incident. The PSM/PD/PM will review the data to validate that the information in question is SAP material. Do not delete e-mail or documents in question until directed by the PSM and do not allow access to the wireless device to any non-SAP personnel.

b. Immediately notify local information system managers, who will take the following actions:

(1) Isolate the affected hardware and label with appropriate classification marking until sanitizing efforts are complete.

(2) Disable the exchange accounts of the sender and all recipients of e-mail related information.

c. Document each step taken.

d. Removal of specific e-mail from Blackberry devices (see para K-5). The information system manager will—

(1) After receiving permission from the PSM, delete the e-mail from the Blackberry device.

(2) Open the Desktop manager and place the device in the cradle. If prompted to perform "automatic backup," click "NO".

(3) Open "Backup and Restore" utility within the Desktop Manager.

(4) Click "Backup" to backup ALL the handheld databases. The e-mail that was deleted will not be saved in the backup. Note the name and location of the backup file.

(5) When the backup is completed, close the Desktop Manager completely.

(6) Open a command prompt and switch to the directory containing the programmer.exe application, which comes bundled with the Blackberry version 2.1 software developers kit. You may need to specify the serial port. Run the following command: C:\Program Files\Research in Motion\Blackberry Handheld SDY 2.1\tools\programmer nuke.

(7) When the "nuke" program is completed, restart the Desktop Manager and open "Application Loader" utility.

(8) Follow the install wizard to reinstall the operating system and any applications desired.

(9) Finally, to restore the user's data, go into the "Backup and Restore" utility again, and this time select "Restore." When the file dialog box appears, be sure to select the correct backup file.

(10) Maintain a log of the serial number and return device to the user. Serial numbers must be maintained to ensure the device is not released outside of Army channels prior to degaussing the device in accordance with the NISPOM Supplement Overprint.

K-6. Incident reporting

For incident reporting, see paragraph 5-9. For additional guidance for AIS incidents, see appendix J.

Appendix L

Format for Information Systems Requirements Package

Use the following format when preparing an ISRP.

L-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.

L-2. Scope of requirement

Hardware/software specifications for information systems.

L-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.

L-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.

L-5. Security management

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

L-6. Funding

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

L-7. Procurement

Concept for procurement of information systems.

L-8. Accountability

Describe the concept for property accountability.

L-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 communications security material/equipment, the supporting communications security account number(s), name, address, and telephone number(s) of communications security custodian(s).
- f.* Resource requirements, engineering, fabrication, installation, operations, training, and maintenance necessary to provide service.

Appendix M

Format for an Information Management Support Plan

Use the format for IMSP to identify the finite information management requirements of a SAP or sensitive activity. The clarity provided in the IMSP merely amplifies the information management requirements generally referred to in the IMSP (see para 8-4). Prepare the plan in the following format.

M-1. Executive summary

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

M-2. Main body

- a. *Purpose.* Summarize the proponent's requirements.
- b. *System description.* Describe, in detail, the general system, network, facilities, equipment, services, and support required, both for current and future proposed system(s), to satisfy the proponent's requirements.
- c. *Technical analysis and cost estimates.* Provide a technical analysis of future IT systems, including a cost estimate covering five fiscal years and an annual estimate for sustaining operations and maintenance over the life cycle of the project.
- d. *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.
- e. *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.
- f. *Resource management.*
 - (1) *Manpower.* Determine the realistic and prudent manpower requirements to support the IS initiative throughout its life cycle.
 - (2) *Material.* Indicate the material required to support the project and identify issues and details relevant to the acquisition and implementation of the project.
 - (3) *Funds.* Indicate the methodologies to be applied against the project, to include estimated cost(s) of proposed IT projects.
- g. *Security.*
 - (1) Note billets and access.
 - (2) Describe, in detail, the information systems security concept.
- h. *Operations security.* Describe the security plan for the project's information systems.
- i. *Architecture and configuration management.*
 - (1) Identify systems, networks, and equipment fielded to ensure compatibility with the Army information architecture.
 - (2) Establish an information systems configuration control board and procedures for controlling changes, enhancements, and system upgrades.
 - (3) Identify a configuration control manager for the information systems project.
- j. *Project implementation.* Describe how the information systems project will be implemented over initial, expanded, and final phases and how the project will be prioritized by phase.
- k. *Operations and maintenance.* Identify roles, relationships, and responsibilities concerning the operation and maintenance of the information systems, networks, and equipment.
- l. *MOA/interservice support agreements.* Indicate any MOA/ interservice support agreements that would be required to effectively execute the project.
- m. *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.
- n. *Property accountability.* Provide details on how accountability of project equipment and material is maintained.
- o. *Service/support agreements.* Provide listing by type (Letter of Agreement, MOA, MOU, and so on) that provides as a minimum the effective dates, brief description of the services/support provided or obtained, the parties signing the document, and its classification.
- p. *Approvals and coordination.* After the proponent has developed the IMSP, the IMSP is submitted via SAP channels through the MACOM or PEO, through the TMO, to CIO/G-6 for approval. Following approval, CIO/G-6 may task USACECOM-TAO to provide information system support.

Appendix N
Reprogramming Request Format

Figure N-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 (U)
(CLASSIFICATION)—ACTION MEMORANDUM

1. (U) Purpose: To obtain Under Secretary of the Army approval to reprogram \$100K of expiring FY2004 funds from RED DOG to SHOWTIME. The enclosure provides a justification for the reprogramming and a current funding profile.
2. Discussion:
 - a. (U) These funds are available for reprogramming because of contract termination. Attached at the enclosure is a request from RED DOG to reprogram FY2004 (OMA, OPA, RDTE, and so on) funds in the amount of \$100K to SHOWTIME. Enclosure 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.
 - c. For obligation to occur before end of fiscal year, reprogramming must be completed on or before 15 September 2004.
3. Recommendation: That the Under Secretary of the Army approve the reprogramming request.

XXX

Colonel, GS
Chief, Transformation and Technologies

Figure N-1. Sample reprogramming request

Encl

COORDINATION:

MACOM Resource Manager	<u>Signature</u>	Date <u>2 Aug 2004</u>
ARSTAF/PEO Principal	<u>Signature</u>	Date <u>5 Aug 2004</u>
DAMO-FD	<u>Signature</u>	Date <u>12 Aug 2004</u>
Appropriate Director	<u>Signature</u>	Date <u>26 Aug 2004</u>
ASA(FM)	<u>Signature</u>	Date <u>1 Sept 2004</u>
DCS, G-8	<u>Signature</u>	Date <u>7 Sept 2004</u>

Under Secretary of the Army	<u>Signature</u>	_____	_____
Decision	Approved	Disapproved	Date

Figure N-1. Sample reprogramming request—Continued

Appendix O Management Control Evaluation Checklist

O-1. Function

Use this management control evaluation checklist for SAPs, AR 380-381.

O-2. Purpose

Use of this checklist assists MACOM commanders, PEOs, and PDs/PMs in their key management controls. It is not intended to cover all controls.

O-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).

O-4. Test questions

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

a. SAP Management.

- (1) Has the Army SAPOC recommended the program for SAP status?
- (2) Has the Secretary of Defense or the Deputy Secretary of Defense approved the program for SAP status?
- (3) Does the PD/PM have a copy of the SAP approval document?
- (4) Have manpower authorizations been validated by the DCS, G-3 within the past 12 months?
- (5) Is the program's nickname and subcompartment nicknames or code words, if appropriate, assigned by the TMO?
- (6) Is the SAP revalidation approval briefing presented annually to the SAPOC?

b. SAP Security Management.

- (1) Are the program's security measures commensurate with the program's category level (under provisions of 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, SCG, and OPSEC plan?
- (4) Are 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 approve the SCG?
- (7) Does the program have required CI documentation to include a CI vulnerability assessment, CI support plan, and technical services plan (when required)?
- (8) Has the ACA identified in writing all access approval authorities for the program?
- (9) Do all access approval authorities have a listing of their duties and responsibilities?

c. Secure environment contracting.

- (1) Do vendors have adequate protection for SAP material?
- (2) Has the DD Form 254 been forwarded to the TMO and DSS?
- (3) If a patent contains SAP information, was FARS (48 CFR 52.227-10) included in the contract?
- (4) Did the vendor forward the proposed patent through the procuring contracting officer to the SAP PD/PM?
- (5) Did the PD/PM forward the patent filing information through HQDA, ASA (ALT), ATTN: SAAL-SO, to the TMO for VCSA approval?

d. Financial management.

- (1) Does the program report accurate information to the HQDA SAP PPBERS committee?
- (2) Are all reprogrammed funds approved by the Under Secretary of the Army or by the Army Staff proponent?
- (3) Are the program's SAP funding nicknames assigned by the TMO?
- (4) Does the program prepare and submit a congressional descriptive summary annually?
- (5) Are annual budgets submitted to support timely receipt of funding for program operations?

e. Audits and inspections.

- (1) Has the PD/PM coordinated with the supporting IRAC office to ensure SAP is included in the command's auditable entity file?
- (2) Has an IRAC auditor reviewed the management control plan annual assurance statement for SAP considerations?
- (3) Do auditors have program access to conduct reviews?
- (4) Has the SAP had an AAA audit or DAIG 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. Information systems and SAP records management.

(1) Is the program IMSP current and has it been submitted through the TMO for approval by CIO/G-6?

(2) Are the program's AIS accredited?

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

(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?

g. Property accountability.

(1) Has the program acquired accountable or reportable property in support of the SAP and has that property been accounted for and reported in accordance with existing regulatory guidance governing property accountability?

(2) If the program is being disestablished, has the program secured disposition instructions for previously accountable and/or reportable material acquired during the life of the program?

O-5. Supersession

This checklist replaces the checklists for management controls previously published in AR 380-81, dated 12 October 1998.

O-6. Comments

Help make this a better tool for evaluating management controls. Submit comment to Office, Chief of Staff of the Army, TMO (DACS-ZDV-TMO), 200 Army Pentagon, Washington, DC 20310-0200.

Glossary

Section I Abbreviations

AAA

Army Audit Agency

ACA

Access control authority

ACCM

Alternative compensatory control measure

AIS

Automated information systems

AMC

Army Materiel Command

AR

Army regulation

ASATS

Army Special Access Tracking System

ASA(ALT)

Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASA(FM&C)

Assistant Secretary of the Army (Financial Management and Comptroller)

ASA(M&RA)

Assistant Secretary for Manpower and Reserve Affairs

ASEP

Army SAP Enterprise Portal

CG

Commanding general

CI

Counterintelligence

CID

Criminal Investigation Division

CIO/G-6

Chief information officer, G-6

CLL

Chief of Legislative Liaison

CSA

Chief of Staff, Army

CTTA

Certified TEMPEST Technical Authority

DA

Department of the Army

DAA

Designated accrediting authority

DAIG

Department of the Army Inspector General

DCAA

Defense Contract Audit Agency

DCID

Director, Central Intelligence Directives

DCS, G-1

Deputy Chief of Staff, G-1

DCS, G-2

Deputy Chief of Staff, G-2

DCS, G-3

Deputy Chief of Staff, G-3

DCS, G-4

Deputy Chief of Staff, G-4

DCS, G-6

Deputy Chief of Staff, G-6

DCS, G-8

Deputy Chief of Staff, G-8

DFAS

Defense Finance and Accounting Service

DITSCAP

Defense Information Technology Security Certification and Accreditation Process

DOD

Department of Defense

DODD

Department of Defense Directive

DODI

Department of Defense Instruction

DODIG

Department of Defense Inspector General

DSS

Defense Security Service

DTIC

Defense Technical Information Center

EIS-TAO

Enterprise Information Systems—Technology Applications Office

EO

Executive Order

FAR

Federal Acquisition Regulation

FIU

Field investigative unit

FOIA

Freedom of Information Act

GAO

General Accounting Office

GSA

General Services Administration

HQ

Headquarters

HQDA

Headquarters, Department of the Army

IMSP

Information management support plan

IRAC

Internal review and audit compliance

IRM

information resource management

ISRP

Information Systems Requirements Package

IT

Information technology

MACOM

Major Army command

MOA

Memorandum of Agreement

MOU

Memorandum of Understanding

NISPOM

National Industrial Security Program Operating Manual

ODUSD(P)(PS)

Office of the Deputy Under Secretary of Defense (Policy) (Policy Support)

OMA

Operation and Maintenance, Army

OPDUSD (A&T)

Office of the Principal Deputy Under Secretary of Defense (Acquisition and Technology)

OPSEC

Operations security

OSD

Office of the Secretary of Defense

PAC

Personnel access ceiling

PD

Program director

PEO

Program executive office(r)

PM

Program manager

POC

Point of contact

POM

Program objective memorandum

PPBERS

Program Performance and Budget Execution Review System

PSAP

Prospective special access program

PSG

Program security guide

PSM

Program security manager

RDT&E

Research, development, test, and evaluation

SA

Secretary of the Army

SAAL–SSP

Secretary of the Army, Acquisition, Logistics, and Technology—Systems Special Programs

SAP

Special access program

SAPCO

Special Access Program Coordination Office (OSD)

SAPF

Special access program facility

SAPOC

Special Access Program Oversight Committee

SAR

Special access required

SCAR

Special control and access required

SCG

Security classification guide

SCI

Sensitive compartmented information

SES

Senior Executive Service

SIRT

Security incident response team

SRO

Special Review Office

TAO

Technology applications office

TDA

Tables of distribution and allowances

TJAG

The Judge Advocate General

TMO

Technology Management Office

TRADOC

U.S. Army Training and Doctrine Command

TRC

Technical review committee

TSCM

Technical surveillance countermeasures

USACE

U.S. Corps of Engineers

USACIDC

U.S. Army Criminal Investigation Division Command

USAFMSA

U.S. Army Force Management Support Agency

USAINSCOM

U.S. Army Intelligence and Security Command

USASMDC

U.S. Army Space and Missile Defense Command

VCSA

Vice Chief of Staff, Army

Section II**Terms****Acquisition SAP**

A special access program established primarily to protect sensitive RDT&E or procurement activities in support of sensitive military and intelligence requirements.

Alternative compensatory control measures (ACCMs)

Used to safeguard sensitive intelligence or operations and support information (acquisition programs do not qualify) when normal measures are insufficient to achieve strict need-to-know controls, and where SAP controls are not required.

Carve-out contracts

Contracts that support Army SAP requirements, which exclude DSS from performing contractor industrial security inspections.

Classified national security information

Information classified in accordance with EO 12958, as amended by EO 13292, 25 March 03, that could reasonably be expected to cause damage to national security if disclosed outside official Government channels.

Collateral information

Classified information that can be adequately safeguarded using the ordinary security measures outlined in AR 380–5.

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—

- a. Program access nondisclosure agreements (read-on statements).
- b. Specific officials authorized to determine "need to know" (ACA/access approval authority).
- c. Nicknames/codewords for program identification.
- d. Special access required markings.
- e. Program billet structure.
- f. Access roster.
- g. Use of cover.
- h. Use of special mission funds or procedures.
- i. Use of a SAP facility/vault.
- j. Use of a dedicated SAP security manager.
- k. Any other security measure beyond those required to protect collateral
- l. information in accordance with AR 380–5.

Foreground information

All information and material jointly generated and funded pertaining to the cooperative program. This information is available for use by all participating governments in accordance with the terms of an MOA.

Intelligence SAP

A SAP established primarily to protect the planning and execution of especially sensitive intelligence or CI operations or collection activities.

Operations and support SAP

A SAP established to protect the planning for, execution of, and support to especially sensitive military operations. An operations and support SAP may protect organizations, property, operational concepts, plans, or activities.

Program executive office—enterprise information systems (PEO–EIS)

The PEO responsible for developing, acquiring, and deploying tactical and nontactical IT systems and communications for the Army (examples include transportation, medical, personnel, and supply automated tracking and communications systems).

Security compromise

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

Security incident

A security compromise, infraction, or violation.

Security infraction

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

Security violation

Any incident involving the loss, compromise, or suspected compromise of classified information.

Sensitive activities

Programs that restrict personnel access, such as ACC measures; sensitive support to other Federal agencies; clandestine or covert operational or intelligence activities; sensitive research, development, acquisition, or contracting activities; special activities; and other activities excluded from normal staff review and oversight because of restrictions on access to information.

Sensitive compartmented information (SCI)

Classified information that can be protected only with security measures authorized by AR 380–28.

Special access programs (SAPS)

A security program established under the provisions of EO 12958 and approved by the Deputy Secretary of Defense to apply extraordinary security measures to protect extremely sensitive information. SAP status is defined by DODD 5200.1–R. Army SAPS include SAPS sponsored by others but for which the Army is designated executive agent.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 053596-000