Sensitive Compartmented Information Facility (SCIF). FAC: 1405

CATCODE: 140422
OPR:
OCR:

1.1. **Description.** An electromagnetic counter-surveillance area where Sensitive Compartmented Information (SCI) is stored and reviewed. Because of special security community controls indicating special handling of end products, special construction and security measures are required in these areas. SCIF areas are accounted for separately from all other parts of a facility.

1.1.1 A SCIF is an enclosed area within a building that is used to process SCI types of classified information. SCI is 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 National Intelligence (DNI). Some entire buildings are SCIFs where all but the front foyer is secure. Access to SCIFs is normally limited to those with clearance. Non-cleared personnel in SCIF must be under constant oversight to prevent unauthorized access to classified material; as part of this process, non-cleared personnel are typically required to surrender recording and other electronic devices. All activity and conversation inside is presumed restricted from public disclosure. A SCIF can also be located in an air, ground or maritime vehicle, or can be established on a temporary basis at a specific site.

1.1.2 TEMPEST is a National Security Agency specification and NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. TEMPEST covers both methods to spy upon others and how to shield equipment against such spying. The protection efforts are also known as emission security (EMSEC), which is a subset of communications security (COMSEC). The NSA methods for spying upon computer emissions are classified, but some of the protection standards have been released by the Office of the Director of National Intelligence. Protecting equipment from spying is done with distance, shielding, filtering and masking. The TEMPEST standards mandate elements such as equipment distance from walls, amount of shielding in buildings and equipment, and distance separating wires carrying classified vs. unclassified materials, filters on cables, and even distance and shielding between wires/equipment and building pipes. Noise can also protect information by masking the actual data. While much of TEMPEST is about leaking electromagnetic emanations, it also encompasses sounds or mechanical vibrations. For example, it is possible to log a user's keystrokes using the motion sensor inside smartphones. Compromising emissions are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

1.1.3 Additional information is available in the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, which may be accessed via the following website: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-ci-security-governance-regulations

1.2. A defined facility standard is not currently available for this CATCode. By default, all requirements are user justified until a standard is established or adopted.