

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
Unit 30400, Box 1000
APO AE 09128

Directive
Number 25-3

29 July 1998

SECURITY

Sensitive Compartmented Information Access Management Program,
SCI Access Certification

-
1. **Summary.** To establish policies and procedures regulating the Sensitive Compartmented Information (SCI) billets managed by the HQ USEUCOM Special Security Office (SSO) in support of the Headquarters and other specified units/activities, the processing of SCI access requirements, and the certification of SCI access for HQ USEUCOM/visitor personnel.
 2. **Applicability.** This Directive applies to organizations/elements whose SCI billets are managed by the HQ USEUCOM SSO.
 3. **Internal Control Systems.** This Directive is not subject to the requirements of AR 11-2.
 4. **Suggested Improvements.** Recommended changes can be sent to HQ USEUCOM/ECJ2-SSO, Unit 30400 Box 1000, APO AE 09128, the proponent responsible for this Directive.
 5. **Reference.**
 - a. DOD 5105.21.M-1, Sensitive Compartmented Information Administrative Security Manual, March 1995 (S).
 - b. Director of Central Intelligence Directive (DCID 1/14) , Personnel Security Standards and Personnel Governing Eligibility for Access to Sensitive Compartmented Information (SCI).

This Directive supersedes ED 25-3, dated 9 August 1993

6. Terms.

a. Sensitive Compartmented Information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

b. DCID 1/14 Eligibility. DCID 1/14 provides eligibility standards based on a successful completion of a background investigation before an individual is granted access to SCI. A Single Scope Background Investigation (SSBI) completed within the last 5 years, or directed period, serves as the basis for granting eligibility.

c. SCI Indoctrination. Indoctrination is the formal information an individual receives prior to being granted access to a SCI system or program. The instructions convey the unique nature, unusual sensitivity, and special security safeguards and practices for SCI handling, particularly the necessity to protect sensitive sources and methods. SCI indoctrination includes the signing of a Nondisclosure Agreement (NDA) and a briefing on the authorized SCI access and programs.

d. SCI Access Management. Although there is no national level requirement for a SCI billet structure, HQ USEUCOM SSO manages a modified billet program. The Director, Defense Intelligence Agency (DIA), the Senior Official of the Intelligence Community (SOIC), through the HQ USEUCOM Senior Intelligence Officer (SIO), the ECJ2, is responsible for approval of all individuals for access to SCI. The program will be managed in a manner that will:

(1) Record all SCI indoctrinations and debriefings.

(2) Identify the number of accesses (by compartment) granted, denied, revoked and suspended.

(3) Identify an individual's DCID 1/14 eligibility date, SSBI date, SCI NDA date, accesses, and waivers, if applicable.

e. The HQ USEUCOM ECJ2 Special Security Officer (SSO) is the designated authority to manage the SCI program on behalf of the USEUCOM SIO. Specific duties and requirements of this individual, the USEUCOM SSO, are spelled out in reference (a) and appropriate appointment orders.

f. Security Managers/SCI Managers. An individual specified in writing to the SSO from each Directorate, Office, Agency, or Security Assistance Organization provided SCI administrative support by SSO USEUCOM will act as the sole point of contact

between the SSO and that entity for SCI certification matters. The SCI Access Manager will be an SCI indoctrinated individual in the grade of E-6, GS-7 or above.

g. Contract Monitors: Specific personnel employed by a DOD cleared contractor whose personnel are supported by the HQ USEUCOM SSO and to whom SCI contract support is rendered.

7. Responsibilities.

a. The ECJ2-SSO will:

- (1) Manage the SCI access program.
- (2) Nominate individuals requiring SCI access to the appropriate military Central Adjudication Facility (CAF).
- (3) Conduct indoctrination's and debriefings as required and authorized.
- (4) In specific instances, forward or pass SCI access certifications of HQ USEUCOM personnel visiting other commands/installations and maintain SCI certification of personnel visiting HQ USEUCOM. Forwarding of SCI access certifications must be passed from SSO to SSO.
- (5) Perform all actions required to ensure timely submission of requisite Personnel Security Investigation (PSI) request and process all follow-up or special action requests from all military CAFs.
- (6) Maintain a SSO clearance database available for electronic access sharing within the European Theater.

b. Directorates, Offices, Agencies, and Security Assistance Organizations will: designate, in writing, to the HQ USEUCOM SSO, the person who will serve as SCI Access Manager and who will function as the primary point of contact between that entity and the SSO on matters relating to SCI accesses and certifications.

c. SCI Access Managers will:

- (1) Monitor the SCI access structure in their organizations on a continuing basis to determine and take actions, as required, ensuring only individuals with a need-to-know are indoctrinated into SCI programs.
- (2) Inform the SSO immediately of any changes in the status of personnel, such as:
 - (a) Assignment/reassignment of personnel

- (b) Change of rank/grade
- (c) Intention to marry or marriage to a foreign national

(d) Information that could adversely impact an individual's loyalty, integrity, discretion, moral character or trustworthiness (e.g. DWI, unresolved financial difficulties, drug/alcohol abuse, arrests, etc..)

(3) Ensure that personnel occupying SCI positions have a current SSBI completed within the last five years or the current designated period. Periodic Reinvestigations (PRs) should be submitted at the 4 year, 6 month date, as applicable or upon receipt of notification from the SSO.

(4) Ensure that Personnel Requisitions submitted to ECJ1 contain the requirement for SCI eligibility and that the required SSBI was, at least, initiated **prior** to departure from the previous duty station. Every effort should be made to ensure that the service member, civilian employee or DOD contractor, retains a file copy of his/her investigative packet for possible use by the HQ USEUCOM SSO upon their arrival.

8. **Policy and Procedures.**

a. **Policy.** SSO USEUCOM administers the SCI Access Management program for HQ USEUCOM and other specified unit activities. Access to SCI is authorized by the Director of Intelligence HQ USEUCOM/ECJ2 to fulfill operational requirements. The appropriate military service authorizes SCI eligibility for access to personnel who occupy valid SCI positions at HQ USEUCOM or other unit/activities. SCI access is not normally granted to personnel unless they are assigned for duty in a position that requires SCI access to perform essential duties.

b. **Procedures.**

(1) Request for SCI Access.

(a) Individuals will be indoctrinated for SCI access only in order to fulfill mission requirements. Upon notification of orders on incoming personnel occupying an SCI billet, the SCI Access Manager will forward to the SSO a HQ USEUCOM Form 28R, 21 Jul 97, Personnel Security Access Request (Appendix A) and a copy of PCS orders for the incumbent, if applicable. This will assist the SSO Personnel Security Section in requesting a transfer-in-status (TIS) from the losing command. For individuals who have already arrived and require access to SCI, forward only the Form 28-R to the HQ USEUCOM SSO via S-LAN, U-LAN, fax or in hard copy to the customer service desk.

(b) Marriage to a foreign national is grounds for reevaluation of SCI access. Each military service has a requirement to submit a SF86, Questionnaire for National Security Position on the spouse with (Blocks 1-4 completed for the DOD personnel) and (Blocks 13-15) completed on the intended spouse. A DD Form 1879, DOD Request for Personnel Security Investigation, must be completed and then signed by the individual's supervisor. All services have a requirement for a Commander's interview of the perspective spouse and a compelling need statement justifying why member should retain SCI access after marriage to a foreign spouse. (Additionally, Navy and Marine Corps personnel must also have a Foreign Spouse Indices Check requested by the SSO through the Naval Criminal Investigative Service.) The results of the interview will be submitted to the SSO Personnel Security Section. This office can also be contacted for assistance and/or additional guidance concerning this policy and conduct of the Commander's interview. All forms are available in the HQ USEUCOM SSO, Room 128, Bldg 2302, Patch Barracks, Stuttgart, Germany.

(c) When the need to grant access to SCI is of such urgency that the benefits to be gained by indoctrination **far outweigh** any security risk involved and denial could endanger operations, cause major repercussions, or impair the mission of the command, a "compelling need" or "Emergency Access - Air Force" request may be submitted. Offices requesting a compelling need access for an individual must provide detailed justification. The request must be signed by an O-6, GS-15 or above, in the direct chain of command. The SSO Personnel Security Section will then forward the request to the individual's military service CAF for approval.

(2) SCI Access Certification Requests:

(a) It is an individual's responsibility to ensure that special accesses have been forwarded to the appropriate command, agency, and/or installation **prior** to commencing TDY/TAD. The USEUCOM SCI Clearance Database includes information regarding all SCI indoctrinated personnel on a PCS assignment at USEUCOM, its elements and Component Commands. Presentation of a valid ID card at any of these on-line SSOs will verify SCI access. Where not available, personnel are required to submit a "SCI Clearance Certification Request" (Appendix B) to the SSO Personnel Security Section at least five (5) working days prior to the intended visit. Failure to submit this form could result in unnecessary delay of SCI clearance access at the individual's destination(s).

(b) The SCI accesses of individuals visiting HQ USEUCOM can be certified by SSO USEUCOM only if a message is received from the visitors SSO via the Defense Special Security Communications Systems (DSSCS) or JDISS-CSE systems or the sponsoring SSO is on-line with the SSO European-Wide database and the individual's clearance can be verified. The DSSCS address for HQ USEUCOM is "SSO USEUCOM//ECJ2-SSO//."

(c) Anyone hosting incoming visitors requiring SCI access should ensure visitors are aware of the SCI requirements. In an effort to eliminate unnecessary delays, individuals should contact the USEUCOM SSO prior to visits/conferences to ensure receipt of clearance

messages and to sign for SCI Visitor badges. Be prepared to provide the SSO with the full name, SSN, grade/rank, and, if known, date time group of clearance certification message sent to SSO USEUCOM.

(d) Personnel assigned to unit/activities geographically separated from HQ USEUCOM and the Stuttgart military community will send/receive access certifications through their supporting SSO.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DAVID L. BENTON III
Lieutenant General, USA
Chief of Staff

SUSAN M. MEYER
LTC, USA
Adjutant General

DISTRIBUTION:

ECJ1	ECDC	ECPLAD
ECJ2 (2)	ECIG	DISA-EUR
ECJ3 (2)	ECPAO	DSWA-EUR
ECJ4 (10)	ECMD	JAC-Molesworth
ECJ5 (2)	ECCH	52 ND Signal
ECJ6	ECCM	NSA/CSS EUR
ECJ6-C	ECLA	PMO
ECSO	EHC	MARFOREUR
ECJS	ECCS	6 th ASG - PAC