
ADAMO
ENRICHING PEOPLE AS WE ADVANCE SECURITY

Overview of ICD/ICS 705

Introduction to IC Tech Spec – for ICD/ICS 705

Secure Facilities Basics

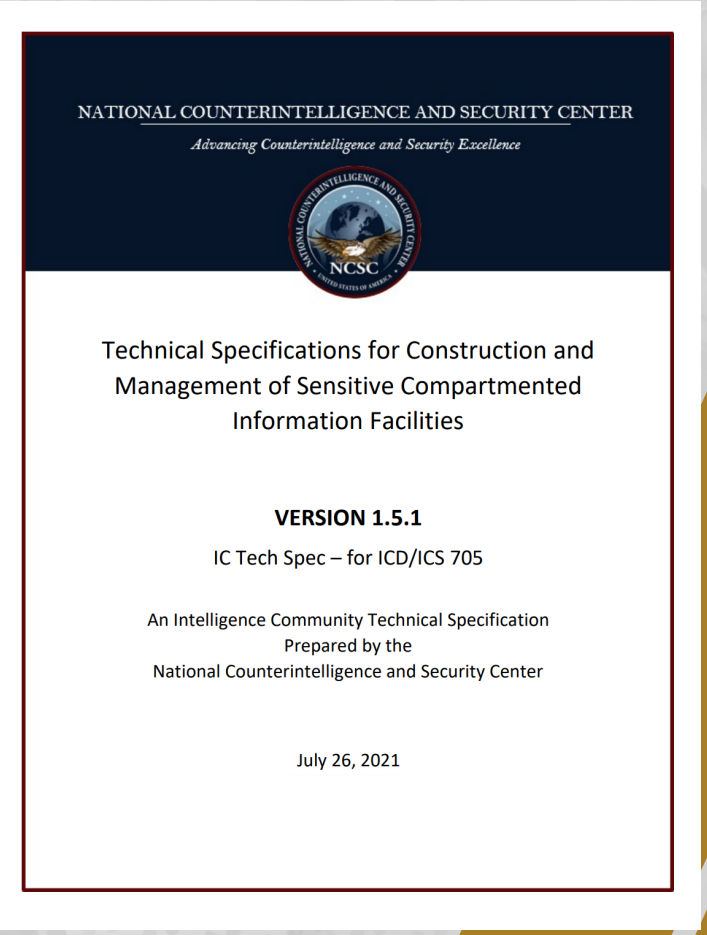
Key Government Project Personnel

Accreditation Process

Q&A

IC Tech Spec – For ICD/ICS 705

- Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities and Special Access Program Facilities
- It is a U.S. Government document that outlines standards for the construction and maintenance of secure facilities.
- Purpose
  - Ensures that facilities are designed and constructed to protect classified information from unauthorized access.
  - Provides guidelines for the physical security, construction, and accreditation of SCIFs and SAPF's.
  - Created to build reciprocity across all 17 IC elements
  - Replaced DCID 6/9 and JFAN 6/9 in 2012


NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Advancing Counterintelligence and Security Excellence

NCSC

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities

VERSION 1.5.1

IC Tech Spec – for ICD/ICS 705

An Intelligence Community Technical Specification
Prepared by the
National Counterintelligence and Security Center

July 26, 2021

Secure Facility Basics

Secure Facility Basics

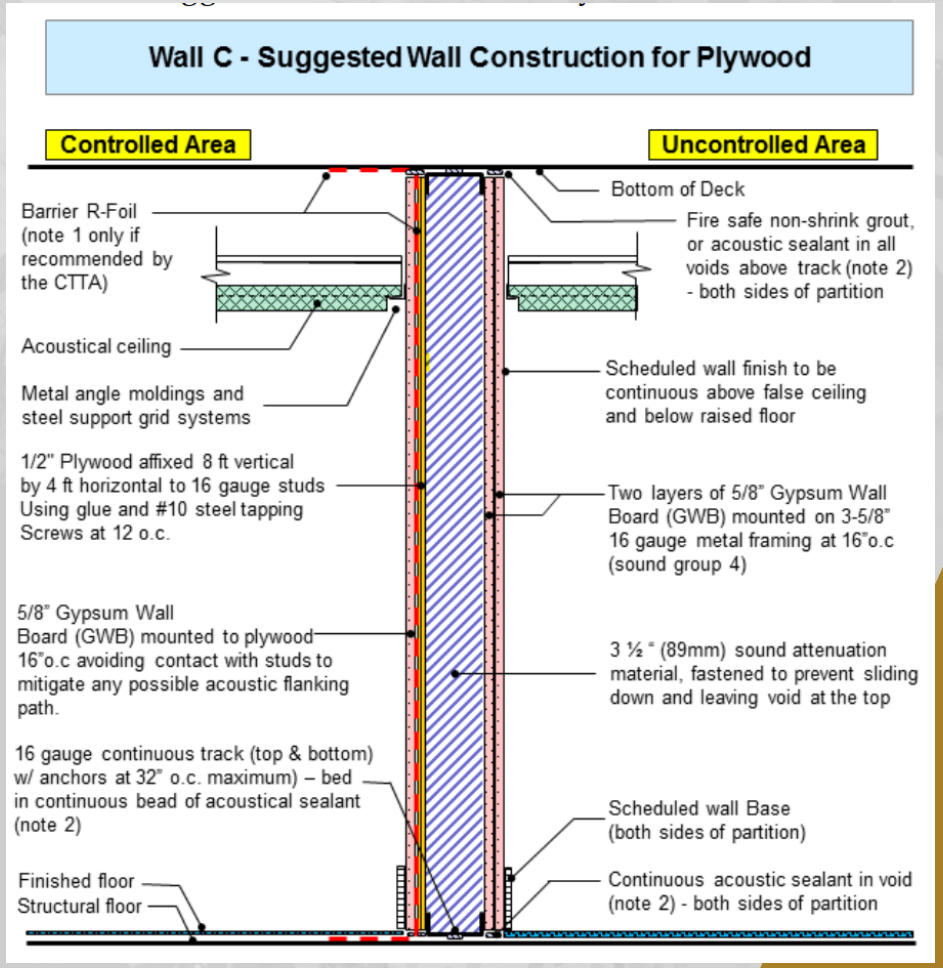
- A secure facility is a room, building or other space where classified information is stored, process and/or discussed. **In order to process/store/discuss classified information on an ongoing (non-temporary) basis**, a space must be accredited by an element of the DoD and Intelligence Community as a permanent facility **beforehand**.
- Each classification level can require a different set of standards for the facility.

Secure Facility Basics

- **Secret only material:** This level of program would typically only need a General Secret space, oftentimes referred to in DoD as an OSS, SECNAV or GENSR. Different branches of the DoD and other Intelligence Community (IC) Elements have their own versions of standards for these spaces.
- **Secret up to Top Secret:** This type of space that could house either/or both Secret and TS information would be called Collateral Program Area. Intelligence Community (IC) elements have their own versions of standards for these spaces.
- **Special Access and Compartmentalization:** This level of information is intentionally segregated into many different sub-classifications (usually called Caveats) but falls into two main categories: Sensitive Compartmented Information (SCI) or Special Access Program (SAP). The sub-classifications (Caveats) would be a suffix or multiple suffixes after the classification level. This type of information requires either an SCI Facility or SAP Facility designed and built to the ICD/ICS 705 standards.

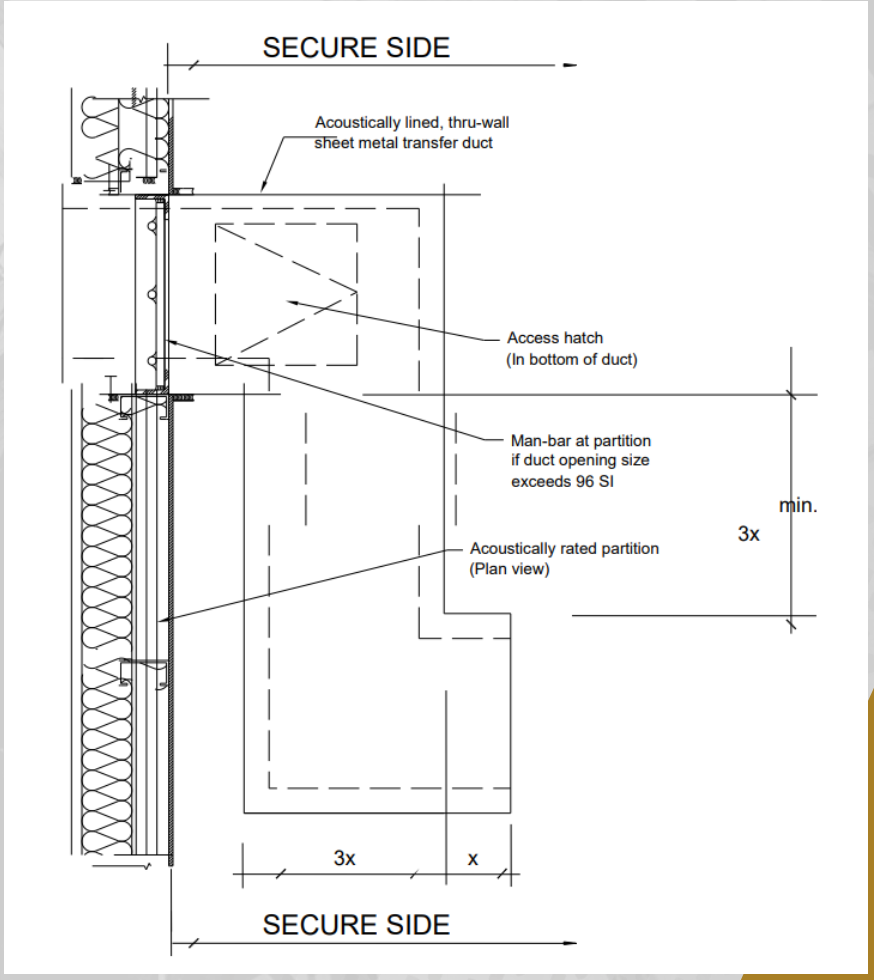
SAP/SCI Facility Basics

- **Physical Security:** the protection materials and denial/detection of unauthorized access to program space and information within
  - 16ga steel studs or 2”x4” wood framing true floor to true ceiling
  - Plywood
  - #9 10ga Expanded metal mesh
  - Concrete or CMU
  - Man-bars at mechanical penetrations



SAP/SCI Facility Basics

- **Acoustic Security:** the proper treatment of sound transmission through the perimeter to protect classified information. Typically requiring STC 45 or STC 50
  - Multilayered wallboard
  - Mechanically fasten insulation in wall cavities
  - Acoustical sealants
  - Treatment of mechanical penetrations with Z-ducts and sound baffles
  - Acoustic infill for all open pathways
  - Acoustic doors

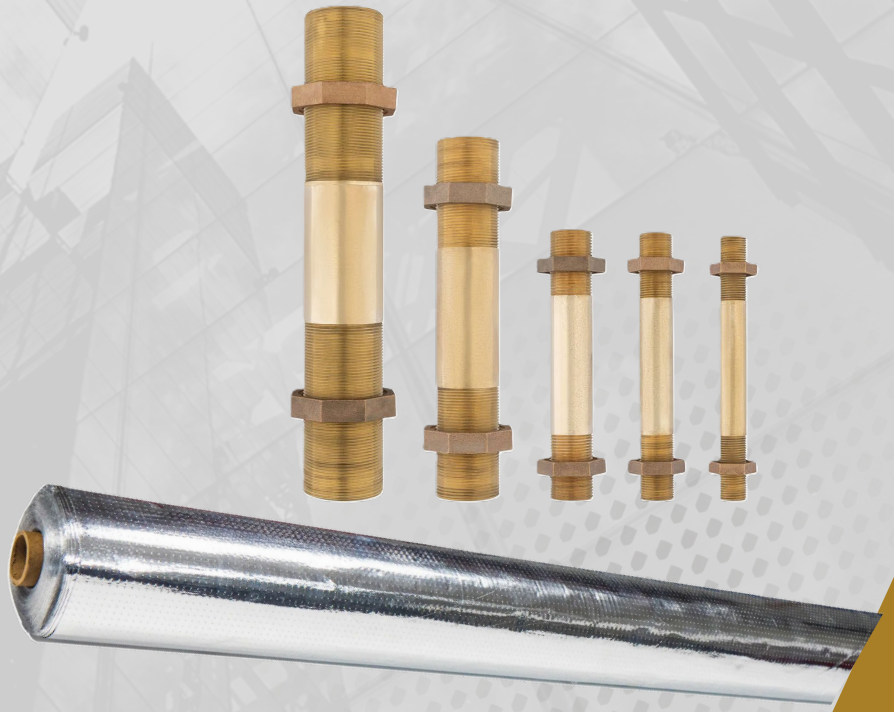


SAP/SCI Facility Basics

- **Operational Security:** the procedures and technologies used to protect classified information from insider threats and other human vulnerabilities.
  - UL 2050 Alarm system
  - GSA approved Access control system
  - Cameras
  - GSA approved main entry lock

SAP/SCI Facility Basics

- **Emanation Security:** addresses the management of unintentional emissions of electromagnetic signals, that could potentially reveal classified information. Often referred to as TEMPEST.
  - RF shielding foils
  - Waveguides
  - Power filters
  - Dielectric breaks
  - RF doors
  - Red/Black network separation



Key Government Project Personnel

Key Government Project Personnel

Accrediting Official (AO)

The Accrediting Official (AO) plays a critical role in overseeing and authorizing the security accreditation of a SAP/SCI Facility projects. Their responsibilities include:

- Risk and vulnerability assessments and mitigation measures
- Design approval of project plans, designs, and security features of work
- Oversight throughout the construction and implementation phases

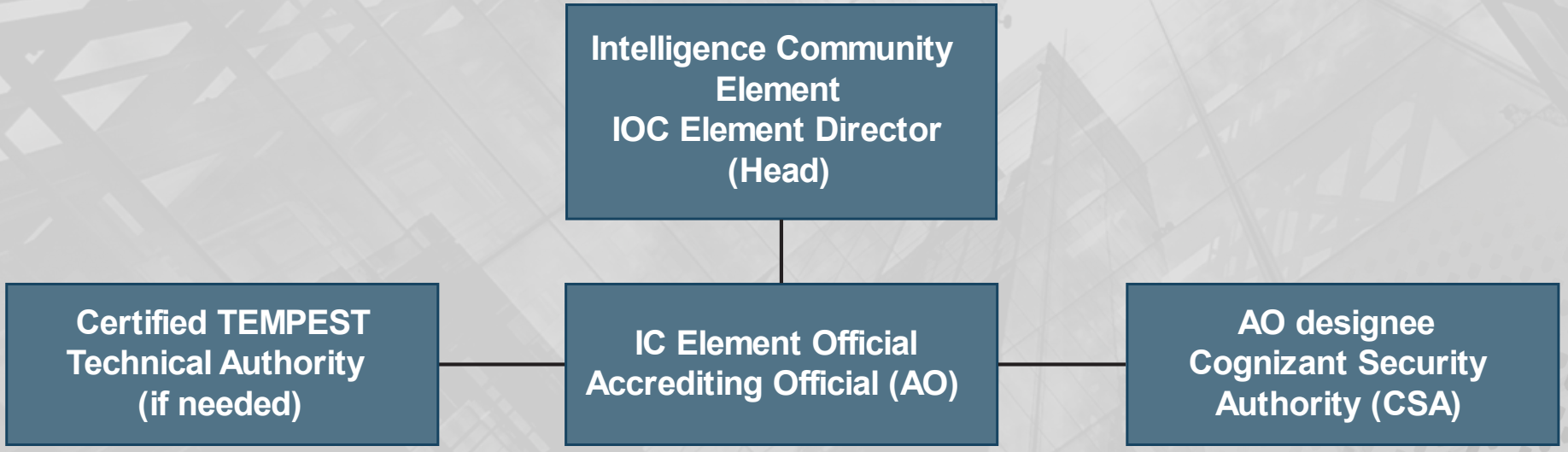
Key Government Project Personnel

Certified TEMPEST Technical Authority (CTTA)

The CTTA is a government employee who specialize in this area of security called TEMPEST, or emanation security on SAP/SCI Facilities. Their responsibilities include:

- Providing *f*inal direction related to any required TEMPEST mitigations on secure facility projects
- Design review of project plans, designs, and security features of work related to TEMPEST
- Collaborates with the Accrediting Official throughout the project

Key Government Project Personnel



ACCREDITATION PROCESS OVERVIEW

ACCREDITATION PROCESS OVERVIEW

How Accreditation (Typically) Works:

- Final accreditation of an ICD 705 facility typically requires a series of approvals before it can be completed. This is similar to a “layered approach”
- The ICD 705 related accreditation precedes other accreditations (networks, sub-compartmented areas, etc.) if/when required
- The overall accreditation cycle(s) will often involve multiple officials or points of contact and each will oversee their respective components of the process so start this as soon as possible

Continued on the next slide…

ACCREDITATION PROCESS OVERVIEW

- The SSM prepares the Pre-construction Checklist, TEMPEST Checklist, FFC, related floor plans and any other appropriate checklists/documentation. Then submits all to the AO
- The AO will often send the TEMPEST Checklist and related documents onto a CTTA for their review and approval
- After the CTTA review is complete and satisfactory, the AO will then review and process the FFC, and any other related documents. Upon satisfactory review, an interim or final accreditation will be given to the program area

Continued on the next slide…

ACCREDITATION PROCESS OVERVIEW

- After the program area is accredited, classified assets may be moved into the space. If/when classified networks and servers are to be utilized within a program space, these systems may only be setup/installed/configured after the ICD 705 accreditation has been processed
    - Interim accreditation may be granted which would allow equipment to be moved into the program space
- After classified data/communication systems are installed and configured, the accreditation for each system may be submitted to the appropriate authority and accreditation will be issued
    - The AO for the data/communication systems may be different than the AO for the physical facility

Q&A