



# Department of Defense MANUAL

NUMBER 5205.07, Volume 2

November 24, 2015

Incorporating Change 2, Effective October 30, 2020

---

---

USD(I&S)

SUBJECT: Special Access Program (SAP) Security Manual: Personnel Security

References: See Enclosure 1

## 1. PURPOSE

a. Manual. This manual is composed of several volumes, each containing its own purpose. The purpose of the overall manual, in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), is to implement policy established in DoDD 5205.07 (Reference (b)), assign responsibilities, and provide security procedures for DoD SAP information.

b. Volume. This volume:

(1) Assigns responsibilities and provides procedures for personnel security for DoD SAPs.

(2) Incorporates and cancels Under Secretary of Defense for Intelligence Memorandum (Reference (c)).

## 2. APPLICABILITY. This volume applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this volume as the "DoD Components").

b. All DoD Component contractors and consultants that require access to DoD SAPs pursuant to the terms and conditions of their contract or agreement.

c. Non-DoD U.S. Government departments, activities, agencies, and all other organizational entities that require access to DoD SAPs pursuant to the terms and conditions of a memorandum of agreement or other interagency agreement established with the DoD.

d. Nothing in this manual will be construed to impair the DoD Inspector General's ability to carry out its responsibilities, as delineated in DoD Directive 5106.01 (Reference (d)), pursuant to the Inspector General Act of 1978, as amended (Reference (e)).

3. POLICY. It is DoD policy, in accordance with Reference (b), that DoD SAPs be established and maintained when absolutely necessary to protect the most sensitive DoD capabilities, information, technologies, and operations or when required by statute.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosures 3 through 5.

6. RELEASABILITY. **Cleared for public release**. This volume is available on the Directives Division Website at <https://www.esd.whs.mil/DD/>.

7. SUMMARY OF CHANGE 2. This administrative change:

a. Updates the title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92 (Reference (f)).

b. Updates references.

8. EFFECTIVE DATE. This volume is effective November 24, 2015.



Marcel Lettre  
Acting Under Secretary of Defense  
for Intelligence

#### Enclosures

1. References
2. Responsibilities
3. Personnel Security Information
4. Special Access Program Nomination Process (SAPNP)
5. Foreign Travel Reporting

#### Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....6

    UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY  
    (USD(I&S)).....6

    DIRECTOR, DEFENSE SECURITY SERVICE (DSS).....6

    CHIEF MANAGEMENT OFFICER (CMO) OF THE DEPARTMENT OF DEFENSE .....6

    DoD COMPONENTS HEADS AND OSD PRINCIPAL STAFF ASSISTANTS (PSAS)  
    WITH COGNIZANT AUTHORITY (CA) AND OVERSIGHT AUTHORITY (OA)  
    OVER SAPS .....6

    DIRECTOR, DoD SAPCO.....6

    DIRECTORS, CA SAPCO.....7

ENCLOSURE 3: PERSONNEL SECURITY INFORMATION .....8

    INTRODUCTION .....8

    SAP RECIPROCITY .....9

    PERSONNEL SECURITY ROLES .....9

        Requestors.....9

        SPOs.....9

        PSOs.....9

        AAAs .....10

        PSOs, GSSOs, Contractor Program Security Officers (CPSO), or SPOs.....10

    INDOCTRINATION BRIEFINGS .....10

    POLYGRAPHS .....11

    BILLET MANAGEMENT.....11

    PERSONNEL SECURITY FILES .....11

    CONGRESSIONAL ACCESS REQUIREMENTS .....12

    INDIVIDUAL REPORTING REQUIREMENTS .....12

        Potentially Disqualifying Information .....12

        Foreign Travel.....12

        Security Incidents.....12

        Reportable Contacts, Activities, Indicators, and Behaviors .....12

    GSSO AND CPSO REPORTING REQUIREMENTS .....13

        Employees Desiring Not to Perform on SAP Activities.....13

        Employees Refusing to Sign a SAPIA.....13

        Change in Employee Status .....13

    DEPLOYED OR TEMPORARILY REASSIGNED PERSONNEL .....13

    TOA .....13

    DEBRIEFING ACKNOWLEDGEMENTS .....13

    ADMINISTRATIVE DEBRIEFINGS .....15

    SAP ACCESS SUSPENSION AND REVOCATION .....15

ENCLOSURE 4: SPECIAL ACCESS PROGRAM NOMINATION PROCESS (SAPNP) .....17

    INTRODUCTION .....17

    NOMINATION REQUIREMENTS.....17

    NOMINATION PACKAGES .....18

    NOMINATION REVIEW PROCESS.....18

    CONTINUED ELIGIBILITY.....19

    DISAPPROVALS.....20

ENCLOSURE 5: FOREIGN TRAVEL REPORTING .....21

    GENERAL.....21

    OFFICIAL GOVERNMENT BUSINESS TRAVEL.....21

    NON-OFFICIAL TRAVEL.....22

    INDIVIDUALS ASSIGNED TO FOREIGN COUNTRIES.....23

    FOREIGN TRAVEL RECORDS.....23

GLOSSARY .....24

    PART I: ABBREVIATIONS AND ACRONYMS .....24

    PART II: DEFINITIONS.....25

TABLE

    PRE-SCREENING QUESTIONNAIRE .....17

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended
- (b) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended
- (c) Under Secretary of Defense for Intelligence Memorandum, "Special Access Program Nomination Process," May 20, 2013 (hereby cancelled)
- (d) DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, as amended
- (e) Inspector General Act of 1978, as amended, Title 5, United States Code Appendix (v)
- (f) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019
- (g) DoD Instruction 3305.13, "DoD Security Education, Training, and Certification," February 13, 2014, as amended
- (h) DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019
- (i) Executive Order 12968, "Access to Classified Information," August 2, 1995
- (j) DoD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures," August 12, 2010, as amended
- (k) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013, as amended
- (l) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017
- (m) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended
- (n) Title 18, United States Code
- (o) Title 50, United States Code
- (p) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended
- (q) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S) coordinates with the Director, DoD Special Access Program Central Office (SAPCO) to assist in the development of procedures for engagement with a DoD adjudications facility to request the facility's rationale for approving any condition, deviation, or waiver associated with an individual nominated for access to a DoD SAP.
  
2. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I&S) and in addition to the responsibilities in section 4 of this enclosure, the Director, DSS, conducts SAP training and education in accordance with Reference (b) and DoD Instruction 3305.13 (Reference (g)).
  
3. CHIEF MANAGEMENT OFFICER (CMO) OF THE DEPARTMENT OF DEFENSE. The CMO, through the Director, DoD Consolidated Adjudications Facility (CAF):
  - a. Upon request, provides rationale for any condition, deviation, or waiver associated with a nominated individual's clearance in accordance with the DoD SAPCO procedures.
  
  - b. Reviews previously unreported derogatory information in accordance with Enclosure 4 of this volume to evaluate continued clearance eligibility for individuals nominated or accessed to DoD SAP.
  
4. DoD COMPONENT HEADS AND OSD PRINCIPAL STAFF ASSISTANTS (PSAs) WITH COGNIZANT AUTHORITY (CA) AND OVERSIGHT AUTHORITY (OA) OVER SAPs. The DoD Component heads and OSD PSAs with CA and OA over SAPs implement the procedures in this volume.
  
5. DIRECTOR, DoD SAPCO. Under the authority, direction, and control of the Deputy Secretary of Defense, the Director, DoD SAPCO:
  - a. Verifies that the personnel security process and training implemented by the CA and OA SAPCOs meet the standards of this volume.
  
  - b. In coordination with the USD(I&S), develops procedures for engagement with the DoD adjudications facility to request the facility's rationale for approving any condition, deviation, or waiver associated with a nominated individual's clearance.

6. DIRECTORS, CA SAPCO. Under the authority, direction and control of their respective DoD Component heads, the Directors, CA SAPCO:

- a. Exercise access approval authority (AAA) and delegate AAA, when necessary, as determined by the DoD Component head consistent with Reference (b).
- b. Exercise AAA for nominated individuals who do not meet the nomination and eligibility criteria described in Enclosure 4 of this volume.
- c. Designate personnel who may contact and provide information to the appropriate DoD adjudications facility.
- d. Evaluate information contained in a letter of compelling need (LOCN).
- e. Formally appoint individuals to serve as Special Access Program Personnel Security Officials (SPOs).

ENCLOSURE 3

PERSONNEL SECURITY INFORMATION

1. INTRODUCTION

- a. All requests for SAP access must be processed as prescribed in this volume.
- b. Nominated individuals who meet the requirements of Enclosure 4 of this volume are eligible for SAP access without further review.
- c. AAAs may disapprove the nomination based upon the individual's failure to possess the access eligibility requirements, need to know (NTK), lack of material contribution to the SAP, or based on unique risk assessment to the program. Requestors may resubmit with additional justification.
- d. Acceptable types of clearances and investigations for SAP access:
  - (1) A SECRET SAP requires a minimum of a final SECRET clearance based upon either a National Agency Check with Law and Credit, or an Access National Agency Check and Inquiries or equivalent investigation, current within 5 years.
  - (2) A TOP SECRET SAP requires a final TOP SECRET clearance based on a Single Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), or a Phased Periodic Reinvestigation or equivalent investigation current within 5 years.
- e. If a nominated individual with current SAP access is outside the 5-year investigative scope, the individual will retain SAP access provided that:
  - (1) No potentially disqualifying information exists.
  - (2) The request for periodic reinvestigation reflects as 'submitted' in the DoD system of records for security clearances within 5 years of the closed date of the last completed investigation.
- f. Potentially disqualifying information not previously reported will be assessed by the program security officer (PSO) or SPO, as appropriate.
- g. A LOCN must accompany a nomination request for individuals who do not meet criteria described in Enclosure 4 of this volume. The LOCN will describe the individual's unique skills or knowledge and the benefit the SAP will gain by accessing the individual. By listing the unique skills and knowledge, the LOCN should reflect clearly why no other individual can fulfill or is readily available to fulfill that position. The requestor will validate that a detailed justification is included in the LOCN before including it in the nomination package.



h. Nomination packages and associated personnel security databases must be administered and maintained in accordance with DoD Instruction (DoDI) 5400.11 (Reference (h)). Only individuals whose duties include conducting nominated individual's reviews for access may view information contained in nomination packages.

## 2. SAP RECIPROCITY

a. A nominated individual with an existing DoD SAP access will not be denied access eligibility to a DoD SAP, or subsequent SAP, of the same sensitivity level provided they:

- (1) Have validated NTK and can materially contribute to the new SAP.
- (2) Have no new potentially disqualifying information.
- (3) Meet nomination requirements for SAP access.
- (4) Have all 'NO' responses on a Pre-Screening Questionnaire dated within the past 365 days.

b. A reciprocity determination for a nominated individual may only be granted when he/she has received a favorable eligibility determination from another access-granting organization. Copies of all such approvals by the CA SAPCO must be maintained with the individual's record of SAP access and be made readily available for review as necessary. This data will be captured and made a part of the individual's record in the component's system of record for SAP access.

## 3. PERSONNEL SECURITY ROLES

a. Requestors. Requestors will:

- (1) Be accessed to the SAP for which the nominated individual is being submitted.
- (2) Fill out the justification section of the Program Access Request (PAR). The justification will address why access is required by establishing NTK and the nominated individual's material contribution to the SAP.

b. SPOs. SPOs will:

- (1) Be responsible for the completeness and accuracy of information submitted in nominated individual's packages.
- (2) Make initial eligibility determination and, or recommendation in accordance with Enclosure 4 of this volume.

c. PSOs. PSOs will:

(1) Evaluate SPO's access eligibility recommendation, any additional information the nominated individual provides to "yes" answers on their Pre-Screening Questionnaire, and concurs or non-concurs with access to the SAP by the nominated individual. All non-concur recommendations for accesses require additional justification in the PAR remarks section or must be provided in a separate memorandum.

(2) Assess unique risks with all eligibility issues and coordinate with the respective counterintelligence (CI) support activity or the appropriate DoD adjudications facility, as necessary.

(3) Review the SAP nomination package and make an access recommendation to the AAA.

d. AAAs. AAAs will:

(1) Make SAP access approval or disapproval decisions, including evaluating a nominated individual's suitability when unique risk is identified in responses to the pre-screening questionnaire and coordinate with the government special access program security officer (GSSO), PSO, program manager (PM), and SAPCO as necessary.

(2) Understand that access approval is a separate and distinct action from the access eligibility determination.

(3) Be trained in their authorities, standards, and limitations in accordance with CA SAPCO guidance.

e. PSOs, GSSOs, Contractor Program Security Officers (CPSOs), or SPOs. PSOs, GSSOs, CPSOs, or SPOs designated by the CA SAPCO will:

(1) Forward all previously unreported derogatory information revealed in response to the pre-screening questionnaire to the DoD CAF.

(2) Advise individuals to report any information that may affect their clearance eligibility to their local security manager or special security officer for coordination with the appropriate DoD adjudications facility as outlined in this volume.

#### 4. INDOCTRINATION BRIEFINGS

a. Individuals designated to conduct indoctrination briefings will ensure individuals sign the special access program indoctrination agreement (SAPIA) prior to indoctrination in accordance with Executive Order 12968 (Reference (i)) acknowledging the requirements for gaining access to SAP(s) and the SAP-specific unique requirements.

b. SAP indoctrinations will be conducted only after the PAR has been approved and the SAPIA has been signed.

c. At a minimum, the indoctrination briefings will cover the topics identified on the SAP Refresher Training Record (see <http://www.dss.mil/isp/specialprograms.html>) and the SAP facility standard operating procedures.

d. PSOs, GSSOs, CPSOs or their designees will give a SAP-specific security briefing to all SAP-indoctrinated personnel annually.

5. POLYGRAPHS. The Deputy Secretary of Defense is the approval authority for the use of polygraph examination as a mandatory access determination requirement; the requirement must be consistently applied to all candidates in accordance with DoDI 5210.91 (Reference (j)). CI-Scope polygraph examination must not be used as the only basis for granting access to DoD SAPs. Exceptions to these requirements will only be granted by the Deputy Secretary of Defense. Specific polygraph examinations to resolve issues related to SAP access eligibility will be administered in accordance with Reference (j). Per DoDI 5205.11 (Reference (k)), CI polygraph examinations are considered current when administered within the past 5 years.

6. BILLET MANAGEMENT. CA SAPCOs may establish or authorize SAP billet structures or access quotas that assign individual access by organization and duty position to SAPs under their cognizance. Security personnel will not count against any billet structure or access quotas.

7. PERSONNEL SECURITY FILES. Records must be maintained within a personnel security file for each SAP-accessed individual. The responsible PSO, GSSO, CPSO, or designee will maintain these files. The files will include, but are not limited to:

- a. Pre-screening questionnaire and supplemental information as required by the CA SAPCO.
- b. Consultant agreements, as necessary.
- c. PARs.
- d. Transfer of access (TOA) approvals.
- e. SAPIAs.
- f. Security education and training awareness records.
- g. Foreign travel records.
- h. Foreign contacts records (includes personal, business, and suspicious contact).

- i. Inadvertent disclosure records.
- j. Reports of security infractions and violations.
- k. Potentially disqualifying information records.
- l. LOCNs, as necessary.

8. CONGRESSIONAL ACCESS REQUIREMENTS. Guidance on congressional access to DoD SAPs is contained in Reference (b).

9. INDIVIDUAL REPORTING REQUIREMENTS. All SAP-accessed personnel will report to the PSO, GSSO, or CPSO any information, in addition to that identified in the pre-screening questionnaire, about themselves or others that may pose an undue risk to the SAP or possibly affect an individual's access to SAP(s). Reporting requirements are found in DoD Manual 5200.02 (Reference (l)). Examples of reporting requirements include, but are not limited to:

a. Potentially Disqualifying Information. All SAP-accessed personnel will report to the PSO, GSSO, or CPSO any information that may impact ability of individuals to maintain their eligibility or properly safeguard SAP information. Examples of potentially disqualifying information include, but are not limited to:

- (1) Wage garnishments.
- (2) Criminal conduct (regardless of whether the individual was formally charged).
- (3) Fired from a job.
- (4) Any illegal drug use.
- (5) Alcohol abuse.

b. Foreign Travel. Report all foreign travel in accordance with Enclosure 5 of this volume.

c. Security Incidents. Immediately report all security infractions and violations to the PSO, GSSO, or CPSO, in accordance with this volume.

d. Reportable Contacts, Activities, Indicators, and Behaviors. SAP- accessed personnel will report to the PSO, GGSSO, or CPSO, in accordance with Enclosure 4 of DoDD 5240.06 (Reference (m)).

## 10. GSSO AND CPSO REPORTING REQUIREMENTS

a. Employees Desiring Not to Perform on SAP Activities. A report will be made to the PSO upon notification by a SAP-accessed individual or an individual for whom access has been requested that they no longer wish to perform on the SAP activities.

b. Employees Refusing to Sign a SAPIA. A report will be submitted to the PSO on an individual who refuses to sign a SAPIA. If a SAPIA is not signed, SAP access will not be granted.

c. Change in Employee Status. A written report of all changes in the employment status of SAP-accessed personnel will be provided to the PSO.

11. DEPLOYED OR TEMPORARILY REASSIGNED PERSONNEL. Personnel assigned away from their home location for over 60 days will be debriefed unless they have a continued NTK at their deployment location. Exceptions to this requirement must be approved in writing by the CA SAPCO.

12. TOA. TOA is negotiated between the losing and gaining PSOs and AAAs. The TOA approval must be maintained in the personnel security file, as well as the SAPIA for the maintained accesses. Individuals with SAP access may exercise TOA under the following guidelines:

a. The individual's personnel security investigation must be current.

b. For contractors, individuals must support the same contract in order to transfer SAP access.

c. No previously unreported potentially disqualifying information exists that could affect the individual's continued eligibility for access to SAP(s).

## 13. DEBRIEFING ACKNOWLEDGEMENTS

a. The PSO, GSSO, or CPSO will implement a formal debriefing program when access to SAP information is no longer required.

b. Procedures for debriefing will be arranged to allow each individual the opportunity to ask questions and receive substantive answers from the individual providing the debriefing.

c. The debriefing acknowledgement portion of the SAPIA will be executed at the time of the debriefing, and forwarded to PSO or designee within 3 business days.

d. SAP-accessed personnel will be debriefed by the PSO, GSSO, CPSO, or designee, and the personnel security access database will be updated to reflect this action.

e. The debriefing will include, at a minimum, a reminder of the individual's responsibilities, as agreed to in the SAPIA, which addresses:

(1) The continuing obligations to not disclose SAP information.

(2) The SAPIA as an enforceable legal contract between the individual and the U.S. Government.

(3) All classified information, including SAP information, as the property of the U.S. Government.

(4) The penalties for espionage and unauthorized disclosure, in accordance with Titles 18 and 50, United States Code (References (n) and (o)).

(5) The obligation not to discuss, publish, or otherwise reveal information about the SAP.

(6) Acknowledgement that all future questions or concerns regarding the SAP (e.g., solicitations for information, approval to publish material based on SAP knowledge or experience) will be directed to the PSO, GSSO, or CPSO.

(a) Provide the individual with a telephone number for the PSO, GSSO, or CPSO.

(b) Where to report suspected foreign intelligence service contacts or any attempt by unauthorized individuals to solicit SAP information. Information to be provided must include last known security officer's (SO) name and contact information. The priority for reporting this information is:

1. PSO.

2. GSSO (if applicable)

3. CPSO (if applicable).

4. Respective counterintelligence element or Military Department Counterintelligence Organization (MDCO).

5. Nearest Federal Bureau of Investigation (FBI) office.

(8) That each provision of the agreement is severable (i.e., if one provision is declared unenforceable by a court of competent jurisdiction, all others remain in force).

(9) Though an individual has signed the debriefing acknowledgment portion of the SAPIA, they are never released from the original SAPIA unless specifically notified in writing.

(10) The requirement to return all SAP classified material and unclassified handle via special access channels only material, and the identification of all security containers to which the individual had access.

(11) How to obtain a security and policy review, pursuant to DoDI 5230.29 (Reference (p)), before publishing or other public release.

(12) What can and cannot be discussed or placed in resumes and applications for security clearances.

(13) The debriefing process, the requirement to sign the SAPIA, and the agreement that all questions about the SAPIA were addressed.

f. When access is suspended or revoked or an individual is debriefed for cause, the PSO, GSSO, or CPSO will notify all DoD Component PSOs holding interest in that individual's SAP accesses, as the GSSO or CPSO may not be aware of all SAPs to which an individual is accessed. The PSO will notify the DoD Component CA SAPCO.

g. The individual conducting the debriefing will advise individuals who refuse to sign the debriefing acknowledgment portion of the SAPIA that such refusal may affect future access to SAPs or continued clearance eligibility. Additionally, refusal to sign the debriefing acknowledgement may be cause for administrative sanctions, and it will be reported to the appropriate DoD adjudications facility and DSS, if applicable. In the event that an individual refuses to execute a debriefing acknowledgement on the SAPIA, the GSSO or CPSO must administer an oral debriefing in the presence of a witness and annotate the debriefing acknowledgment portion "ORAL DEBRIEFING CONDUCTED; INDIVIDUAL REFUSED TO SIGN." The briefer and witness sign beneath the statement attesting to this action. Immediately report this fact to the PSO. The PSO will promptly contact other organizations as required.

14. ADMINISTRATIVE DEBRIEFINGS. Efforts to have all SAP-accessed personnel sign a debriefing acknowledgement portion of the SAPIA may prove difficult. If attempts to locate an individual either by telephone or mail are unsuccessful, and the whereabouts of the individual cannot be determined in 30 days, the PSO, GSSO, or CPSO must administratively debrief the individual by completing the debriefing acknowledgment portion of the SAPIA with "INDIVIDUAL NOT AVAILABLE – ADMINISTRATIVELY DEBRIEFED." The appropriate database should be updated to reflect that the individual was debriefed. The PSO, GSSO or CPSO must check to ensure that no SAP information is charged out to, or in the possession of these individuals.

15. SAP ACCESS SUSPENSION AND REVOCATION. The PSO in consultation with the AAA may suspend SAP accesses based on CA SAPCO guidance. The CA SAPCO will make

the decision regarding revocation of SAP access. The individual must be notified in writing of all suspension and revocation actions.



ENCLOSURE 4SPECIAL ACCESS PROGRAM NOMINATION PROCESS (SAPNP)

1. INTRODUCTION. The SAPNP provides a timely, standardized, program-level review of the nominated individual's package for access to a DoD SAP. The SAPNP takes advantage of existing DoD resources and consists of three parts: final security clearance based on a favorable adjudication of an appropriate investigation; demonstrated NTK and material contribution and access eligibility. It is not an investigation or adjudication; rather it is a standardized security management process that applies enhanced security procedures to determine personnel suitability for access to DoD SAPs. A pre-screening questionnaire as seen in the Table must be completed to initiate the process. The nominated individual must provide additional information pertaining to each pre-screening question for which a "yes" response is provided.

Table. Pre-Screening Questionnaire

Foreign Affections	Is any of your immediate family a citizen of a country other than the United States or do you or anyone in your immediate family claim dual citizenship?
Foreign Associations	- <u>Foreign Associations</u> – Do you, your spouse or cohabitants have any continuing contact with citizens or dual citizens of a country other than the United States? <b>Reporting is not required if contact with a foreign national only occurs while in the performance of official United States Government business.</b>  - <u>Foreign Assets</u> – Do you, your spouse, and/or cohabitant have any financial interest or assets in a country other than the United States?
Other Than Official Government Foreign Travel	Have you visited any foreign countries since your last completed investigation?
Personal Conduct	Has your clearance or access been suspended, denied or revoked; or have you been arrested since your last completed investigation?
Financial Responsibility	Have you had any bills referred to a collection agency, had your wages garnished, have any tax liens against you or filed for bankruptcy since your last completed investigation?

2. NOMINATION REQUIREMENTS

a. Candidate prerequisites:

- (1) Must be a U.S. citizen.

(2) Must possess a final TOP SECRET or SECRET clearance as appropriate to the SAP access requested.

(3) Must have a current investigation. CA SAPCO may approve exceptions to this requirement.

(4) Contractor nominated individuals must have a DD Form 254, "Department of Defense Contract Security Classification Specification," or consultant agreement authorizing SAP access in accordance with DoD 5220.22-M (Reference (q)).

b. When the requirements of paragraphs 2a(2), 2a(3), or 2a(4) of this enclosure cannot be met, requestor will submit an LOCN providing facts to support a determination that it is in the national interest for the CA or OA SAPCO to approve access.

c. Non-US citizens' access to DoD SAPs will be evaluated in accordance with Reference (b).

### 3. NOMINATION PACKAGES

a. The PAR will be used to nominate an individual for SAP access. A single PAR may be prepared for multiple SAPs under the cognizance of the same AAA.

b. Only an individual already accessed to a SAP may make a request for a nominated individual's SAP access.

c. The requestor will complete the PAR or provide the nominated individual's personal information, qualifications, his or her potential material contribution to the SAP, and NTK to the individual filling out the PAR.

d. All nomination packages for access to a DoD SAP will contain a current pre-screening questionnaire completed within the last 365 days, PAR, and supplemental information supporting 'Yes' answers.

e. The pre-screening questionnaire, and any supplemental information supplied by the nominated individual, will be maintained in the appropriate SAP access management database or personnel security file.

### 4. NOMINATION REVIEW PROCESS

a. The SAP nomination review process will be performed by an SPO, designated in writing by the CA or OA SAPCO or designee, who has completed the requisite training. The DoD SAPCO, in coordination with the DSS Center for Development of Security Excellence, will establish training guidelines and curriculum.

b. The pre-screening questionnaire will be considered current and reciprocally accepted by all DoD Components if the questionnaire was completed within the last 365 days and the answers to all questions are “No.” CA SAPCO may provide guidance to the SPO pertaining to processing pre-screening questionnaire’s with “Yes” responses. The CA SAPCO may require a LOCN.

c. The responsible SPO will review the nomination package for completeness and accuracy and will validate that the nominated individual meets the criteria in this volume or requires additional review for SAP access.

(1) The SPO will check the approved security clearance database to validate that the nominated individual has the appropriate clearance and the investigation completed date is current in accordance with Reference (1) and this volume.

(2) If the individual’s investigation is not current or in-progress, the SPO will refer the individual to their security manager or special security officer to initiate Electronic Questionnaires for Investigations Processing (e-QIP) Standard Form (SF)-86, “Questionnaire for National Security Positions.” Once reflected as submitted in the approved security clearance database, the SPO will prepare the nomination package in accordance with section 3 of this enclosure and execute the Pre-Screening Questionnaire.

(3) If the pre-screening questionnaire contains no potentially derogatory information, the SPO will make a recommendation to the AAA to approve access. If the pre-screening questionnaire contains derogatory information, the SPO will notify the PSO who will provide an access recommendation to the AAA.

(4) If the SPO determines that the answers to the pre-screening questionnaire qualify as previously unreported derogatory information, the SPO will refer the individual to their local security officer who will report the new derogatory information to the appropriate DoD adjudications facility in accordance with Reference (1).

(5) Whether or not the individual’s investigation is current, if the pre-screening questionnaire contains derogatory information, then the SPO must take appropriate action in accordance with section 5 of this enclosure.

d. The SPO may not disqualify a candidate for SAP access but may recommend additional review to the PSO.

e. The government program manager (GPM) may also review the PAR for the individual’s material contribution and NTK, and concur or non-concur on the PAR.

f. The AAA provides the final access decision (approval or disapproval) on the PAR.

5. CONTINUED ELIGIBILITY. Continued eligibility for SAP access is contingent on the individual’s compliance with the following requirements:

- a. Pursuant to References (l) and (q), SAP-accessed personnel have a responsibility to immediately report any changes in status that may affect their access eligibility.
- b. SAP-accessed personnel annually revalidate access eligibility by either recertifying answers provided to the pre-screening questionnaire and any supplemental information provided, or by completing a new pre-screening questionnaire.
- c. Failure to comply with the requirements of paragraphs 5a and 5b may result in suspension or revocation of SAP access.
- d. SPOs will instruct the nominated individual to forward previously unreported derogatory information to their local security officer for submission to the appropriate DoD adjudications facility. The SPO will forward nomination package via the PSO to the appropriate CA SAPCO for decision to approve or continue access pending final disposition.
- e. Any decision by the appropriate DoD adjudications facility to suspend or revoke the individual's clearance supersedes the SAPNP.

6. DISAPPROVALS. The AAA may disapprove nominated individuals for access by appropriately annotating and summarizing the reason for disapproval in the remarks section of the PAR. Nominated individuals disapproved for access may be resubmitted at the discretion of the requestor.

ENCLOSURE 5

FOREIGN TRAVEL REPORTING

1. GENERAL. SAP-accessed personnel must always be aware of their vulnerability to exploitation by foreign intelligence services. They are particularly susceptible during periods of foreign travel. Individuals must continuously exercise good judgment when contemplating travel. Failure to comply with the reporting requirements may result in suspension and possible loss of SAP access.

2. OFFICIAL GOVERNMENT BUSINESS TRAVEL

a. SAP-accessed personnel will:

(1) Report anticipated foreign travel to the GSSO or the CPSO as applicable; the traveler will ensure they report this travel to the GSSO or CPSO before leaving. Notification must be provided in sufficient time to allow for the completion of an appropriate country-specific threat awareness briefing based on the Defense Intelligence Agency (DIA) foreign intelligence threat level or CA SAPCO guidance and notification of foreign travel using the template (see <http://www.dss.mil/isp/specialprograms.html>).

(2) Report any suspicious foreign contacts immediately upon return.

(3) Within 5 business days upon return, contact the GSSO or CPSO to complete a post-travel debriefing.

b. GSSOs or CPSOs will:

(1) Obtain the notification of foreign travel and other relevant documentation by the SAP-accessed traveler before leaving.

(2) Conduct pre-travel threat awareness briefings and post-travel debriefings.

(3) Inform the PSO about any foreign travel, contacts, or security issues identified by any SAP-accessed individual.

(4) File all completed documentation in the SAP-accessed traveler's personnel security file.

(5) Evaluate foreign travel trends based on SAP-accessed individuals' reported travel. The travel information will be maintained in a readily accessible form.

c. PSOs will:

(1) Upon request, provide GSSOs or CPSOs with the necessary country-specific threat information to be used during foreign travel awareness briefings.

(2) As necessary, coordinate all CSP requests, additional inquiries, and investigations.

(3) Evaluate foreign travel trends based on SAP-accessed personnel reported travel. The travel information will be maintained in a readily accessible form (i.e., a spreadsheet or database).

(4) Assess the risk of any proposed travel to a foreign country and provide defensive briefing covering potential threats specific to the location being traveled to the GSSO or CPSO, and SAP-accessed traveler as appropriate.

(5) Report suspicious travel incidents to their respective CI element or their supporting MDCO.

### 3. NON-OFFICIAL TRAVEL

#### a. SAP-accessed personnel will:

(1) Report anticipated foreign travel 30 days before the date of travel to the GSSO or CPSO to allow for the completion of appropriate country-specific threat awareness briefings based on the DIA foreign intelligence threat level or CA SAPCO guidance and notification of foreign travel using the template (see <http://www.dss.mil/isp/specialprograms.html>). If not practical (validated reasons are determined by the responsible GPM, GSSO, or CPSO), the SAP-accessed traveler must ensure he/she reports this travel to the GSSO or CPSO before leaving. Same day travel must be reported immediately upon return.

(2) The SAP-accessed traveler may undergo a CI polygraph examination upon return as part of the overall threat mitigation strategy.

(3) Report any suspicious foreign contacts immediately upon return.

(4) Within 5 business days upon return, contact the GSSO or CPSO to complete the notification of foreign travel debriefing.

#### b. CPSOs or GSSOs will:

(1) Verify justification for travel requests reported with less than 30 days notice.

(2) Review all proposed foreign travel itineraries and conduct pre-travel country-specific threat awareness briefings and post-travel debriefings.

(3) Inform the PSO about any foreign travel, contacts, or security issues identified by any SAP-accessed individual.

(4) File all foreign travel requests in the SAP-accessed traveler's personnel security file.

(5) Report any foreign travel trends to the PSO. The travel information will be maintained in a readily accessible form (i.e., a spreadsheet or database).

c. PSO will:

(1) Verify justification for travel requests reported with less than 30 days notice.

(2) When requested, provide GSSOs or CPSOs with the necessary country-specific threat information to be used during foreign travel awareness briefings.

(3) Assess the risk of any proposed travel and develop a risk mitigation strategy.

(4) As necessary, coordinate all CSP requests, additional inquiries, and investigations.

(5) Evaluate foreign travel trends reported by the GSSO or CPSO.

(6) Report suspicious travel incidents to their respective CI element or their supporting MDCO.

4. INDIVIDUALS ASSIGNED TO FOREIGN COUNTRIES. SAP-accessed personnel stationed in a foreign country are not required to report travel (official or unofficial) within that country. Same day foreign travel to countries adjacent to the foreign country of station does not require prior notification, but must be reported immediately upon return. All other foreign travel will be reported in accordance with the requirements in sections 2 and 3 of Enclosure 5. Each SAP-accessed individual must inform the GSSO or CPSO of any suspicious foreign contacts encountered.

5. FOREIGN TRAVEL RECORDS. All foreign travel will be documented using the notification of foreign travel template and retained in the individual's personnel security file. Travel records will be retained until the individual is no longer SAP-accessed.

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

AAA	access approval authority
CA	cognizant authority
CAF	consolidated adjudications facility
CI	counterintelligence
CMO	Chief Management Officer of the Department of Defense
CPSO	contractor program security officer
CSP	counterintelligence-scope polygraph
DIA	Defense Intelligence Agency
DoDD	DoD directive
DoDI	DoD instruction
DSS	Defense Security Service
e-QIP	Electronic Questionnaires for Investigations Processing
FBI	Federal Bureau of Investigation
GPM	government program manager
GSSO	government special access program security officer
LOCN	letter of compelling need
MDCO	Military Department Counter Intelligence Organization
NTK	need to know
OA	oversight authority
PAR	program access request
PM	program manager
PSA	Principal Staff Assistant



PSO	program security officer
SAP	special access program
SAPCO	special access program central office
SAPIA	special access program indoctrination agreement
SAPNP	special access program nomination process
SCI	sensitive compartmented information
SF	standard form
SO	security officer
SPO	special access program personnel security official
SSBI	single scope background investigation
SSBI-PR	single scope background investigation periodic reinvestigation
TOA	transfer of access
USD(I&S)	Under Secretary of Defense for Intelligence and Security

## PART II. DEFINITIONS

These terms and their definitions are for the purpose of this volume.

AAA. Individual designated by CA SAPCO to make approval and disapproval decisions for personnel nominated for access to DoD SAP.

Access National Agency Check and Inquiries. The minimum initial investigation for civilian personnel applying for non-critical sensitive national security positions.

billet. A determination that in order to meet NTK criteria, certain SAPs may elect to limit access to a predetermined number of properly cleared employees.

condition. Access eligibility granted or continued with the provision that additional security measures will be required. Such measures include, but are not limited to, additional security monitoring, access restrictions, submission of periodic financial statements, and attendance at counseling sessions.

CSP. A screening polygraph examination that uses relevant questions limited to prescribed CI issues.

current investigation. An investigation not older than 5 years from the closed date of the previous investigation. Individuals who have submitted their SF 86 via e-QIP and the approved

security clearance database shows submitted or open investigation prior to the expiration of the previous investigation are deemed to be current.

deviation. Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or out-of-date investigation. “Significant gap” for this purpose means either complete lack of coverage for a period of 6 months or more within the recent 5 years investigated or the lack of an FBI name check or technical check, or the lack of one or more relevant checks.

e-QIP. A web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations for federal security, suitability, fitness and credentialing purposes. e-QIP allows the user to electronically enter, update, and transmit their personal investigative data over a secure internet connection to a requesting agency.

equivalent investigation. An investigation equal to or greater in scope.

expanded-scope screening. A screening polygraph examination that includes the questions from a CSP polygraph and questions related to falsification of security forms, involvement with illegal drugs, and criminal activity.

immediate family. A spouse, parent, sibling, child, or cohabitant. This includes any step-parents, half and step-siblings, and step-children of the subject.

issue-based examination. An issue-based polygraph examination that is predicated on an allegation or a specific issue under investigation.

LOCN. A written description of an individual’s unique skills or knowledge, the benefit the SAP will gain by accessing the individual, and why no other individual can fulfill or is readily available to fulfill that position.

National Agency Check With Law and Credit Check. The minimum initial investigation for military accessions and contractor personnel that require eligibility for a Confidential or Secret security clearance.

periodic reinvestigation. A reinvestigation conducted at pre-determined intervals for personnel occupying non-critical sensitive or critical sensitive national security positions.

personnel security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

requestor. An individual who requests SAP access for an individual not higher than the classification level and SAPs that the requestor is assessed to, and completes the justification section of the PAR.

revocation. Rescinding SAP access when a currently SAP-accessed individual is determined to be ineligible.

SPO. Individual that has been trained and nominated to apply enhanced security procedures to determine personnel eligibility for access to DoD SAPs in accordance with this volume.

SSBI. The minimum investigation for personnel applying for special or critical-sensitive national security positions or for personnel that require eligibility for a Top Secret security clearance.

SSBI-PR. A modification to the investigative standards for SSBI – periodic reinvestigations. Applies to all civilian and military personnel, as well as consultants, contractors, licensees, certificate holders, grantees, and their employees, and all other individuals who require access to SCI and SAPs.

suspension of access. An action taken regarding a currently SAP-accessed individual, as a result of certain personnel security conditions or questionable circumstances.

system of record. Defined in Reference (h).

TOA. An action that enables an individual to retain SAP accesses when the individual is transferred from one location to another for continued SAP access.