

# Chapter 2

## Security Clearances

### Section 1. Facility Clearances

**2-100. General.** Contractors will possess a Facility Security Clearance to receive, generate, use, and store classified information that is protected in SAPs.

- a. If a facility clearance has already been granted, the SAP Program Executive Agent may carve in the Facility CSA. The agreement entered into by the Secretary of Defense (**SECDEF**) with the other **CSA's** will determine the terms of responsibility for **the** Facility CSA with regard to SAP programs. Due to the sensitivity of some SAPS, the program may be carved out by the Executive Agent designated by the CSA.
- b. The CPSO shall notify the PSO of any activity which affects the Facility Security Clearance, (**FCL**).
- c. In certain instances, security and the sensitivity of the project may require the contract and the association of the contractor with the Program CSA be restricted and kept at a classified level. The existence of any unacknowledged effort, to include its **SAPF**, will not be released without prior approval of the **Pso**.

2-101. Co-Utilization of SAPF. If multiple SAPS are located within a SAPF, a Memorandum of Agreement (**MOA**) shall be written between government program offices defining areas of authorities and responsibilities. The first SAP in an area shall be considered to be the senior program and therefore the CSA for the zone unless authority or responsibility is specifically delegated in the MOA. The MOA shall be executed prior to the introduction of the second SAP into the **SAPF**.

2-102 Access **of Senior Management Officials.** *Only those Senior Management Officials requiring information pertaining to the SAP shall be processed SAP access.*

#### **2-103. Facility Clearances for Multifacility Organizations.**

- a. When cleared employees are located at uncleared locations, the CPSO may designate a cleared **management** official at the uncleared location who shall:
  - (1) Process classified visit requests, conduct initial or recurring briefings for cleared employees, and provide written confirmation of the briefing to the **CPSO**.
  - (2) Implement the reporting requirements of the **NISPOM** and this Supplement for **all** cleared employees and furnish reports to the CPSO for further submittal to the CSA.
  - (3) Ensure compliance with **all** applicable measures of the **NISPOM** and this Supplement by all cleared employees at that location.
- b. If a cleared management official is not available at the uncleared location, the CPSO (or designee) shall conduct the required briefing during visits to the uncleared location or during employee visits to the location or establish an alternative procedure with CSA approval.

## Section 2. Personnel Clearances and Access

2-200. General. This section establishes the requirements for the selection, processing, briefing, and debriefing of contractor personnel for SAPS.

2-201. Program **Accessing Requirements and Procedures.**

a. *The individual will have a valid need-to-know (NTK) and will materially and directly contribute to the Program,*

b. *The individual will possess a minimum of a current, final SECRET security clearance or meet the investigative criteria required for the level of access.* If a person's periodic reinvestigation (PR) is outside the five-year scope and **all** other access processing is current and valid, the PSO may authorize access. However, the individual will be immediately processed for either a Single Scope Background Investigation (SSBI) or National Agency Check with Credit (NACC) as required by the level of clearance or as otherwise required by the contract.

c. *The contractor will nominate the individual and provide a description of the NTK justification. The CPM will concur with the nomination and verify Program contribution by signature on the Program Access Request (PAR). The CPSO will complete the PAR and review it for accuracy ensuring all required signatures are present.* The CPSO signature verifies that the security clearance and investigative criteria are accurate, and that these criteria satisfy the requirements of the Program. Information regarding the PAR may be electronically submitted. While basic information shall remain the same, signatures may not be required. The receipt of the PAR package via a preapproved channel shall be considered sufficient authentication that the required approvals have been authenticated by the CPSO and contractor program manager.

d. **Access Criteria and Evaluation Process.** In order to eliminate those candidates who clearly will not meet the scope for access and to complete the Personnel Security Questionnaire (PSQ), access evaluation may be required. In the absence of written instructions from the contracting activity, the evaluation process will conform to the following guidelines:

- (1) Evaluation criteria will not be initiated at the contractor level unless both the employee and contractor agree.
  - (2) Contractors will not perform access evaluation for other contractors.
  - (3) Access evaluation criteria will be specific and will not require any analysis or interpretation by the contractor. Access evaluation criteria will be provided by the government as required.
  - (4) Those candidates eliminated during this process will be advised that access processing has terminated.
- e. Submit a Letter of Compelling Need or other documentation when requested by the PSO.
- f. Formats required for the processing of a SAP access fall into two categories: those required for the conduct of the investigation and review of the individual's eligibility, and those that explain or validate the individual's NTK. These constitute the PAR package. The PAR package used for the access approval and NTK verification will contain the following: the PAR and a recent (within 90 days) PSQ reflecting pen and ink changes, if any, signed and dated by the nominee.
- g. Once the PAR package has been completed, the CPSO will forward the candidate's nomination package to the PSO for review:
- (1) The PSO will review the PAR package and determine access eligibility.
  - (2) Access approval or denial will be determined by the GPM and/or access approval authority.
  - (3) The PSO will notify the contractor of access approval or denial.
  - (4) Subcontractors may submit the PAR package to the prime. The prime will review and concur on the PAR and forward the PAR and the unopened PSQ package to the PSO.

h. SCI access will follow guidelines established in DCID 1/14.

**2-202. Supplementary Measures and Polygraph.**

- a. Due to the sensitivity of a Program or criticality of information or emerging technology, a polygraph may be required. The polygraph examination will be conducted by a properly trained, certified, U.S. Government Polygraph Specialist. If a PR is outside the 5-year investigative scope, a polygraph may be used as an interim basis to grant access **until** completion of the PR.
- b. There are three categories of **polygraph**: Counterintelligence (**CI**), Full Scope (CI and life style), and Special Issues Polygraph (SIP). The type of polygraph conducted will be determined by the CSA.

2-203. **Suspension and Revocation.** All PSO direction to contractors involving the suspension or revocation of an employee's access will be provided in writing and if appropriate, thru the contracting officer.

2-204. **Appeal Process.** The CSA will establish an appeal process.

2-205. **Agent of the Government-** The Government may designate a contractor-nominated employee as an Agent of the Government on a case-by-case basis. Applicable training and requirements will be provided by the Government to contractor designated as Agents of the Government.

2-206 **Access Roster or List.** *Current access rosters of Program-briefed individuals are required at each contractor location. They should be properly protected and maintained in accordance with the PSG. The access roster should be continually reviewed and reconciled for any discrepancies. The data base or listing may contain the name of the individual organization, position, billet number (if applicable), level of access, social security number, military rank/grade or comparable civilian rating scheme, and security clearance information. Security personnel required for adequate security oversight will not count against the billet structure.*