Security Guidance and Procedures

Category: A. Director of Central Intelligence Directives (DCIDs) **Subcategory:** 1. DCIDs

Subject: 1/21 Physical Security Standards for SCI Facilities

Effective Date (mm/dd/yy): 07/29/94

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIF)

EFFECTIVE 29 JULY 1994

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

(Effective 29 July 1994)

PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES

Pursuant to the provisions of Section 102 of the National Security Act of 1947 and Executive Order 12333, physical security standards for sensitive compartmented information facilities (SCIFs) are hereby established.

1. PURPOSE

The purpose of this directive is to establish construction and security protection standards required for all US Government facilities or US Government-sponsored contractor facilities where sensitive compartmented information (SCI) may be stored, used, discussed, and/or processed.

2. GENERAL

All SCI must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets physical security standards imposed by the DCI in the physical security standards manual that supplements this directive. The DCI is the accrediting authority for all SCIFs except where that authority has been delegated or otherwise provided for (see DCID 1/19).

3. APPLICABILITY

This directive is applicable to all SCIFs. Senior Officials of the Intelligence Community (SOICs) are charged with implementation and enforcement of the provisions of this directive. SCIFs established in all organizations outside the cognizance of Intelligence Community agencies/ departments as defined in Executive Order 12333 are directly under the authority and oversight of the DCI. SCIFs are established primarily for SCI and are intended to provide the highest level of physical security protection. It is sometimes necessary for non-SCI programs to be afforded an equal level of protection by introduction of such material into SCIFs. Should this occur, the express approval of the accrediting authority is required, and appropriate documentation shall be included in the accreditation records.

4. POLICY

SOICs shall establish and maintain within their agencies formal physical security programs to ensure that SCI is properly protected. The physical security requirements for such protection are contained in the Manual for Physical Security Standards for Sensitive Compartmented Information Facilities, the supplement to this directive. Annexes to this manual addressing specific technical and tactical applications of standards shall be published separately and periodically updated as required.

5. INTERPRETATION

Questions concerning the interpretation and implementation of SCIF physical security standards shall be referred to the Community Counterintelligence and Security Countermeasures office/Intelligence Community Staff (CCISCMO/ICS) or successor organization.