

# Chapter 3

## Security Training and Briefings

### Section 1. Security Training and Briefings

**3-100. General.** *Every Special Access Program (SAP) will have a Security Training and Briefing Program.*

As a minimum, SAP-indoctrinated personnel will be provided the same or similar training and briefings as outlined in the baseline **NISPOM**. *In addition, CPSOs responsible for SAPs at contractor facilities will establish a Security Education Program to meet any specific or unique requirements of individual special access programs.* Topics which will be addressed, if appropriate to the facility or the SAP(s), include:

- a. Security requirements unique to SAPs;
- b. Protection of classified relationships;
- c. **Operations Security (OPSEC)**;
- d. Use of nicknames and code words;
- e. Use of special transmission methods;
- f. Special test-range security procedures;
- g. Procedures for unacknowledged SAP security. An unacknowledged SAP will require additional security training and briefings, beyond that required in the baseline. Additional requirements will be specified in the Contract Security Classification Specification and will address steps necessary to protect sensitive relationships, locations, and activities.
- h. Specific procedures to report fraud, waste, and abuse.
- i. Computer security education that is to include operational procedures, threats, and vulnerabilities.
- j. Writing unclassified personnel appraisals and reviews.
- k. Third-Party Introductions. The purpose of the Third-Party Introduction is to provide a clearance, and/or access verification to other cleared personnel. The introduction is accomplished by a briefed third party, who has knowledge of both individual's access.

**3-101. Security Training.** *The CPSO will ensure that the following security training measures are implemented:*

- a. **Initial Program Security Indoctrination.** *Every individual accessed to a SAP will be given an initial indoctrination. The briefing will clearly identify the information to be protected, the reasons why this information requires protection, and the need to execute a NDA. The individual will be properly briefed concerning the security requirements for the Program, understand their particular security responsibilities, and will sign a NDA. This indoctrination is in addition to any other briefing required for access to collateral classified or company proprietary information. It will be the responsibility of the PSO to provide to the contractor information as to what will be included in the initial indoctrination to include fraud, waste, and abuse reporting procedures.*
- b. Professionalized AIS training maybe required of all contractor Information Systems Security Representatives (ISSRs) to ensure that these individuals have the appropriate skills to perform their job functions in a competent and cost-effective manner. This training will be made available by the CSA. The training should consist of, but not be limited to, the following criteria:
  - (1) Working knowledge of all applicable and national CSA regulations and policies including those contained in this supplement;
  - (2) Use of common Information Security (INFOSEC) practices and technologies;
  - (3) AIS certification testing procedures;
  - (4) Use of a risk management methodology;
  - (5) Use of configuration management methodology.

**3-102. Unacknowledged Special Access Programs (SAP).** Unacknowledged SAPS require a significantly greater degree of protection than acknowledged SAPS. Special emphasis should be placed on:

- a. **Why** the SAP is unacknowledged;
- b. Classification of the **SAP**;
- c. Approved communications system;
- d. Approved transmission systems;
- e. **Visit** procedures;
- f. Specific program guidance.

**3-103. Refresher Briefings.** *Every accessed individual will receive an annual refresher briefing from the CPSO to include the following, as a minimum:*

- a. Review of Program-unique security directives or guidance;
- b. Review of those elements contained in the original NDA.

**Note.** The PSO may require a record to be maintained of this training.

**3-104. Debriefing and/or Access Termination.** *Persons briefed to SAPS will be debriefed by the CPSO or his designee. The debriefing will include as a minimum a reminder of each individual's responsibilities according to the NDA which states that the individual has no Program or Program-related material in his/her possession, and that he/she understands his/her responsibilities regarding the disclosure of classified Program information.*

- a. Debriefings should be conducted in a SAPF, Sensitive Compartmented Information Facility (SCIF), or other secure area when possible, or as authorized by the PSO.
- b. Procedures for debriefing will be arranged to allow each individual the opportunity to ask questions and receive substantive answers from the debriefer.
- c. *Debriefing Acknowledgments will be used and executed at the time of the debriefing and include the following:*

- (1) *Remind the individual of his/her continuing obligations agreed to in the SAP NDA.*
  - (2) *Remind the individual that the NDA is a legal contract between the individual and the U.S. Government.*
  - (3) *Advise that **all** classified information to include Program information is now and forever the property of the U.S. Government.*
  - (4) *Remind the individual of the penalties for espionage and unauthorized disclosure as contained in Tides 18 and 50 of the U.S. Code. The briefer should have these documents available for handout upon request. Require the individual to sign and agree that questions about the NDA have been answered and that Tides 18 and 50 (U.S. Codes) were made available and understood.*
  - (5) *Remind the individual of his/her obligation not to discuss, publish, or otherwise reveal information about the Program. The appearance of Program information in the public domain does not constitute a de facto release from the continuing secrecy agreement.*
  - (6) *Advise that any future questions or concerns regarding the Program (e.g., solicitations for information, approval to publish material based on Program knowledge and/or experience) will be directed to the CPSO. The individual will be provided a telephone number for the CPSO or PSO.*
  - (7) *Advise that each provision of the agreement is severable, i.e., if one provision is declared unenforceable, all others remain in force.*
  - (8) *Emphasize that even though an individual signs a Debriefing Acknowledgment Statement, he/she is never released from the original NDA/secrecy agreement unless specifically notified in writing.*
- d. Verify the return of any and all SAP classified material and unclassified Program-sensitive material and identify all security containers to which the individual had access.

- e. When debriefed **for cause, include a brief statement as to the reason** for termination of access and notify the PSO. In addition the CPSO will notify all agencies holding interest in that person's clearance/ accesses.
- f. The debriefer will advise persons who refuse to sign a debriefing acknowledgment that such refusal could affect future access to special access programs and/ or continued clearance eligibility. It could be cause for administrative sanctions and it will be reported to the appropriate" Government Clearance Agency.
- g. Provide a point of contact for debriefed employees to report any incident in the future which might affect the security of the Program.

**3-105. Administrative Debriefings.** Efforts to have all Program-briefed personnel sign a Debriefing Acknowledgment Statement may prove difficult. If attempts to locate an individual either by telephone or mail are not successful, the CPSO should prepare a Debriefing Acknowledgment Statement reflecting the individual was administratively debriefed. *The Debriefing Acknowledgment Statement will be forwarded to the PSO. The CPSO will check to ensure that no Program material is charged out to, or in the possession of these persons.*

**3-106. Recognition and Award Program.** Recognition and award programs could be established to single out those employees making significant contributions to Program contractor security. If used, CPSOs will review award write-ups to ensure recommendations do not contain classified information.