

ICD 705

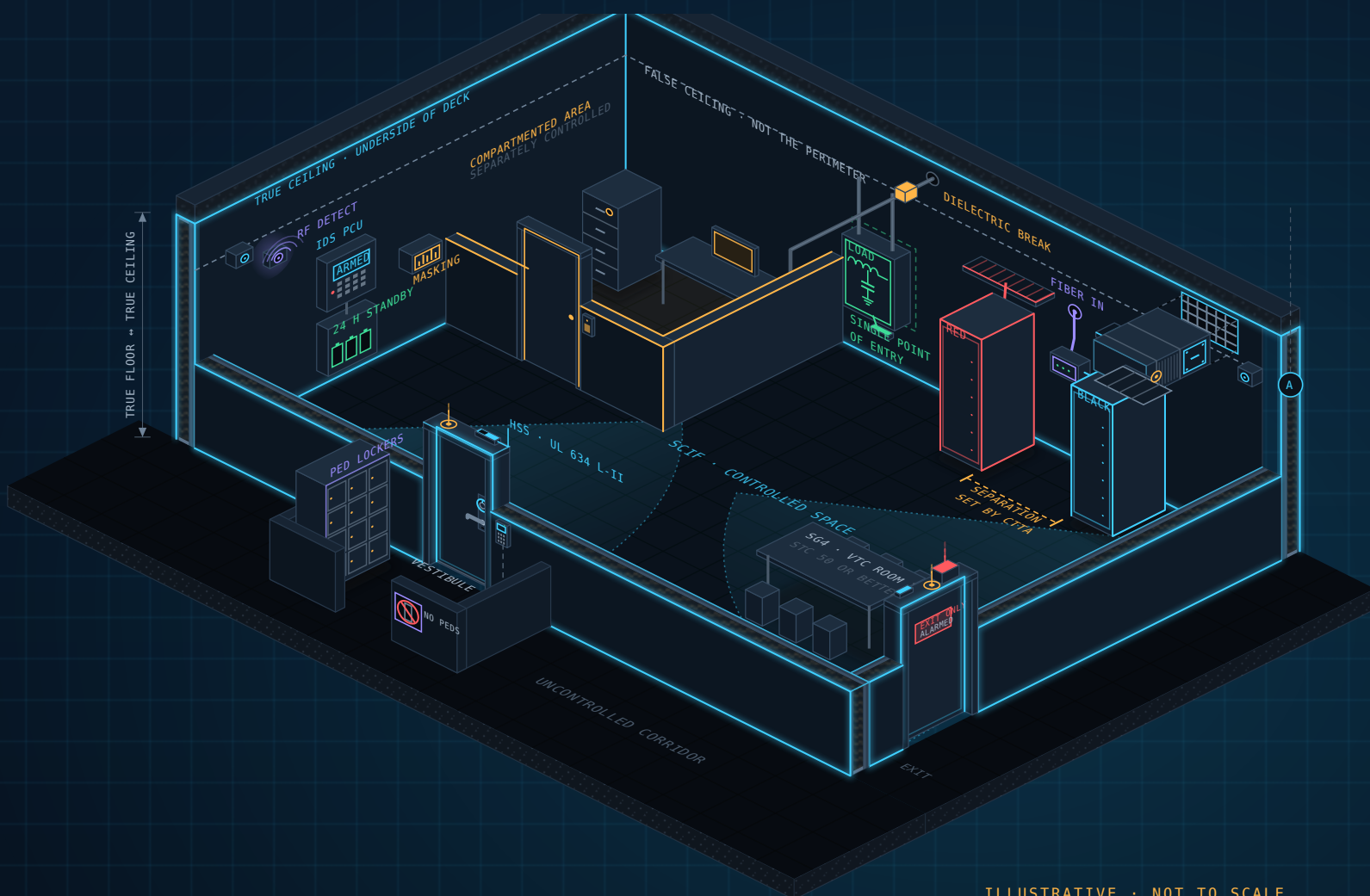
ICS 705-1 / 705-2

TECH SPEC v1.5.1

UL 2050 • EXTENT 3

SCIF & SAPF Security Primer

Public Edition. How accreditation, construction, intrusion detection, access control, acoustics and RED/BLACK discipline fit together, in plain English, with the published requirements behind every point.



ILLUSTRATIVE • NOT TO SCALE

FOR owners • architects • general contractors • low-voltage installers • security managers

LA CCTV Supply • PO Box 4327, La Puente, CA 91747 • 1-626-789-2267 • lacctvsupply.com • Since 2009



READ THIS FIRST · IMPORTANT NOTICE

Educational, public-level information. This primer explains the published, publicly released baseline for Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program Facilities (SAPFs). It is not a design standard, a specification, legal advice or a substitute for the documents it cites.

- **Not affiliated with or endorsed by** ODNI, NCSC, DoD, DCSA, DIA, NSA or UL Solutions. Names of agencies, standards and products are used for identification only.
- **Your AO / CSA / CTTA sets requirements.** Your Accrediting Official, Cognizant Security Authority and Certified TEMPEST Technical Authority decide what applies to your facility, and their written direction controls your project.
- **Nothing here is FOUO, CUI or classified.** Restricted TEMPEST documents are named but never reproduced. No RED/BLACK separation distances, shielding attenuation requirements, facility addresses or filled-in checklists appear in this document.
- **Historical documents are labeled.** Superseded or FOIA-released material is cited for context only, never as a current requirement.

Do not send classified information, CUI or facility addresses by unencrypted email, including to us. The combination of an address and “SCIF” is itself protected information in DoD. Ask your AO for the approved channel.

How to use this primer

Chapters 1–5 are the frame: what a SCIF is, the documents, the people and the accreditation path. Chapters 6–14 follow the build from perimeter to turnover. Chapter 15 collects the traps that most often delay accreditation, and Chapters 16–17 are the glossary and the official reference library with links.

Paragraph citations (for example **Tech Spec 3.G.7** or **UFC 3-4.6.5**) let you find the exact text in the source. Every chapter ends with its sources. Current versions used throughout: **ICD 705** (26 May 2010), **ICS 705-1** (17 Sep 2010), **ICS 705-2** (22 Dec 2016), **IC Tech Spec v1.5.1** (26 Jul 2021), **DoDM 5205.07** consolidated (17 Jan 2025), **UL 2050 Edition 6** (7 Apr 2025), **32 CFR Part 117** and **UFC 4-010-05** (26 May 2023).

SCIF & SAPF SECURITY PRIMER · PUBLIC EDITION
SEPTEMBER 2026 · CONTENT CURRENT TO PUBLIC SOURCES CHECKED SEPTEMBER 2026
PUBLISHED BY LA CCTV SUPPLY · PO BOX 4327, LA PUENTE, CA 91747 · 1-626-789-2267 · LACCTVSUPPLY.COM

Reading the callouts

TRAP A mistake that fails inspection or causes rework.

FIELD NOTE A practitioner tip for installers, GCs and designers.

VERIFY WITH YOUR AO The requirement varies by AO or CSA, or is not publicly fixed.

PLAIN ENGLISH A short explanation for non-specialists.

HISTORICAL Superseded or FOIA-released material. Context only; never a current requirement.

Who this is for

If you are a...	Start with
Owner or sponsor	Ch. 1, 4, 5 and 15
Architect / engineer	Ch. 6, 8, 9 and 12
General contractor	Ch. 7, 8, 14 and 15
Low-voltage installer	Ch. 10, 11, 12 and 13
Security manager	Ch. 3, 4, 10 and 13

Figures

All figures are original schematic illustrations drawn for teaching. They are **illustrative and not to scale**. Build only to your stamped, AO-approved drawings, the CTTA’s TEMPEST Countermeasures Review and manufacturer installation instructions.

Companion download

RED/BLACK, Filters & Shield Penetrations: Field Guide for GCs & Installers expands Chapter 12 with installer methods: line vs load, bonding, stored charge, waveguides, fiber entries, fastening without breaching the shield, and pre-test hold points.

Contents

Seventeen chapters, read in order or by role. Chapters 1–5 are the frame; 6–14 are the build; 15–17 are the tools you will keep open.

01	What SCIFs & SAPFs are	4
02	The document stack	5
03	Roles & responsibilities	7
04	The accreditation lifecycle	8
05	Facility types, modes & Security-in-Depth	10
06	Perimeter, walls & vaults	11
07	Doors, locks & containers	13
08	Penetrations, utilities & life safety	14
09	Acoustics & sound masking	15
10	Intrusion detection & UL 2050 / Extent 3	17
11	Access control & identity	18
12	RED/BLACK, EMI filters & shield penetrations	20
13	PEDs, telecom & CCTV	21
14	Construction security & build sequence	22
15	Top traps	23
16	Glossary of 60 key terms	24
17	Reference library	26

The one-sentence version

A SCIF is proven, not purchased: an Accrediting Official accredits a documented facility after the right people approved the design, watched the build and tested the systems.

Three gates that never move

Coordinate with the AO before design, orders or contracts. No construction award without an approved CSP. No SCI in the space before the accreditation letter.

Three things nobody can certify

A product as “ICD 705 certified.” A room as “TEMPEST compliant” without a CTTA. A panel as “UL 2050 listed”: UL 2050 certifies the alarm service company.

CHAPTER 01 FOUNDATIONS

What SCIFs & SAPFs are

A SCIF is a room, suite or building that a government Accrediting Official has formally approved for Sensitive Compartmented Information. The approval, not the construction, makes it a SCIF. A room built “to ICD 705” but never accredited is just an expensive room.

Accreditation, not construction

ICD 705 (26 May 2010) requires that SCI be handled only in accredited SCIFs, that SCIFs meet uniform Intelligence Community (IC) standards, and that they be built for reciprocal use across IC elements. Facilities must be accredited *before* SCI operations begin. DoD puts it bluntly: “SCI will not be discussed or introduced into the proposed SCIF until the facility is accredited” (DoDM 5105.21 Vol. 2).

Every SCIF also has a **mode** (closed storage, open storage or continuous operation) and may be a lesser **type** (SWA, TSWA, T-SCIF). Those choices drive walls, alarm response and cost (Chapter 5).

Where SAPFs fit

A Special Access Program Facility (SAPF) protects SAP information. Its current governing manual is the consolidated **DoDM 5205.07** (17 Jan 2025), which cancelled the 2015 Volume 3 on physical security. A **SAPF Accrediting Official**, appointed in writing by the Cognizant Authority SAP Central Office, approves preconstruction plans and inspects and accredits the facility.

SAPFs are built to the *equivalent* Tech Spec criteria, and DCSA's January 2026 SAP checklist cites Tech Spec Chapter 7 throughout for SAPF intrusion detection. A SAPF may be accredited as a SCIF after

TABLE 1.3 · ACRONYMS THAT MEAN TWO THINGS

Term	In ICD 705 / IC documents	The other meaning you will meet
SSM	Site Security Manager: owns security during planning, design and construction; writes the CSP	Used loosely for whoever runs day-to-day SCIF security (that is the SSO / SSR or CSSO)
CSA	Cognizant Security Authority: the official over the SCI security program	NISPOM Cognizant Security Agency: DoD, DOE, NRC, ODNI, DHS
CSSO	SCI: Contractor Special Security Officer	SAP: Contractor SAP Security Officer
CUA	Co-Use Agreement between AOs (Tech Spec 12.N-P)	Misread as a “controlled unclassified area”
AO	Accrediting Official for the facility	Authority to Operate (ATO) for a networked system under RMF, a separate approval
Extent	UL 2050 Extent 3: an alarm installation designation	Not a TEMPEST, RF or acoustic rating; web “Extent 1–5” ladders conflict with 32 CFR 117.15

the AO reviews all required SCIF construction documentation (Tech Spec 1.B.2). Moving SAP into a SCIF, or SCI into a SAPF, requires a Co-Use Agreement first.

TRAP No product, wall system, door or alarm panel is “ICD 705 certified.” The AO accredits the *facility*, based on documented construction, testing and procedures.

What a SCIF is not

- **A NISPOM open storage area** (formerly “closed area”): protects collateral classified information and is approved by DCSA. SCI cannot enter without SCI accreditation.
- **A GSA-approved container:** storage equipment, not a facility. A closed storage SCIF *uses* containers inside an accredited perimeter.
- **A vault:** a construction method (Tech Spec 3.C.5; FED-STD 832) that may sit inside or form part of a SCIF.
- **A “SCIF-ready” modular product:** the Tech Spec warns such claims “may not be accurate.”
- **An RF-shielded room:** shielding is one possible TEMPEST countermeasure a CTTA may recommend. It accredits nothing.

TRAP A DCSA-approved open storage area is not a SCIF, and a SCIF accreditation does not by itself authorize SAP. Co-use needs a signed agreement first (Chapter 4).

FIELD NOTE The first question on any project is “**Who is the AO?**” The answer tells you which manual applies, which forms and channel to use, and whose inspection you are building toward. Ask the government sponsor; don't guess from the contract name.

VERIFY WITH YOUR AO This primer explains the published baseline. Many items are left to AO or CSA determination; exceeding a published standard requires a waiver. Their written direction controls.

TABLE 1.1 · SCIF VS SAPF VS NISPOM OPEN STORAGE AREA VS GSA CONTAINER · PUBLISHED BASELINES; MANY ITEMS ARE LEFT TO AO OR CSA DETERMINATION, AND EXCEEDING A PUBLISHED STANDARD REQUIRES A WAIVER

Attribute	SCIF	SAPF	NISPOM open storage area	GSA-approved container
Protects	SCI	SAP information	Collateral classified (contractor)	Collateral; SCI when inside a closed storage SCIF
Governing documents	ICD 705, ICS 705-1/-2, IC Tech Spec; DoDM 5105.21 in DoD	DoDM 5205.07 (17 Jan 2025), built to equivalent Tech Spec criteria	32 CFR 117.15; construction per 32 CFR 2001.53	32 CFR 2001.43; DoD Lock Program specs
Who approves	IC element AO (DIA for most DoD and DoD contractors)	SAPF Accrediting Official	DCSA approves the space and IDS before installation	Must be GSA-approved; supplemental controls per 2001.43
IDS installation	UL 2050 Extent 3 TS 7.A.2.b	UL 2050 Extent 3 DCSA F-30	Extent 3 baseline; Extent 5 only with CSA approval	No IDS sensors on the container itself 117.15(d)(4)
Alarm response (TS / SCI)	Closed 15 min; open 15 min with SID, 5 min without	Same as SCIF	TS open storage: 15 min with SID, 5 min without	2-hour checks, or IDS with 15-min response, or SID + FF-L-2740 lock
Reciprocity	Mandatory across IC elements if no waivers	May be accredited as a SCIF on documentation review; co-use needs a CUA	Not applicable	Not applicable

TABLE 1.2 · THE THREE THINGS EVERY ACCREDITATION PACKAGE PROVES

Pillar	What must be demonstrated	Typical evidence	FFC v1.5 sections
Physical	The perimeter resists and shows evidence of penetration; doors, locks and penetrations meet the Tech Spec; speech does not leave the room	As-built drawings, wall and penetration details, photographic construction record, door and hardware schedule, acoustic test data	B Security-in-Depth · C SCIF Security · D SCIF Doors · G Acoustical Protection
Technical	Intrusion detection, access control, telecom and emanations risks are controlled	UL 2050 certificate, IDS spec sheets and acceptance tests, encryption certificate, telecom baseline, TEMPEST Checklist and the CTTA's review	E IDS · F Telecom Systems & Equipment Baseline · I INFOSEC / TEMPEST / Technical Security
Procedural	People run the space correctly every day	SOP, emergency plan, Construction Security Plan, destruction methods, visitor and combination control, end-of-day checks (SF 701/702)	A General Information · H Classified Destruction Methods · plus SOP and plans

SOURCES ICD 705 · IC Tech Spec v1.5.1 · DoDM 5105.21 Vol. 2 · DoDM 5205.07 (2025) · 32 CFR 117.15 · 32 CFR 2001.43 · DCSA SAP Checklist (Jan 2026) · UFC 4-010-05

CHAPTER 02 FOUNDATIONS

The document stack

One directive sets policy, two standards set the rules, and one technical specification tells you how to build and run the space. DoD, the State Department and the SAP community layer their own manuals on top. Read top-down for authority and bottom-up for method.

The Tech Spec, chapter by chapter

Chapter 1 Introduction · 2 Risk management (SID, compartmented areas) · 3 **Fixed facility construction** (inside the U.S.) · 4 Outside the U.S., not under Chief of Mission · 5 Under Chief of Mission · 6 Temporary, airborne, shipboard · 7 **Intrusion detection** · 8 **Access control** · 9 **Acoustics** · 10 PEDs · 11 Telecommunications · 12 Management & operations · 13 Second Party intergee & liaison spaces (new in v1.5.1) · 14 **Forms and plans**.

The v1.5 and v1.5.1 change histories list no Chapter 7 (IDS) changes. Co-use sections N–P sit above the Chapter 13 heading in the v1.5.1 contents but belong to Chapter 12 (12.N–12.P).

Version traps that show up in specs and proposals

- “**The 2020 Tech Spec.**” That is v1.5 (cover date 13 Mar 2020). The current public version is **v1.5.1**, which moved Forms and Plans to Chapter 14.
- “**DoDM 5205.07 Volume 3 governs SAPFs.**” Volume 3 (23 Apr 2015) was cancelled by the consolidated manual effective 17 Jan 2025.
- “**Extent 3 is in the Tech Spec.**” Extent 3 is a **UL 2050** installation designation; Tech Spec 7.A.2.b points to it.
- “**DCSA will accredit our SCIF.**” DCSA administers the NISP for collateral work. It does not accredit SCIFs or SAPFs.

- “NISPOM closed area.” 32 CFR Part 117 replaced closed areas with **open storage areas**. UL’s alarm form still says “closed area.”
- “Exceeding the standard is always safe.” Tech Spec 2.A: exceeding a standard, even based on risk, requires a waiver, and a waiver ends mandatory reciprocity.

HISTORICAL DCID 6/9 (rescinded by ICD 705 in 2010) and JAFAN 6/9 still appear on legacy forms and older specifications, and FOIA-released TEMPEST documents such as NSA 94-106 and NSTISSAM TEMPEST/2-95 circulate online. Treat all of them as context, never as current requirements.

VERIFY WITH YOUR AO Since 2025, industry sources have reported non-public ODNI direction on SCIFs, focused on TEMPEST and RF protection and on re-accrediting older facilities, and later a reported partial rescission. None of it was publicly posted as of September 2026, and the public Tech Spec remains v1.5.1. Ask your AO in writing whether your facility can be re-accredited under the standards in force at its last accreditation.

TABLE 2.1 · CURRENT PUBLIC VERSIONS, CHECKED SEPTEMBER 2026

Layer	Document	Current public version	What it does
Directive	ICD 705, <i>SCI Facilities</i>	26 May 2010	SCI only in accredited SCIFs; AO and waivers; reciprocity
Standard	ICS 705-1, <i>Physical & Technical Security</i>	17 Sep 2010	The “shall” standards: perimeter, IDS, ACS, TEMPEST, PEDs, telecom
Standard	ICS 705-2, <i>Accreditation & Reciprocal Use</i>	22 Dec 2016	Accreditation, re-evaluation, de-accreditation, co-use
Specification	IC Tech Spec for ICD/ICS 705	v1.5.1, 26 Jul 2021	Build-to document; FFC, TEMPEST Checklist, CSP and other forms
DoD SCI	DoDM 5105.21 Vol. 2	2012, Change 2 (2020)	DoD SCIF physical security; DIA accredits for most of DoD
DoD SAP	DoDM 5205.07, <i>SAP Security Manual</i>	17 Jan 2025	Consolidated manual; SAPF physical security in Section 15
DoD design	UFC 4-010-05, <i>SCIF/SAPF Design</i>	26 May 2023	A-E and GC design detail; implements, never overrides, the Tech Spec
Collateral	32 CFR Part 117 (NISPOM) and Part 2001	Current eCFR	Contractor safeguarding, open storage areas, IDS response
Alarm	UL 2050, <i>National Industrial Security Systems</i>	Ed. 6, 7 Apr 2025	Alarm company certification; the Extent 3 installation
State Dept.	12 FAM 710; OSPB standards in 12 FAH-6	Current FAM	Chief of Mission SCIFs; the more stringent standard applies

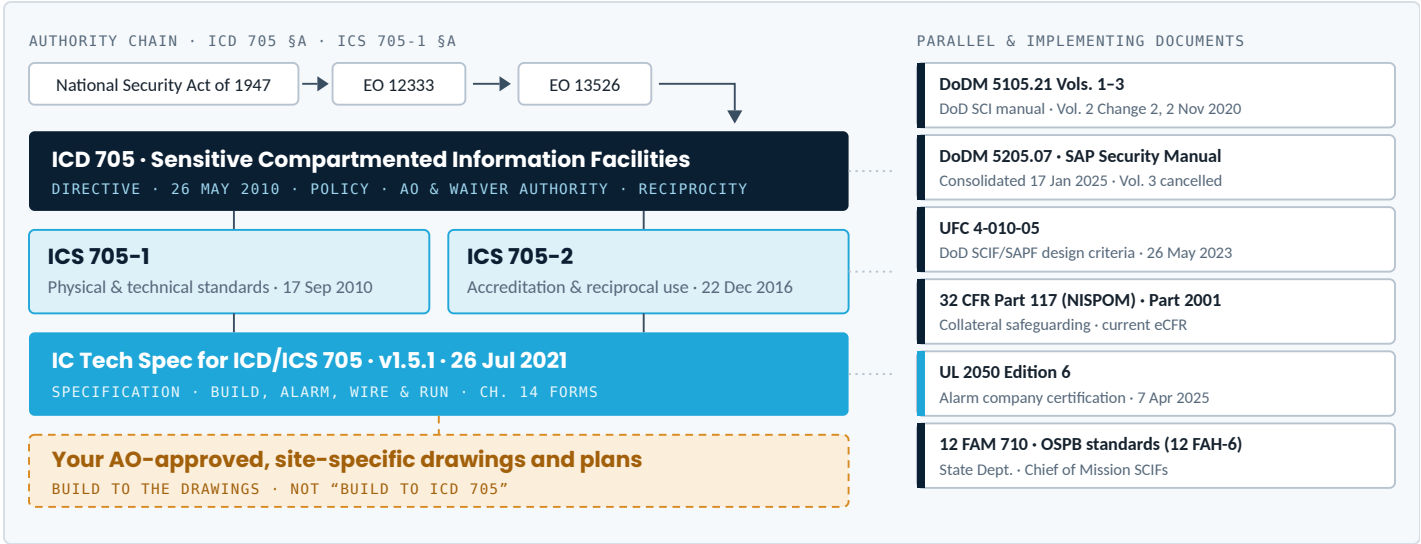


Figure 2.1 · The SCIF document stack. Authority flows down the left column; implementing and parallel documents sit alongside. Where layers disagree, the stricter applicable requirement and your AO’s written direction win.

ILLUSTRATIVE — NOT TO SCALE

SOURCES NCSC Security Governance & Regulations · ICD 705 · ICS 705-1 · ICS 705-2 · IC Tech Spec v1.5.1 · DoDM 5205.07 (2025) · UFC 4-010-05 · UL 2050 Ed. 6 · 12 FAM 710 · SAME 2026 (practitioner)

CHAPTER 03 FOUNDATIONS

Roles & responsibilities

Three groups touch every SCIF. **Deciders** approve: the IC element head, AO, CSA, the CTTA for TEMPEST and the AHJ for life safety. **Security staff** plan and run the space: SSM, SSO, SSR, CSSO and CSTs. **Builders** produce the evidence: designer, general contractor and integrator. Builders never approve their own work.

Separation rules that invalidate approvals

- **The AO does not grant waivers.** ICD 705: “In no case may this official be the same person as the Accrediting Official.” Approved waivers are reported to the Director, NCSC within 30 days.
- **The CTTA recommends; the AO approves.** Integrators, shielding vendors and architects do not decide TEMPEST countermeasures.
- **SSM means Site Security Manager** in ICS 705-1 and the Tech Spec: planning, design and construction only. Operations belong to the SSO/SSR (government) or CSSO (contractor).
- **DCSA does not accredit SCIFs.** DIA provides physical and TEMPEST accreditation for DoD components and most DoD contractors; NSA, NGA and NRO accredit under their own cognizance.
- **The GC cannot approve field changes to the perimeter.** Deviations go through the SSM to the AO.
- **The AO cannot waive a fire code.** Life safety is the AHJ’s determination (Tech Spec 3.E.5), and neither office can waive the other’s requirements.
- **A commercial bug sweep is not accreditation TSCM.** TSCM for accreditation is requested through the AO and, as quoted in a practitioner summary (Armag) of Tech Spec 12.G.8, “will only be conducted by USG TSCM teams.”

TRAP Treating the AO as a final inspector who appears at the end. The Tech Spec requires AO coordination “before construction design, material ordering, or contracts are finalized.” Late engagement is one of the most expensive failures on SCIF projects.

- IDS installation, components and monitoring stations comply with **UL 2050**; installation is **Extent 3** (Tech Spec 7.A.2.a–b).
- Contractor SCIFs “shall maintain a current UL certificate of installation and service,” renewed after IDS changes (ICS 705-1).
- Installation and testing inside the U.S. by **U.S. companies using U.S. citizens** (Tech Spec 7.D.1; UFC 1-18.1).
- System variables and passwords restricted to SCI-indoctrinated U.S. personnel (7.A.2.j); maintenance staff TOP SECRET-cleared or escorted, with repairs started within 4 hours of a trouble signal (7.C.2).
- The DoD package includes IDS specification sheets, the UL 2050 certificate, the NIST encryption certificate and IDS test results (DoDM 5105.21 Vol. 2).

An integrator does **not** accredit the space, approve the design, decide TEMPEST countermeasures or overrule life safety, and should never self-certify a room as “SCIF compliant.”

FIELD NOTE Put the SSM on every design meeting invite and RFI distribution, and put a one-page responsibility matrix in the CSP appendix: every named person, their role, clearance level and what they may approve. Hand the SSO an IDS/ACS turnover binder at accreditation: zone map, test records, battery log, code-change record and catastrophic failure plan inputs.

VERIFY WITH YOUR AO TEMPEST vulnerabilities associated with a physical location are classified at a minimum of CONFIDENTIAL (UFC 4-010-05 1-16.3). Never circulate a CTTA’s site findings on unclassified channels.

Where a low-voltage integrator fits

The integrator’s work is some of the most heavily documented in the package, because the IDS is the detection layer when nobody is inside. What the public documents require of that scope:

TABLE 3.1 · WHO PRODUCES AND WHO SIGNS

Role	Primary phase	Produces	Approves or signs
IC element head	All	Delegations	Original accreditation authority; waivers, or delegates them to a named senior official who is not the AO
Accrediting Official (AO)	All	Waiver requests; letters of accreditation	Design concept, CSP and final design; accreditation, re-accreditation, de-accreditation
Cognizant Security Authority (CSA)	Oversight	Repository data; re-evaluation schedule	Co-use concurrence; in DoD Services, concept approval and TSWAs/T-SCIFs
SAPF Accrediting Official	SAP facilities	—	SAPF preconstruction plans; SAPF accreditation (DoDM 5205.07)

TABLE 3.1 · WHO PRODUCES AND WHO SIGNS

Role	Primary phase	Produces	Approves or signs
Site Security Manager (SSM)	Planning → accreditation	CSP; inspection reports; violation notices to the AO within 3 business days; assembled accreditation documents	— (advises the AO)
SSO / SSR / CSO	Operations	SOP, emergency plans, SF 701/702 records, posture-change reports, withdrawal requests	Occasional conference-room use without a Co-Use Agreement (SSO)
CTTA	Planning & design	TEMPEST Countermeasures Review (TCR) with recommendations	Recommends ; the AO approves
CST, cleared guards, escorts	Construction	Surveillance logs; screening and escort records	—
TSCM team (U.S. Government)	As required	TSCM report	—
Designer of record (A-E)	Design	Drawings and project data for the SSM (UFC 1-19.1)	—
General contractor	Construction	Work per approved drawings and CSP; photographic record	—
IDS / low-voltage integrator	Install & test	UL 2050 certificate, spec sheets, acceptance test results, turnover records	—
Authority Having Jurisdiction (AHJ)	Design → occupancy	—	Building code, fire and accessibility compliance

SOURCES ICD 705 · ICS 705-1 · ICS 705-2 · IC Tech Spec v1.5.1 · DoDM 5105.21 Vol. 1 · DoDM 5105.21 Vol. 2 · DoDM 5205.07 (2025) · UFC 4-010-05 · Armag v1.5 summary (practitioner)

CHAPTER 04 FOUNDATIONS

The accreditation lifecycle

Accreditation is not a certificate you collect at the end of construction. ICS 705-2 calls it “the beginning of a life-cycle process of continuous monitoring and evaluation, periodic re-evaluations, and documentation reviews.” Most failures trace back to steps skipped at the start.



Figure 4.1 · The lifecycle in four phases and seventeen steps. Steps 3 through 8 normally precede contract award; CSP approval always does. Exact submittals and sequence vary by agency; your AO sets them.

ILLUSTRATIVE — NOT TO SCALE

Plan: sponsor, concept, risk and TEMPEST

A SCIF exists to meet a government mission need, so every project needs a sponsor and an identified AO before design starts. For a DoD SCIF, the commander requests SCI from the Service CSA, designee or senior intelligence official, and “proof of sponsorship in the form of a SCIF number or written documentation of Concept Approval ... is required” (UFC 4-010-05 2-2.1). SAPF sponsorship is generally formalized at the program level.

The AO and SSM assess “threats, vulnerabilities, and assets to determine the most efficient countermeasures” and document Security-in-Depth. The **Pre-Construction Checklist** (added in v1.5) gives the AO project data, points of contact and the “security in-depth starting point location.” If classified information will be processed electronically, the **TEMPEST Checklist** goes to the CTTA during planning, and the answer, the TEMPEST Countermeasures Review, may add filtering, dielectric breaks or shielding.

Design and approve: two gates before work

The AO must “review and approve the design concept, Construction Security Plan (CSP), and final design ... prior to the start of SCIF construction” (Tech Spec 3.A). UFC 4-010-05 1-15 is blunt: “Do not award a construction contract without an approved CSP.” The CSP template’s baseline “may not be reduced without coordination and approval.”

Build and prove: the evidence trail

Inspectors cannot see inside finished walls, so the evidence is created now or never: SSM inspections for the duration of the project, violation notices to the AO within 3 business days, CST logs where required, and a photographic record of penetrations, door installations and wall assemblies (UFC 4-7). Systems testing produces the most paper: IDS acceptance tests (Tech Spec 7.D.3), the UL 2050 certificate, encryption certificates and acoustic results. The final FFC, SOP, emergency plan and (in DoD) catastrophic failure plan complete the package.

TRAP Moving furniture, IT equipment or people in and “starting quietly” before the letter arrives. Introducing SCI before accreditation is a security violation, not a schedule shortcut.

What the letter says, and what it does not

The letter of accreditation (ICS 705-2 §D.1.a) states the SCIF identity, type (for example open or closed storage), effective date, compliance with physical, TEMPEST and technical standards, and any waivers

with the standard not met and when it will be. It enables SCI operations within that type and perimeter, reciprocal acceptance if there are no waivers, and co-use under a signed agreement. It does **not** authorize SAP, a different storage mode or a larger perimeter.

Operate: monitoring, re-evaluation, change

Continuous monitoring means SF 701 and SF 702 checks, random after-hours inspections at least monthly, posture changes reported to DIA’s accreditation office within 24 hours (DoD), and semiannual IDS tests with records kept two years. The CSA ensures periodic re-evaluations “or at least every five years” (ICS 705-2 §D.3.a). Re-accreditation is required for “major modifications to the SCIF, changes to the sensitivity of programs, or to the threat” (§D.4.b); in DoD that includes perimeter changes, storage-mode changes and leaving continuous operation.

VERIFY WITH YOUR AO The legacy SAPF re-inspection interval (“no less frequently than every 3 years”) could not be confirmed in the public text of the 2025 consolidated DoDM 5205.07. Ask the SAPF Accrediting Official.

Waivers, co-use and closeout

A waiver is limited to “exceptional circumstances” or a documented mission need to *exceed* a standard. The package states the standard affected, mitigations considered, justification, residual risk, compensating procedures, a compliance timeline and acceptance of lost mandatory reciprocity (ICS 705-1). DoD waivers normally last up to one year.

A **Co-Use Agreement** is signed by both parties’ AOs and is required for each contractor contracting effort; the tenant accepts the host accreditation and pays for changes it needs. Short-term exceptions: temporary SCI storage for another organization up to seven calendar days, and occasional conference-room use approved by the SSO. A SCIF de-accredited but held at SECRET for less than one year may be re-accredited (Tech Spec 1.B.1).

FIELD NOTE Walk the space with the SSM a week before inspection, using the FFC as the script: test every door switch, walk-test motion coverage, confirm the monitoring station receives each signal, and confirm the certificate, the response agreement and FFC Section E show the same response time. Inspectors compare documents against each other as well as against the room.

SOURCES ICS 705-2 · ICS 705-1 · IC Tech Spec v1.5.1 · Pre-Construction Checklist v1.5 · Fixed Facility Checklist v1.5 · CSP v1.5 · UFC 4-010-05 · DoDM 5105.21 Vol. 2 · CDSE SA501

Facility types, modes & Security-in-Depth

“SCIF” is the family name. The **storage mode** decides where SCI sits when nobody is working; the **facility type** decides how long the space is accredited and whether it stores anything at all; **Security-in-Depth** decides how much credit the surroundings earn. Each choice changes walls, alarm response and cost.

Choosing a mode

Closed storage allows the standard wall and a 15-minute response without relying on SID. The trade-off is operational: every classified item, including equipment and media, goes into a container at the end of the day. UFC 4-010-05 is explicit that closed storage “includes all classified materials, equipment and information.”

Open storage lets equipment, media and documents stay in place, which suits operations centers and heavy IT use. The cost is either a qualifying SID layer the AO accepts, or hardened walls plus a

response force that can arrive in five minutes, which in practice often means an on-site guard force. In DoD, changing storage mode later requires re-accreditation.

SWAs suit briefing rooms and conference space next to an existing SCIF: when unoccupied, all SCI is removed to containers “within a SCIF, a vault, or be destroyed.” A **TSWA** is part-time and short-term; its extension “requires a plan to accredit as a SCIF or SWA.”

TRAP

“Closed storage” (a SCIF mode where SCI lives in containers) and “closed area” (the legacy NISPOM term for a room where collateral material sat *in the open*) mean nearly opposite things.

TABLE 5.1 · FACILITY TYPES AT A GLANCE

Type	Definition (short)	Storage?	Duration	SAP twin	Source
Closed storage SCIF	All SCI (including classified equipment) stored in GSA-approved containers inside the facility	Containers only	Until de-accredited	SAPF	ICS 705-1; UFC 1-11.4
Open storage SCIF	SCI may be openly stored and processed without GSA containers; the room is the safe	Yes, in the open	Until de-accredited	SAPF	ICS 705-1
Continuous operation	“Staffed and operated 24 hours a day, seven days a week”	Per accreditation	Until de-accredited	SAPF	ICS 705-1
Secure Working Area	Discussing, handling or processing SCI “but where SCI will not be stored”; 15-min initial response	No	No time limit (DoD)	SAPWA	Tech Spec 3.I
Temporary SWA	SCI use “less than 40-hours per month”; accreditation “12 months or less”	No	≤ 12 months	SAPTSWA	Tech Spec 3.J
Temporary SCIF	For “tactical, emergency, or immediate operational requirements”	Per approval	DoD: up to 1 year	T-SAPF	ICS 705-1; DoDM 5105.21
Compartmented Area	Rooms inside a SCIF that separate compartments or programs; Types I-III (only Type III stores); no independent alarm system (2.C.4)	Type III only	With parent SCIF	SAPCA	Tech Spec 2.C
Vault	Storage room built to Tech Spec 3.C.5 (or FED-STD 832 for collateral)	Yes	With parent	—	Tech Spec 3.C.5

TABLE 5.2 · HOW THE PROFILE DRIVES THE PERIMETER WALL AND ALARM RESPONSE (INSIDE THE U.S.)

SCIF profile	Perimeter wall (Tech Spec 3.C)	Initial response force (3.H)	Then
Closed storage	Wall A (standard)	15 minutes	An SCI-indoctrinated person arrives within 60 minutes (UL 2050) or the AO-approved time 7.C.1.c
Secure Working Area	Wall A	15 minutes	
Open storage with AO-accepted SID	Wall A	15 minutes	
Open storage without SID	Wall B or Wall C (enhanced)	5 minutes	
Continuous operation	Wall A	Not separately stated in 3.H. Get the AO’s determination in writing and record it on the FFC.	

Security-in-Depth: the credit for what surrounds you

Tech Spec 2.B.1: “SID describes the factors that enhance the probability of detection before actual penetration to the SCIF occurs.” It “may alter construction requirements with AO approval” and can “extend security alarm response time to the maximum of 15 minutes.” At least one primary means is required (2.B.3):

1. A military installation, embassy compound, U.S. Government compound, or contractor compound with a dedicated U.S. response force.
2. A controlled building with separate building access controls, alarms and elevator controls.
3. Controlled office areas adjacent to or surrounding the SCIF, protected by alarm equipment.
4. A fenced compound with access-controlled vehicle and/or pedestrian gates.

SID is **documented, not assumed**: on FFC Section B (including external CCTV coverage maps), in the CSP’s SID block and on the Pre-Construction Checklist. SID is mandatory outside the U.S. (2.B.2) and “desired for all SCIF or SAPF” under UFC 4-010-05 1-12.

TRAP Treating SID as a building amenity rather than an accreditation condition. When a landlord removes lobby access control, a new tenant mix arrives or a campus gate moves, an open storage SCIF may suddenly need a 5-minute response it cannot meet. Report SID changes to the AO before they happen.

FIELD NOTE Building access control, corridor CCTV and guard posts are the SID evidence an integrator can most directly strengthen. Provide coverage maps and system descriptions for FFC Section B, while keeping cameras outside the SCIF perimeter.

Three construction regimes

Chapter 3 covers SCIFs inside the U.S. **Chapter 4** covers SCIFs outside the U.S. not under Chief of Mission authority: SID is mandatory, construction criteria follow threat Category, CSTs hold U.S. TOP SECRET clearances, and materials move under secure procurement, transport and storage. **Chapter 5** covers Chief of Mission facilities, governed by ICDs and Overseas Security Policy Board standards in 12 FAH-6; the more stringent standard applies.

Category is set from the State Department’s Security Environment Threat List **technical** threat rating: **Category I** “Critical or High Technical Threat, High Vulnerability Buildings”; **Category II** “High Technical Threat, Low Vulnerability Buildings”; **Category III** “Low and Medium Technical Threat.” There is no Category IV, and open storage “is to be avoided” in Category I (and in Categories I and II under Chief of Mission).

VERIFY WITH YOUR AO The AO provides your site’s Category through appropriate channels. Never publish, email or put in a proposal which Category a country or post falls into; threat-location associations can be classified. This primer lists no countries.

SOURCES ICS 705-1 · IC Tech Spec v1.5.1 · DoDM 5105.21 Vol. 2 · UFC 4-010-05 · 32 CFR 2001.43 · FFC v1.5 · DCSA Form 147 Guide · 12 FAM 710

CHAPTER 06 THE BUILD

Perimeter, walls & vaults

The perimeter is a sealed box: every wall, the true floor, the true ceiling, every door and window, and every duct, pipe and conduit through them. It is judged as a whole. A perfect wall with an untreated duct running through it is a failed perimeter.

What the perimeter must do

ICS 705-1 §G.1: the perimeter “shall provide a physical barrier to forced, covert and surreptitious entry,” with walls, floor and ceiling “permanently and solidly constructed and attached to each other,” providing “visual evidence of unauthorized penetration.” UFC 4-010-05 §3-3.2 adds that this “includes above the false ceilings and below raised floors.” A compliant perimeter does four jobs at once:

- **Resist** forced, covert and surreptitious entry (Tech Spec 3.C).
- **Show** visual evidence of any penetration: hard-finished, painted, inspectable surfaces.
- **Contain speech** to Sound Group 3 or 4 (Chapter 9).
- **Provide TEMPEST/RF protection** only when the CTTA recommends it (3.C.4).

PLAIN ENGLISH Standard SCIF walls are not built to stop a determined intruder with power tools. They are built so nobody can quietly get through, or plant something, without leaving marks. The IDS and response force supply the delay-and-response half; enhanced walls and vaults add real delay where storage risk is higher.

True floor to true ceiling

Every perimeter wall runs from the structural slab to the underside of the deck above; a wall that stops at a suspended ceiling is not a perimeter wall. The Tech Spec wall figures require the “entire wall assembly” to be “finished and painted from true floor to true ceiling.” At the top and bottom that means:

1. 16-gauge continuous top and bottom track, anchors at 32 in. on center maximum, bedded in a continuous bead of acoustical sealant.

2. Remaining voids filled with fire-safe grout or acoustic sealant, including deck flutes.
3. The full height finished and painted, including the portion above any drop ceiling.

TRAP Walls that stop at the drop ceiling, or that leave open fluted-deck voids above the top track, fail both the slab-to-slab rule and the acoustic requirement. Discovering this after ceilings close usually means demolition.

Existing walls, fire ratings and RF

An existing wall of substantial material (brick, concrete, block) equal to the perimeter standard may be used with AO approval (Tech Spec 3.C.1), but it still must run slab to slab and every old sleeve must be found and treated. The Tech Spec figures are **security details, not listed fire-rated assemblies**; UFC 4-010-05 §3-4.1 requires fire-retardant-treated plywood in noncombustible construction and tells designers to make Tech Spec details comply with the building code.

RF protection “shall be installed at the direction of the CTTA when a SCIF utilizes electronic processing and does not provide adequate RF attenuation at the inspectable space boundary” (3.C.4), typically foil-backed wallboard or an approved radiant-barrier foil. ICS 705-1 wants it planned “during initial construction” because retrofit costs far more.

Ceilings, floors and plenums

Floors and ceilings meet “the same standards for force protection and acoustic protection as walls,” with penetrations “kept to a minimum” (Tech Spec 3.D). A drop ceiling or raised floor is a finish, not the perimeter. If an above-ceiling or raised-floor plenum connects to non-SCIF space, the true perimeter has a hole in it; the

AO may require plenum motion detection or other mitigation. Motion sensors “are not normally required above false ceilings or below false floors” in the U.S. (UFC 3-4.17.3).

Utilities on perimeter walls

On walls treated for acoustics or RF, interior distribution must be “surface mounted, contained in a raceway, or an additional wall” on furring stand-offs (Tech Spec 3.G.5). UFC 4-010-05 extends that to recessed outlet boxes and panels, and prohibits recessed fire extinguisher cabinets (§3-4.4.8) and recessed PED cabinets (§3-4.7) on perimeter walls.

FIELD NOTE Flag perimeter walls on the electrical and low-voltage sheets: “No recessed devices — surface raceway only.” Electricians and cabling crews build from their own sheets, not the architectural wall types. Ask the AO early whether it prefers surface raceway or an inboard furred wall; some prefer surface mount because furring hides the boundary.

Windows and the 18-foot rule

“Every effort should be made to minimize or eliminate windows in the SCIF, especially on the ground floor” (3.F.1). Windows are non-opening and provide visual and acoustic protection; RF treatment follows the CTTA. Windows **within 18 ft** of the ground or an accessible platform must meet the perimeter standard for forced entry and be alarmed per Chapter 7 (3.F.3, 3.F.5). UFC 4-010-05 §3-4.10 specifies visual protection by acid etching, sand blasting or an obscure PVB interlayer.

VERIFY WITH YOUR AO Whether a roof, ledge, canopy or parking structure counts as an “accessible platform” is an AO determination that can change the wall and IDS scope for an entire elevation. Get it in writing during site due diligence.

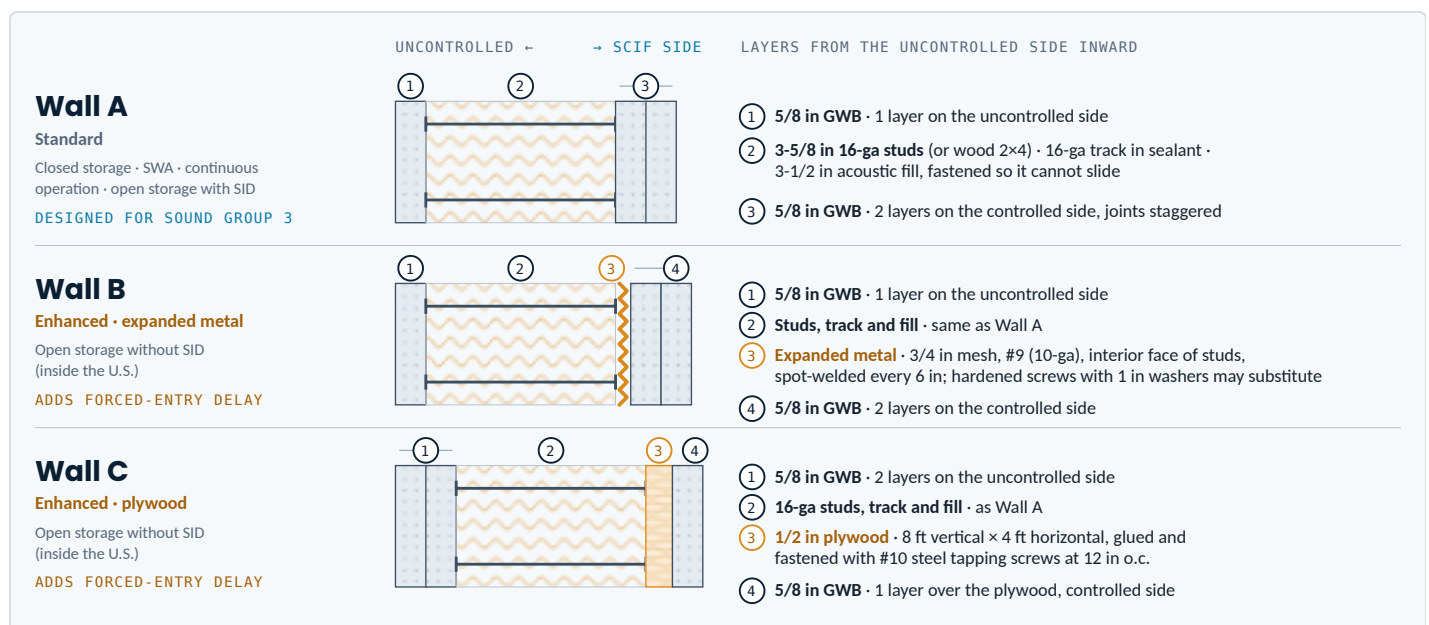


Figure 6.1 · Tech Spec perimeter wall types in plan section (after Tech Spec 3.C, Figures 1–3). Layer thicknesses exaggerated for legibility. The hardening layer always sits on the controlled side; a mirror-image install means rework.

ILLUSTRATIVE — NOT TO SCALE

TABLE 6.1 · VAULT CONSTRUCTION: TECH SPEC 3.C.5 VS FED-STD 832

Item	Tech Spec 3.C.5 (SCIF)	FED-STD 832 (collateral)
Modular	GSA-approved modular vault, AA-V-2737	Class B = AA-V-2737
Concrete	Min. 8 in reinforced; ≥ 2,500 psi; 5/8 in rebar 6 in o.c. each way, centered	Class A: 8 in reinforced; 28-day strength ≥ 3,000 psi
Steel-lined	1/4 in high-yield plate, continuously welded to load-bearing members	Class C: 3/8 in plate, continuously welded
Door	"GSA-approved Class 5 vault door"; ABA-equipped (UFC 3-4.6.11)	Class 5 vault door (AA-D-600)
Day access	A vault door cannot be day-access control; build a vestibule with an access control device (Tech Spec 3.E.6)	

TRAP Mixing Tech Spec and FED-STD 832 vault details on one drawing set. For a SCIF or SAPF the Tech Spec and your AO govern; the two standards use similar but not identical numbers.

VERIFY WITH YOUR AO The Tech Spec text reviewed sets no blanket rule requiring a vault for a U.S. SCIF. Vaults are a risk, program or threat-driven choice; confirm the storage method before design, because it changes structure, schedule and door procurement.

SOURCES ICS 705-1 · IC Tech Spec v1.5.1 · UFC 4-010-05 · FED-STD 832 · AA-V-2737 · Milham, ICD 705 lessons (practitioner)

CHAPTER 07 THE BUILD

Doors, locks & containers

A SCIF door is a reinforced pedestrian door, not a vault door. During the day an access control system controls its latch; at night an FF-L-2740 combination lock throws an FF-L-2890 deadbolt and the IDS stands guard. Most door findings are hardware selection or installation errors.

Every perimeter door

- Automatic, **non-hold** closer on the SCIF side; hinge pins accessible from outside secured against removal (3.E.5).
- Solid: "All perimeter doors must be solid with no lites or sidelites" (UFC 3-4.6).
- Alarmed with a **UL 634 Level II High Security Switch and a motion sensor** (7.A.2.d, 7.A.3.a(7)).
- Acoustic performance per Chapter 9 unless a declared non-discussion area; a vestibule is recommended "to preclude visual observation and enhance acoustic protection."
- TEMPEST requirements per CTTA guidance; life safety and accessibility per the AHJ.

Fabrication

Wood: 1-3/4 in solid core. Steel: 1-3/4 in thick with faces equal to 18-gauge minimum. Hinges reinforced to 7-gauge (cam-lift for acoustic assemblies), closer to 12-gauge, lock area predrilled or reinforced to 10-gauge (Tech Spec 3.E.6; UFC 3-4.6.1–6). DoD door **assemblies** are factory-tested per ASTM E90 to at least **STC 50** for an STC 45 perimeter, and **STC 55** for STC 50. Roll-up doors are 18-gauge steel, deadbolted on both sides inside and alarmed; double doors need the fixed leaf bolted top and bottom, an astragal and a **contact on each leaf**.

TRAP Ordering a standard hollow-metal door and adding reinforcement in the field, or assembling an "STC door" from separately rated parts. Reinforcement is factory work, and only the tested assembly (leaf, frame, seals, threshold, drop seal) carries the rating.

TABLE 7.1 · THE THREE PERIMETER DOOR CATEGORIES (TECH SPEC 3.E.1–3.E.4)

Category	Locking hardware	Access control and alarm	How many
Primary door	FF-L-2890 pedestrian deadbolt device plus an FF-L-2740 combination lock	Approved access control device (Ch. 8); by-pass keyway allowed for ACS failure; HSS + motion	One, where visitor control happens, unless the AO approves otherwise
Secondary door	FF-L-2890 egress device with deadbolt; no added standalone deadbolts	ACS "must be deactivated when the SCIF is not occupied"; HSS + motion	Only with AO authorization
Emergency egress-only	FF-L-2890 exit-only device; no exterior hardware	Alarmed 24/7 with a local audible annunciator; no entry capability	As the building code and AHJ require

The locks: FF-L-2740B and FF-L-2890C

FF-L-2740B electromechanical combination locks resist 20 man-hours of surreptitious entry and 30 man-minutes of covert entry, with at least 1,000,000 combinations; sales are restricted to the government and authorized contractors. Current approved models are the **Kaba Mas X-10** (self-powered dial) and **Sargent & Greenleaf 2740B**. **FF-L-2890C** (22 Feb 2019) defines ten lock-extension types: primary doors use Types I-IV, rooms not regularly occupied V-VI, secondary doors VII-VIII, and exit-only doors IX-X. QPL-FF-L-2890-5 (21 Mar 2022) lists Kaba Mas CDX-10, the Lockmasters LKM10K series and the S&G 2890 series.

VERIFY WITH YOUR AO The DoD Lock Program posts revision C as current; one industry source reports a later revision. The Tech Spec requires “the most current version,” so confirm the revision and QPL, and check with the AHJ before buying: the program itself says to “check with your local fire marshal ... prior to procurement.”

Electrified hardware: latch by day, deadbolt by night

ICS 705-1 approves automated access control “using at least two technologies” but **not** “for securing SCIF entrances when the SCIF is unoccupied.” UFC 3-4.6.5: electric strikes or electrified mortise locks “must have a positive engagement, fail secure, and approved under UL 1034 for burglar resistance.” FF-L-2890C Types II, IV, VII and VIII provide fail-secure electric release; once the combination-lock bolt is thrown it cannot be opened from outside without dialing again. Free egress stays mechanical from inside.

TRAP Treating the electric strike as the SCIF lock, or installing a maglock. Maglocks release on power loss, which conflicts with positive-engagement, fail-secure hardware. A request-to-exit device that can be triggered from outside, or that shunts the door contact, defeats both the ACS and the IDS.

Containers, vault doors and the forms

In a closed storage SCIF the **GSA-approved container** is the storage protection. Current classes: **Class 5** (10 min forced, 30 min covert, 20 hr surreptitious) and **Class 6** (no forced-entry rating; 30 min covert, 20 hr surreptitious); 5-W is weapons-only and 6-S is for DoD ships. **Black-label** (pre-1990) containers cannot be recertified: black-label Class 1-4 cabinets became obsolete 1 Oct 2024, and **Class 5 and 6 follow by 1 Oct 2028**. Vault doors (AA-D-600D) use **Class 5-V** for national security information; the 5-A armory door and its FF-L-2937 lock are not for classified material.

Combinations change when first placed in use, when someone who knows it no longer needs access, and on possible compromise (32 CFR 2001.43(c)). **SF 700** records container or door information; **SF 701** is the end-of-day activity checklist; **SF 702** logs every open, close and “checked by” event for the SCIF door, vaults and containers.

FIELD NOTE Most SCIF doors fail on installation, not product. Set frames plumb, level and square before the wall is finished; after closers and seals are adjusted, confirm the door latches and the deadbolt throws freely under seal compression, and re-check the HSS gap. The DoD Lock Program hotline, (800) 290-7607, answers revision, model and container questions before you buy.

SOURCES IC Tech Spec v1.5.1 · UFC 4-010-05 · FF-L-2740B · FF-L-2890C · QPL-FF-L-2890-5 · DoD Lock Program: containers · NISPPAC black-label briefing · 32 CFR 2001.43 · ISO 9001 forms

CHAPTER 08 THE BUILD

Penetrations, utilities & life safety

Every duct, pipe, conduit and cable that crosses the perimeter is a potential path for sound, forced entry, covert access and, sometimes, compromising emanations. Solve each one on paper before anyone drills it, and remember that a second authority, the AHJ, has an equal say at every exit.

The general rules

- “All penetrations of perimeter walls shall be kept to a minimum” (Tech Spec 3.G.1); the same for floors and ceilings (3.D).
- Utilities serving other areas “shall not transit the SCIF unless mitigated with AO approval” (3.G.3).
- “Electrical Utilities should enter the SCIF at a single point” (3.G.4); UFC 3-4.19 adds that cabling enters “from a single location,” labeled and color-coded by classification.
- Spare conduit is allowed if “filled with acoustic fill and capped” (3.G.6).
- Seal both sides with acoustical foam or sealant “finished to match adjacent wall”; firestop where assemblies are rated (UFC 3-4.11.3).

- Metallic penetrations “may require TEMPEST countermeasures, to include dielectric breaks or grounding, when recommended by the CTTA” (3.G.2).

FIELD NOTE Build a penetration schedule early: one line per duct, pipe, conduit, sleeve and cable bundle, with size, location, system and treatment. It becomes the pre-cover checklist and part of the accreditation package. Anything not on the schedule is an unapproved penetration until the SSM says otherwise.

Ducts: the 96 square inch trigger

Vents or ducts through the perimeter that “exceed 96 square inches shall be protected with permanently affixed bars or grills,” unless “one dimension of the penetration measures less than six inches”

(3.G.7). Every duct, regardless of size, still meets the SCIF’s acoustic requirement and is finished tight to the wall.

Opening at the wall	Area	Bars or grille?
12 × 10 in	120 sq in	Yes
24 × 5 in	120 sq in	No: one side < 6 in
12 × 8 in	96 sq in	No: equals, not exceeds

Man-bars are at least 1/2 in steel, welded vertically and horizontally 6 in on center; 3/4 in #9 expanded metal, 1-1/2 in #10 diamond mesh or 4×4 W2.9 welded wire fabric are alternatives, and permanently installed metal baffles set no more than 6 in apart may replace bars. An **access port** for inspecting them goes inside the perimeter, or outside with an AO-approved high-security lock.

VERIFY WITH YOUR AO

The Tech Spec lists bars, grilles or baffles for qualifying ducts; it does not list IDS as a substitute. Do not design in-duct motion sensors instead of bars without written AO approval.

Pipes, conduit and dielectric breaks

When the TEMPEST Countermeasures Review calls for it, UFC 4-010-05 §3-4.11.2 gives the DoD treatments: a nonconductive union on metal conduit inside the perimeter next to the penetration, or grounding within 6 in of the penetration with a No. 4 wire to the building grounding system; sprinkler and refrigerant lines grounded the same way; and a nonconductive flexible connection on a short section of duct inside the perimeter. At an RF shield the logic reverses: metal is bonded to the shield and openings become waveguides (Chapter 12).

TRAP

Installing dielectric fittings “just in case” in sprinkler or rated piping without a listed product and firestop detail. It creates a life-safety deficiency to solve a TEMPEST problem nobody asked you to solve. Break lengths come only from the CTTA’s review and the stamped drawings.

Life safety: two authorities, no override

Every perimeter door must “comply with applicable building code, safety, accessibility standards” as the AHJ determines (3.E.5). Egress from lower-security areas “must not pass through a higher security area” (UFC 3-3.3.2). Delayed egress “is recommended with NFPA 101 compliance,” and FF-L-2890C Types III, IV, VIII and X provide fire-rated panic hardware. Egress must never depend on the access control system or its power supply.

Fire alarm and mass-notification appliances inside the SCIF are life-safety devices whose circuits also cross the perimeter. The FFC asks whether PA, music or notification systems use “fiber isolation, self-amplified speakers, other method to ensure no audio back feed,” and the IDS “shall be separate from, and independent of, fire, smoke, radon, water, and other systems” (7.A.2.h).

TRAP

Extending the building voice-evacuation speaker circuit straight into the SCIF. A speaker works in both directions; with no isolation it fails the back-feed question and is expensive to rewire after ceilings close. Coordinate the AHJ, fire protection engineer, AO and CTTA in schematic design.

SOURCES IC Tech Spec v1.5.1 · UFC 4-010-05 · FFC v1.5 · FF-L-2890C · NFPA 101 · ADA Standards

CHAPTER 09 THE BUILD

Acoustics & sound masking

SCIFs where SCI is discussed “shall provide acoustic protection to prevent conversations from being inadvertently overheard outside of the SCIF” (ICS 705-1). The standard assumes an ordinary person with ordinary hearing on the other side of the wall. Deliberate technical interception is handled by TSCM, TEMPEST countermeasures and PED controls.

STC and NIC in plain English

Sound Transmission Class (STC) is a single number for how well a wall, door or window blocks airborne sound, measured in a **laboratory** (ASTM E90, rated per E413). **Noise Isolation Class (NIC)** is the similar number measured between two real rooms in the **finished building** (ASTM E336). The field number includes every **flanking path**: over the wall, under the door, through ducts and electrical boxes. The lab number describes the product; the field number describes what you built.

Sound Group 3 and Sound Group 4

Sound Group 3 (STC 45 or better; field NIC 40): “Loud speech from within the SCIF can be faintly heard but not understood outside the SCIF. Normal speech is unintelligible with the unaided human ear.” It is the default perimeter. **Sound Group 4** (STC 50 or better; field NIC 45): “Very loud sounds ... such as loud singing, brass music, or a radio at full volume, can be heard with the human ear faintly or not at all outside the SCIF.” Rooms with amplified audio such as VTC “must meet Sound Group 4” (UFC 3-4.3.2).

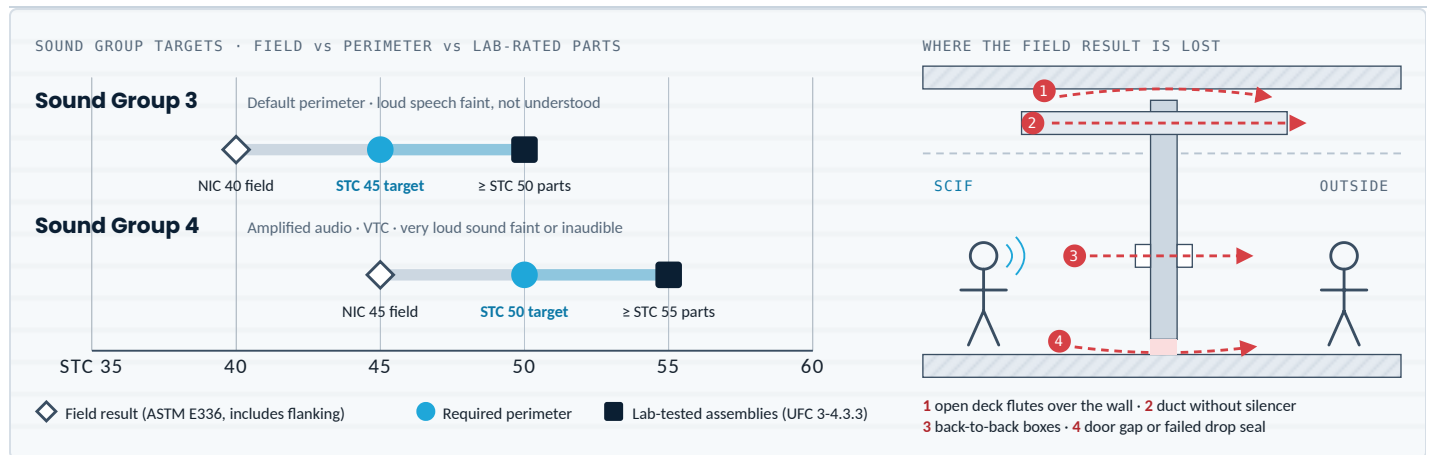


Figure 9.1 · Lab-rated door and wall assemblies are specified five points above the perimeter target because field performance is almost always lower. The margin absorbs normal imperfection; it cannot absorb an untreated flanking path.

ILLUSTRATIVE – NOT TO SCALE

Build it so the field number holds

- Walls true floor to true ceiling; track bedded in sealant; deck flutes filled (Tech Spec wall figures; UFC 3-4.4).
- Insulation “fastened to prevent sliding”; board joints staggered; gaps sealed both sides “with a non-hardening caulk” (UFC 3-4.4.5).
- For STC 50, four layers of 5/8 in GWB (two each side), or factory-laminated GWB meeting ASTM C1766 (UFC 3-4.4.2–3).
- No recessed or back-to-back boxes on perimeter walls (Tech Spec 3.G.5).
- Tested door assemblies with cam-lift hinges; silencers or Z-ducts on every duct and return (UFC 3-4.6.1, 3-4.13).

TRAP Building a small conference room to Sound Group 3, then adding a speakerphone or VTC after accreditation. Amplified audio requires Sound Group 4. Ask for the AV plan during design; some practitioners design every discussion room to Sound Group 4.

Testing at accreditation

“With all SCIF doors closed, all perimeter walls and openings ... shall be tested along multiple points” to confirm the Sound Group (Tech Spec Ch. 9, as quoted by practitioner sources). Audio (non-

instrumental) tests “must be approved by the AO”; instrumental tests are performed only by those trained in audio testing, with results of NIC 40 (Group 3) or NIC 45 (Group 4). The quoted setup places the speaker 6 ft from the wall and 4 ft above the floor, at “loud” or “very loud” speech.

VERIFY WITH YOUR AO Whether your AO wants audio checks, instrumented NIC testing or both, and who may test, varies. Ask before the schedule is set: instrumented testing needs a qualified tester and quiet conditions.

Mitigations and sound masking

When construction cannot reach the Sound Group at a specific weak point, the Tech Spec allows AO-approved **structural enhancement**, **stand-off distance** or **sound masking**. Masking rules (Ch. 9.E, as quoted): transducers “placed close to, or mounted on” the leakage paths; volume set by listening outside until conversations are unintelligible; generators “permanently installed,” with no AM/FM receiver, located within the SCIF; any recording capability disabled; wiring within the perimeter to the greatest extent possible. Masking systems are subject to TSCM evaluation.

SOURCES ICS 705-1 · UFC 4-010-05 · ASTM E90 · ASTM E413 · ASTM E336 · K.L. Security (quotes Ch. 9) · Speech masking: ICD 705 (quotes Ch. 9) · PSC (practitioner)

CHAPTER 10 THE BUILD

Intrusion detection & UL 2050 / Extent 3

The IDS guards a SCIF when nobody is inside. It must detect entry at every door and along every path to the material, report at once over a protected line to a qualified station, and bring a response force fast enough that nothing is compromised. ICS 705-1: installation, components and monitoring stations “shall comply with Underwriters Laboratories (UL) 2050 Extent 3 standards.”

TABLE 10.1 · THE 12 NUMBERS EVERY SCIF IDS INSTALLER SHOULD KNOW (TECH SPEC CH. 7 AS QUOTED FROM THE PUBLIC V1.4-ERA COPY; CONFIRM AGAINST V1.5.1; SOME VALUES ALLOW AO-APPROVED ALTERNATIVES)

#	Requirement	Value	Cite
1	UL installation level	UL 2050 Extent 3	7.A.2.b
2	Perimeter door switch	UL 634 listed High Security Switch, Level II (new accreditations)	7.A.2.d
3	Motion sensors	UL 639 listed; HSS and motion on every perimeter door	7.A.2.d; 7.A.3.a(7)
4	Entry delay at the primary door	≤ 30 seconds	7.A.3.a(6)
5	Backup power	24 hours uninterruptible	7.B.5
6	False alarms	≤ 1 per 30 days per IDS partition	7.A.2.p
7	Response force, closed storage	15 minutes	3.H(a)
8	Response force, open storage	15 minutes with Security-in-Depth; 5 minutes without	3.H(b); 32 CFR 2001.43
9	SCI-indoctrinated person on site	60 minutes (UL 2050) or the AO-approved time	7.C.1.c
10	Service start after a trouble signal	Within 4 hours	7.C.2
11	Recurring IDS test	Semiannual	7.D.3
12	Motion walk-test pass	Alarm on 3 of every 4 consecutive four-step trials	7.D.3

What Extent 3 actually means

“Extent of protection” is UL’s term for “the amount of alarm protection installed to protect a particular area, room or container” (UL CS-ASD-NISS instructions). Tech Spec 7.A.2.b: “Installation shall comply with an Extent 3 installation as referenced in UL 2050.”

Extent 5 is a reduced, patrol-based level that needs CSA approval under 32 CFR 117.15(d)(4); the Tech Spec offers no Extent 5 option, so it never applies to a SCIF or SAPF. Systems built and used by the U.S. Government need no UL certificate but must still meet Extent 3 installation requirements (7.A.2.c).

TRAP Web glossaries that publish an “Extent 1–5” ladder in which Extent 5 is “complete coverage.” Primary sources contradict that. The full extent definitions live in the licensed texts of UL 681 and UL 2050; check designs against licensed copies, not summaries.

Sensors, panel and modes

- **Sensors inside the SCIF**; failed sensors cause “immediate and continuous alarm activation”; dual-technology sensors only if each technology reports independently.
- **The PCU is inside the SCIF**, and “only SCIF personnel may initiate changes in access modes” (7.A.3.b(1)); it displays which sensor tripped, holds alarms until cleared locally (auto-reset disabled), and signals power changes locally and at the station.

- **Cabling that leaves the SCIF** uses encrypted line security or ferrous conduit with permanently sealed joints (no set screws), with junction boxes on GSA-approved locks (7.A.2.e).
- **Independent** of fire, smoke, radon and water systems (7.A.2.h); no audio or video capability without AO approval (7.A.2.l).
- **Modes**: only SCI-indoctrinated people arm or disarm; who armed and disarmed is recorded; tamper and emergency-exit circuits stay armed in disarmed mode; failures to arm or disarm are reported and kept two years.

UL 2050 certifies a company, not a product

The CRZH-listed alarm service company completes UL Form **CS-ASD-NISS** for each protected area, installs and tests, and issues the **National Industrial Security System certificate**. Contractor SCIFs “shall maintain a current UL certificate of installation and service,” renewed after any IDS change. The current edition is **UL 2050 Edition 6** (7 Apr 2025); much public UL guidance was written under Edition 5.

Check on the certificate	What to confirm
File number and CCN	Matches the UL Product iQ listing: CRZH (company); CRZM only if a NIMS monitors; not mercantile CVSG
Dates	Current; renewed after any IDS change
Each system	Extent 3, monitoring location, line security encrypted
Response time	Matches the AO/CSA approval, the FFC and the response agreement

TRAP “Extent 3” also appears on mercantile burglar-alarm certificates. A mercantile certificate is not a UL 2050 certificate, and a brochure that calls a panel “UL 2050 listed” is wrong. Specify listed products (UL 1076 or UL 1610 panels, UL 634 switches, UL 639 sensors) installed under a UL 2050 certificate.

Encryption and the FIPS 140–2 sunset

Transmission to the station uses FIPS-certified encryption: a UL 1610 PCU needs FIPS 197 (AES) or FIPS 140-2; a UL 1076 PCU needs FIPS 140-2 (7.A.3.b(10)). NIST’s CMVP moves FIPS 140-2 validations to the Historical List on **21 September 2026**; NIST says historical modules remain supported “for existing systems.”

VERIFY WITH YOUR AO For any new installation after September 2026, ask whether a module validated only to FIPS 140-2 is acceptable. Prefer FIPS 140-3 validated modules and keep the CMVP certificate number in the package.

Acceptance testing: what it should prove

1. Every motion sensor passes the walk test: four steps at one step per second, about 30 in each, alarm on at least 3 of 4 trials.
2. Every HSS alarms before the non-hinged side opens farther than the door’s thickness, emergency exits included.
3. Every equipment cover trips tamper in both modes.
4. Intrusion, failed-sensor, tamper, maintenance and shunt events annunciate at the PCU and the station.
5. Backup transfer without alarm; entry delay ≤ 30 s; defaults changed; encryption end to end.

FIELD NOTE Battery calculations often fail by leaving out the IP or cellular communicator, encryption module and network switch in the alarm path. Put all twelve numbers on the IDS submittal cover sheet with the paragraph beside each, and write into the monitoring contract that the station will deliver alarm, opening/closing and shunt histories on request.

SOURCES ICS 705-1 · IC Tech Spec v1.5.1 · UL CS-ASD-NISS instructions · UL NISS certification · UL 2050 Ed. 6 · 32 CFR 117.15 · DCSA SAP Checklist (Jan 2026) · NIST FIPS 140-3 transition · UFC 4-010-05

CHAPTER 11 THE BUILD

Access control & identity

Card readers control who walks in during the workday. They never lock up an empty SCIF. When the last person leaves, the FF-L-2740 combination lock and the armed IDS take over. Everything about an access control design follows from that division of labor.

Two technologies at the door

ICS 705-1 §G.2.b approves “automated access control systems using at least two technologies (badge, PIN, biometric, etc.),” electromechanical or mechanical devices, and personal recognition in small facilities or at a single monitored entrance, and states these methods are **not approved for securing SCIF entrances when the SCIF is unoccupied**. UFC 3-4.17.1: “At a minimum, provide card reader with keypad at the primary entrance and when provided, the secondary entrance,” with the CAC as the default DoD credential. If ACS and IDS are integrated, ACS notifications rank below IDS alarms (Tech Spec 7.A.2.i).

TRAP A card-and-keypad reader programmed for “card only” during business hours is a single-factor door, whatever the hardware can do. The configured mode counts. Lock the PIN requirement into the door schedule and the SOP.

Where the head-end lives, and how its lines are protected

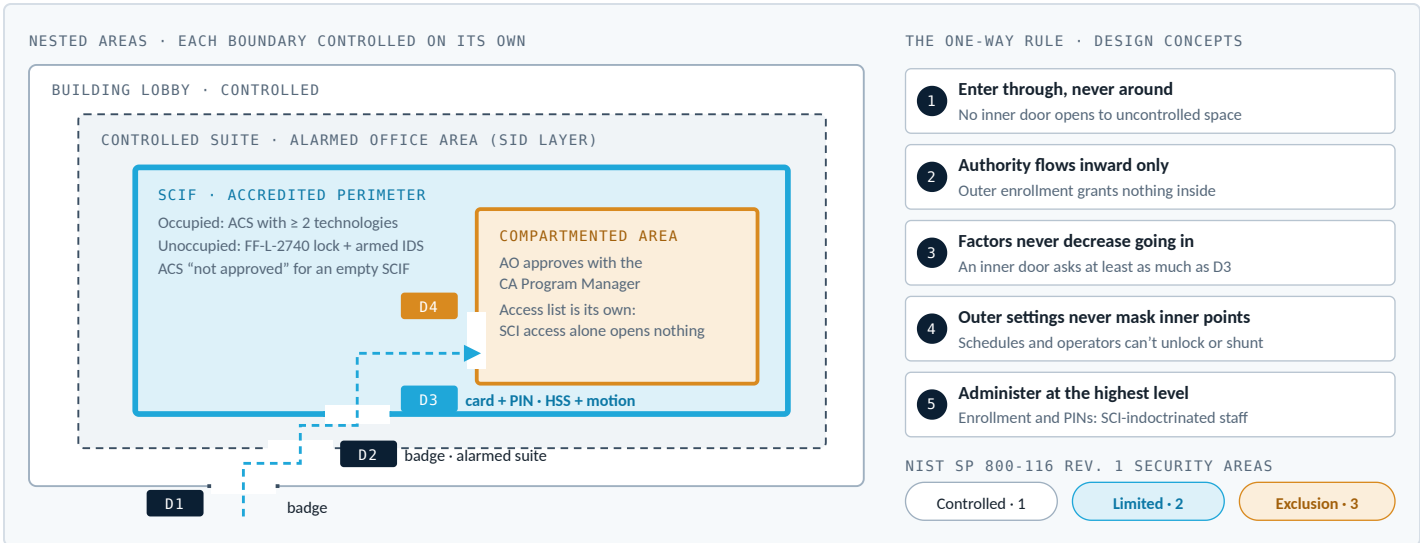
The Fixed Facility Checklist asks: “Is automated access control system located within a SCIF or an alarmed area controlled at the SECRET level?” It also asks whether transmission lines are “protected by 128-bit encryption/FIPS 140,” whether external devices have tamper protection, and whether “ID data and PINs [are] restricted to SCI-indoctrinated personnel.” A campus server or cloud head-end in unsecured space does not meet this without an AO-approved architecture, and routine remote support by uncleared vendor technicians is ruled out.

Secondary doors go dark when the SCIF closes

Tech Spec 3.E.3: the secondary-door ACS “must be deactivated when the SCIF is not occupied.” Tie deactivation to the closing procedure (for example the IDS arming sequence), not to a clock schedule that drifts and breaks on holidays, and demonstrate the disabled state at acceptance.

TABLE 11.1 · WHO CONTROLS EACH DOOR, BY SCIF STATE

State	Primary door	Secondary door	Egress-only door	IDS
Occupied	ACS with ≥ 2 technologies, or personal recognition at a monitored single entrance; visitor control here	ACS active, if the AO authorized the door	Alarmed 24/7; exit only	Disarmed; tamper and emergency-exit circuits stay armed
Closing	Last person clears the space, locks the FF-L-2740 (throwing the 2890 deadbolt), arms the IDS	ACS deactivated	Alarmed	Armed; record of who armed
Unoccupied	FF-L-2740 lock and IDS only	Secured by its 2890 deadbolt	Alarmed	Armed (secure mode)
Opening	Authorized person dials in and disarms from inside within the entry delay (≤ 30 s)	Reactivate per SOP	Alarmed	Disarmed; record of who disarmed



CHAPTER 12 THE BUILD

RED/BLACK, EMI filters & shield penetrations

RED is anything carrying classified information in the clear. BLACK is everything carrying only encrypted or unclassified information: building power, phones, the unclassified LAN, fire alarm, IDS, access control, CCTV. RED/BLACK discipline keeps RED signals from leaking onto anything BLACK that leaves the room, and the CTTA, not the build team, decides which countermeasures a facility needs.

Who decides

The **Certified TEMPEST Technical Authority** reviews plans “to determine if TEMPEST countermeasures are required and recommend solutions” (Tech Spec 3.A.3). UFC 4-010-05 calls the output the **TEMPEST Countermeasures Review** (TCR), requested through the TEMPEST addendum during planning. The public construction documents state *when* the CTTA’s direction applies (walls 3.C.3–3.C.4, doors 3.E.5, metallic penetrations 3.G.2, single-point entry 3.G.4) but never list filter ratings or separation distances.

The controlling TEMPEST issuances are named here for orientation only: CNSSP No. 300 (national policy), CNSSI No. 7000 (*TEMPEST Countermeasures for Facilities*, which defines inspectable space), CNSSAM TEMPEST/1-13 (*RED/BLACK Installation Guidance*) and CNSSI No. 7003 (Protected Distribution Systems). Their technical content is not public and is not reproduced.

VERIFY WITH YOUR AO RED/BLACK separation distances are applied by your CTTA to your facility. They are not published in this primer. Industry slides that repeat distance tables are summarizing a controlled document; do not copy them into drawings or submittals. Take distances only from the stamped drawings or the TCR.

Inspectable space and why many SCIFs aren’t shielded

Inspectable space is the three-dimensional zone around classified equipment that the government can see into and control; the CTTA determines it. RF protection is installed “at the direction of the CTTA when a SCIF utilizes electronic processing and does not provide adequate RF attenuation at the inspectable space boundary” (3.C.4). Outside the U.S. and not under Chief of Mission authority, “TEMPEST countermeasures shall be pre-engineered into the construction” (4.H.1). An unshielded SCIF still depends on basics: label RED and BLACK, never share trays, bundles or patch panels, use fiber where called for, and add no metallic penetrations.

TRAP Advertising a room as “TEMPEST compliant,” or buying filters and shielding before the TCR arrives. Recommendations can be partial: foil on certain walls, shielded racks or filtered power only.

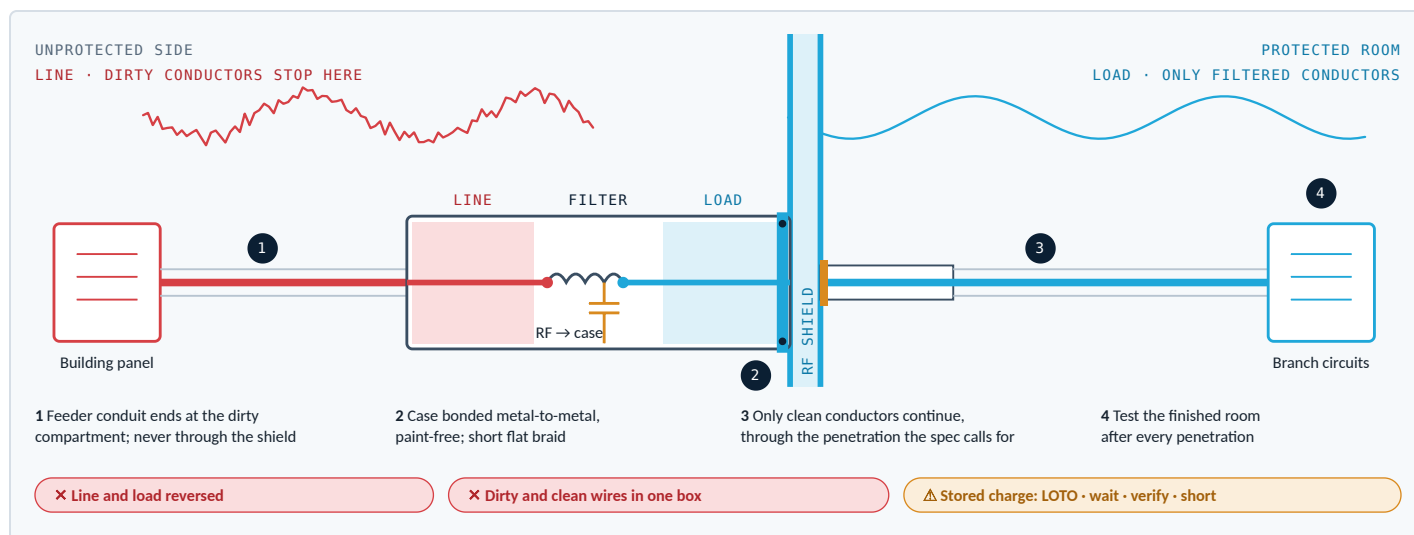


Figure 12.1 · Filter orientation at a shield. The rule is about **conductors, not boxes**: unfiltered (dirty) conductors terminate on the unprotected side and never cross; only filtered (clean) conductors continue. The case is bonded into the shield at the power entry point so it closes its own hole — the housing may project from either face (MIL-HDBK-1195 §2.8). Reverse it and unfiltered conductors run inside the room; share a box and RF couples around the filter. **ILLUSTRATIVE — NOT TO SCALE**

What a power filter does

A power-line filter is a passive **low-pass** network of inductors and capacitors: 60 Hz passes, RF is blocked and shunted to the metal case, and from there to the shield. It is rated by **insertion loss** in dB

across a frequency range, bench-tested per MIL-STD-220 with 50-ohm source and load; installed impedances differ, which is why the finished room is tested. Vendor datasheets commonly publish “100

dB class” figures; the level your project needs comes from the CTTA, shield designer and specification, not a catalog.

Mounting, safety and power quality

- **Bond the case** metal-to-metal on paint-free surfaces; a long round “ground wire” is not an RF bond. Keep input and output wiring physically apart.
- **Stored charge:** filter capacitors hold charge after the breaker opens. Lock out and tag out, wait the labeled discharge time, verify zero with a rated meter, apply a shorting stick, then open the compartment.
- **Leakage:** line-to-case capacitors leak small currents that add across filters and phases; that current can nuisance-trip a GFCI upstream of a filter. GFCI placement is an engineer-of-record and AHJ decision. Never lift grounds.
- **kVAR:** high-capacitance filters can overload a generator, destabilize voltage or prevent startup. Include filter kVAR in generator and UPS sizing and test transfer with filters energized.

Every other conductor and opening

Low-speed signal lines (phone, fire alarm loops, door contacts, readers) get **signal-line filters** at the penetration panel. High-speed data goes through the shield on **all-dielectric fiber in a waveguide**, with converters on filtered power; no PoE or copper Ethernet through the wall. At a shield, metal pipe, conduit and tray are welded or bonded and openings are sized as **waveguides-beyond-cutoff**; ducts get bonded **honeycomb vents**. At a non-shielded perimeter the logic reverses to a **dielectric break** or grounding, only where the CTTA directs. Never pass any conductor through a waveguide: a wire in a tube makes a coaxial line with no cutoff.

FIELD NOTE Count every conductor before the shield vendor builds the penetration panel; a missed two-wire door contact found after the shield test means a new penetration and a retest. The companion **Field Guide for GCs & Installers** covers line vs load, bonding, waveguide math, fiber entries and fastening without breaching the shield.

SOURCES IC Tech Spec v1.5.1 · ICS 705-1 · UFC 4-010-05 · NIST glossary: TEMPEST · Genisco: how filters work · Premier: installation practices · ETS-Lindgren filter manual · Premier: filters & generators · 2-95 (historical mirror)

CHAPTER 13 THE BUILD

PEDs, telecom & CCTV

Anything that can record, transmit or observe is a risk inside a SCIF: phones, watches, speakers, cameras, wireless locks and building controls. ICS 705-1 says PEDs “pose a risk to SCI,” and RF transmitters may not be introduced unless a competent authority such as the CTTA evaluates them as low risk and the AO approves.

Portable electronic devices

Tech Spec Chapter 10 covers PEDs with recording capabilities and embedded technologies: approved use, prohibitions, risk levels and mitigation. As summarized from a public edition, low-risk devices have no recording or transmitting capability, medium-risk devices have features that “can be physically disabled,” and high-risk devices need “more extensive or technically complex mitigation”; personally owned devices are prohibited from processing SCI, and medical devices go through separate review. A 30 June 2023 Secretary of Defense memo directed DoD components to program electronic device detection systems and mitigation in all DoD SCIFs and SAPFs by 30 September 2024.

PED lockers sit outside the primary entrance, are never recessed into the perimeter wall, and cannot be within 10 ft of equipment processing unencrypted national security information (UFC 3-4.7).

VERIFY WITH YOUR AO The Chapter 10 risk-level wording above was checked against an older public edition. Device categories, medical device approvals and any newer DoD or IC detection direction must come from your AO; DCSA’s January 2026 SAP checklist asks whether all approvals were obtained *before* a device was introduced.

Detection technology: what each can and cannot see

Category	Detects	Misses
Passive RF sensor network (WIDS)	Transmitting cellular, Wi-Fi, Bluetooth/BLE; locates emitters	Powered-off or silent devices; sensors are equipment inside the SCIF needing AO/CTTA review
Fixed RF detector at the vestibule	Cellular and often Wi-Fi/BT in a set radius	Can’t identify the device; nuisance alarms from outside RF
Handheld RF / direction finder	Sweeps and localizes	Operator-dependent; standby phones transmit rarely
Ferromagnetic or metal screening	Ferrous or metallic objects, powered or not	Not phone-specific; throughput and false alarms

Telecommunications

Tech Spec Chapter 11 covers unclassified telephones and information systems, CCTV at entry points, wireless, environmental infrastructure, emergency notification, system access, cable control and Protected Distribution Systems. Practical rules for the build team:

- **Phones:** NCSC’s Telephone Security Group publishes an approved endpoints list for SCIF use; the FFC asks whether speakerphones and microphones are disabled or AO-approved, and whether remote room monitoring is disabled.
- **Telecom rooms** with encryption equipment go “within or adjacent (shared wall) to the secure area” to minimize PDS (UFC 3-3.3.2).
- **PDS** (CNSSI 7003) protects unencrypted classified lines crossing lesser areas; “Avoid the use of PDS whenever possible” (UFC 3-4.20). Most IDS and ACS cabling is not PDS.
- **Cabling** enters at a single location, labeled and color-coded by classification (UFC 3-4.19).
- **Wireless** anything (locks, readers, sensors, cellular communicators, building-automation radios) needs CTTA evaluation and AO approval. Design wired first.

CCTV at the entrance, never inside

UFC 3-4.17.2: “Cameras are not allowed within the perimeter or enable observation within the perimeter.” An exterior camera at the primary entrance is permitted for remote control of the door from inside, and a video intercom may provide this. Tech Spec Chapters 8.E and 11.D treat CCTV as a supplement to entry control, never a substitute for the lock, the ACS or the IDS.

Do	Don't
Frame faces and the door approach	Capture keypad PINs, the combination dial, badge data or a view through the open door
Keep monitors and release controls inside, run by SCI-indoctrinated staff	Put IP cameras, doorbells or intercoms with microphones inside the perimeter
Use cameras without audio near SCIF walls	Run camera cable through the SCIF to reach the other side of the building
Map corridor coverage on FFC Section B for SID credit	Present CCTV as a reason to relax the lock, ACS or IDS

SOURCES ICS 705-1 · IC Tech Spec v1.5.1 · SECDEF memo, 30 Jun 2023 · UFC 4-010-05 · DCSA SAP Checklist (Jan 2026) · NCSC TSG approved endpoints · NIST glossary: PDS · Apple: Airplane Mode · I Dig Hardware: interlocks

CHAPTER 14 THE BUILD

Construction security & build sequence

A SCIF tenant improvement follows the normal design-bid-build path with security gates in front of every big commitment: designing, signing the contract, closing the walls and moving in. The controls exist so the AO can trust work it will never see.

TABLE 14.1 · PHASE 0–5 BUILD SEQUENCE WITH SECURITY GATES (PLANNING AID; THE AO-APPROVED CSP AND DESIGN GOVERN)

Phase	Key outputs	GC and integrator focus	Security gate
0 • Sponsorship & due diligence	Sponsor and AO identified; SSM appointed; site feasibility	Walk above ceilings and below floors; map slab cores, deck flutes, shared utilities, monitoring path	“Security begins when the initial requirement for a SCIF is known” (Tech Spec 2.A)
1 • Planning & pre-design	Concept approval; preliminary CSP; FFC; TEMPEST addendum	Price CSP site controls; confirm response time and monitoring	AO and CTTA engaged before design is final
2 • Design	Wall types, door and penetration schedules, IDS/ACS design, AHJ life-safety review	Security notes on the trade sheets; no TBDs on hardware, penetrations or IDS layout	AO approves design concept, CSP and final design (3.A)
3 • Procurement & award	Award; citizenship flow-down; long-lead orders	FF-L-2890/2740 from the QPL; tested STC assemblies; UL 2050 company	No award without an approved CSP (3.B.1)
4 • Construction	Site controls; inspections; photo record; change log	Pre-cover hold point; every field change through the SSM	Violations or deviations to the AO within 3 business days (3.A)
5 • Test & accredit	Acoustic, IDS, UL 2050 certificate, TEMPEST/RF and TSCM as required; as-builts; final FFC	Deliver test reports, certificates and turnover binder	AO inspection and accreditation; no SCI before the letter

The Construction Security Plan

“Prior to awarding a construction contract, a CSP for each project shall be developed by the SSM and approved by the AO” (Tech Spec 3.B.1). It documents project identity and adjacencies, Security-in-Depth, control of plans and documents, protection of IDS technical documentation, workforce vetting and badging, escorts and CSTs, site

access controls, material procurement and storage, the inspection schedule with hold points, violation reporting, and renovation barriers that segregate workers from operational areas.

Who may design, build and install

- **Design:** U.S. companies using U.S. citizens or U.S. persons (UFC 1-17).
- **Construction:** “should be performed by U.S. companies using U.S. citizens ... but may be performed by U.S. companies using U.S. persons,” with AO-ensured mitigations (3.B.5).
- **IDS installation and testing:** “U.S. companies using U.S. citizens” (7.D.1; UFC 1-18.1). U.S. person status does not satisfy this.

Citizenship, U.S. person status and clearance are separate tests. Flow the requirements to every subcontractor.

Site controls and materials

Tech Spec 3.B.6 lists identity verification, random searches at entry and exit, prohibited-item signage, physical barriers and vehicle inspections; “the AO may impose procedures for the procurement, shipping, selection, and secure storage of construction materials” (UFC 4-3). Overseas, controls scale with threat Category: CST start points, cleared finish workers, secure transport and secure storage areas.

FIELD NOTE Schedule a **pre-cover hold point**: before board closes, the SSM (and the AO or TSCM team if they ask) inspects in-wall and above-ceiling work, and every wall segment, penetration and top-of-wall seal is photographed and logged against the drawings (UFC 4-7). Put CSP costs (escorts, badging, searches, document control) in the bid documents; bidders who don't see them won't price them.

TRAP Handling SCIF drawings like ordinary construction documents. SCIF location and identity are protected at minimum as CUI (UFC 4-2), TEMPEST vulnerabilities tied to a location are at least CONFIDENTIAL (UFC 1-16.3), and completed FFCs may be CUI or classified. No public plan rooms, open bid portals or “anyone with the link” shares.

TRAP Starting demolition under an early contract before the CSP is approved, or letting “minor” field changes go untracked. Any deviation from the approved design, however small, is documented and approved through the SSM.

SOURCES IC Tech Spec v1.5.1 · UFC 4-010-05 · CSP form v1.5 · ICS 705-2 · PSC: crafting a CSP (practitioner) · SAME 2026 (practitioner) · CenCore Q&A (practitioner)

CHAPTER 15

REFERENCE

Top traps

The mistakes that recur across SCIF projects are rarely exotic. They are basic details done out of sequence, left unfinished or never documented. Items in the first group are schedule problems no amount of field effort fixes; most of the rest are cheapest to catch at the pre-cover inspection.

Trap	Why it fails	Do this instead
AUTHORITY, PAPERWORK & SEQUENCE		
Engaging the AO after design, material orders or contracts	Tech Spec 2.A requires coordination first; late findings force redesign	Identify the AO at kickoff; submit concept, preliminary CSP and TEMPEST addendum in planning
Awarding the contract or starting demo before the CSP is approved	Violates Tech Spec 3.B.1; workers enter before site controls exist	Treat CSP approval as the award gate
Calling a product “ICD 705 certified,” “TEMPEST compliant” or “UL 2050 listed”	The AO accredits facilities; the CTTA recommends countermeasures; UL 2050 certifies the alarm company	Use verifiable listings and “subject to AO/CSA approval” wording
Exceeding a standard “to be safe”	Needs a waiver and costs mandatory reciprocity (Tech Spec 2.A; ICS 705-1)	Discuss enhancements with the AO before they reach the drawings
Assuming Security-in-Depth, or letting it lapse	Without accepted SID, open storage needs Wall B/C and a 5-minute response	Get the SID determination in writing; put SID systems under change control
Sending drawings, checklists or TEMPEST findings through open channels	Location + “SCIF” is CUI; TEMPEST findings at a location are at least CONFIDENTIAL	Secure file transfer set up before design; handle per the CSP
PERIMETER, DOORS & PENETRATIONS		
Walls stop at the drop ceiling or leave deck flutes open	Not true floor to true ceiling; acoustic and visual-evidence failure	Detail flute infill before bid; photograph every top-of-wall segment
Recessed or back-to-back boxes and cabinets on perimeter walls	Tech Spec 3.G.5; UFC 3-4.4.7–8; direct flanking path	Surface raceway or furred wall; note it on the trade sheets
Ducts over 96 sq in without bars, baffles or access ports	Tech Spec 3.G.7; IDS is not listed as a substitute	Mechanical engineer lists every perimeter duct opening and treatment
Other tenants’ utilities routed through the SCIF; scattered entries	Tech Spec 3.G.3–3.G.4	One planned utility entry; reroute mains in design

Trap	Why it fails	Do this instead
Non-QPL locks, fail-safe strikes or maglocks; exterior hardware on egress-only doors	Tech Spec 3.E; UFC 3-4.6.5; FF-L-2890C	Door schedule lists FF-L-2890 type, UL 1034 strike and HSS per door
“STC door” assembled from mixed parts; racked frames	Only tested assemblies carry the rating; binding bolts and seal gaps	Specify the tested assembly; set frames plumb, level, square
ACOUSTICS, IDS & ACCESS CONTROL		
VTC or speakerphone added to a Sound Group 3 room	Amplified audio requires Sound Group 4 (UFC 3-4.3.2)	Get the AV plan in design; zone rooms before walls are detailed
Perimeter door with HSS but no motion (or motion but a standard contact)	Tech Spec 7.A.3.a(7) requires both; Level II for new accreditations	Door and sensor schedule reviewed against the 12 numbers (Table 10.1)
PCU or keypad outside the SCIF; set-screw conduit; unlocked junction boxes	Tech Spec 7.A.3.b(1), 7.A.2.e	PCU and arming stations inside; encrypted lines or sealed ferrous conduit
Batteries short of 24 h; communicator left off the calculation	Tech Spec 7.B.5; the alarm never reaches the station	Measured-current calculation including every device in the alarm path
Mercantile certificate, expired certificate, or not renewed after changes	ICS 705-1 requires a current UL 2050 certificate	Verify CRZH listing and certificate fields; track the expiration date
ACS head-end in the cloud or an unsecured server room; unencrypted reader runs	FFC SC.1: SCIF or SECRET-controlled alarmed area; FIPS-protected lines	AO-approved architecture before bid
TEMPEST, SHIELDING & OPERATIONS		
Filters reversed, shared boxes, painted bonds; copper through a waveguide	RF bypasses the filter; a wire in a tube has no cutoff	Dirty outside, clean inside; all-dielectric fiber only; see the Field Guide
A penetration added after the shield test	The test describes a room that no longer exists	Freeze the penetration schedule; review and retest every change
Moving SCI, furniture or people in before the letter	SCI before accreditation is a violation (DoDM 5105.21 Vol. 2)	Treat the letter as Gate C

CHAPTER 16 REFERENCE

Glossary of 60 key terms

Plain definitions of the terms that appear most often in SCIF and SAPF submittals, with the chapter where each is explained. Where one abbreviation means two things, both are given.

A – C

Accrediting Official (AO)

The single named official, delegated by the IC element head, who approves the design and CSP and accredits the SCIF. Ch. 3

Authority Having Jurisdiction (AHJ)

Building and fire officials who enforce building, fire and accessibility codes. Security approvals don't override them. Ch. 8

BLACK

Equipment, wires and signals carrying only encrypted or unclassified information. Ch. 12

Closed storage

SCIF mode in which all SCI, including classified equipment, is stored in GSA-approved containers. Not the same as a legacy NISPOM “closed area.” Ch. 5

Co-Use Agreement (CUA)

Agreement, signed by both parties' AOs, that lets a tenant use a host SCIF under the host's accreditation. Ch. 4

Compartmented Area (CA)

Area within a SCIF that separates compartments or programs; Types I–III, of which only Type III stores. Ch. 5, 11

Compromising emanations (CE)

Unintentional radiated or conducted signals that could reveal information being processed. Ch. 12

Construction Security Plan (CSP)

The SSM's project security plan, approved by the AO before any construction contract is awarded. Ch. 14

CRZH / CRZM

UL listing categories for National Industrial Security System alarm companies and monitoring stations. Ch. 10

CSA

In ICD 705 documents, the Cognizant Security Authority (an official). In NISPOM, the Cognizant Security Agency (DoD, DOE, NRC, ODNI, DHS). Ch. 1, 3

Construction Surveillance Technician (CST)

Supplements site access control and monitors construction when the AO requires it; required overseas per threat Category, except that under Chief of Mission authority CSTs are not required when contractors are U.S. citizens with TOP SECRET clearances. Ch. 3, 14

CTTA

Certified TEMPEST Technical Authority: reviews plans and recommends TEMPEST countermeasures; the AO approves. Ch. 12

D – F

De-accreditation

Formal notice via the IC SCIF Repository that a facility is no longer accredited; a space held at SECRET for less than a year may be re-accredited. Ch. 4

Dielectric break

Short, listed non-metallic section in a pipe, conduit or duct that interrupts a conductive path, used when the CTTA directs. Ch. 8, 12

EMI/RFI filter

Passive low-pass network that passes power or wanted signals and shunts RF to its bonded case. Ch. 12

Extent 3

UL 2050 installation designation required for SCIF and SAPF intrusion detection. Not a TEMPEST, RF or acoustic rating. Ch. 10

Extent 5

Reduced, patrol-based alarm protection allowed only with CSA approval under NISPOM; never for SCIFs. Ch. 10

FF-L-2740B

Federal specification for electromechanical combination locks (e.g., Kaba Mas X-10, S&G 2740B) on containers, vault doors and SCIF doors. Ch. 7

FF-L-2890C

Federal specification for pedestrian door lock extensions, Types I–X, used with an FF-L-2740 lock on SCIF doors. Ch. 7

Fixed Facility Checklist (FFC)

Tech Spec form, Sections A–I, documenting physical, technical and procedural security for accreditation. May be CUI or classified when completed. Ch. 1, 4

FIPS 140-2 / 140-3

NIST cryptographic module validation standards. 140-2 validations move to the NIST Historical List on 21 Sep 2026. Ch. 10

FIPS 201-3 / PIV

Federal Personal Identity Verification credential standard; the CAC is DoD's version. Ch. 11

Flanking path

Any route sound takes around a wall: over it, under a door, through ducts or boxes. Ch. 9

Fortuitous conductor

Metal never meant to carry signals (conduit, pipe, duct, armor) that carries them anyway. Ch. 12

G – N**GSA-approved security container**

Class 5 or Class 6 container for classified storage; black-label units cannot be recertified and Class 5/6 black labels phase out by 1 Oct 2028. Ch. 7

High Security Switch (HSS)

UL 634 door contact; Level II (balanced magnetic switch) is required on SCIF perimeter doors for new accreditations. Ch. 10

IC SCIF Repository

NCSC-managed inventory of accreditations, waivers, re-evaluations and de-accreditations. Ch. 4

ICD 705

The Intelligence Community Directive (26 May 2010) requiring SCI to be handled only in accredited SCIFs. Ch. 2

ICS 705-1 / ICS 705-2

Standards for physical and technical security (17 Sep 2010) and for accreditation and reciprocal use (22 Dec 2016). Ch. 2

Intrusion Detection System (IDS)

The alarm system protecting a SCIF when unoccupied: sensors, PCU, communication path and monitoring station. Ch. 10

Inspectable space

Three-dimensional zone around classified equipment that the government can see into and control, as determined by the CTTA. Ch. 12

Line side / load side

A filter's dirty, unfiltered input, whose conductors stop on the unprotected side, and its clean, filtered output, whose conductors are the only ones that continue in. A rule about conductors, not about which way the housing projects. Ch. 12

Noise Isolation Class (NIC)

Field-measured sound isolation between rooms (ASTM E336); NIC 40 for Sound Group 3, NIC 45 for Group 4. Ch. 9

O – S**Open storage**

SCIF mode in which SCI may be stored and processed outside containers; the room is the safe. Ch. 5

Premise Control Unit (PCU)

The IDS control panel. Located inside the SCIF; only SCIF personnel change its modes. Ch. 10

Protected Distribution System (PDS)

Protected cable path for unencrypted classified information crossing lesser areas (CNSSI 7003); avoided where possible. Ch. 13

Portable electronic device (PED)

Phones, watches, tablets and other devices able to record or transmit; restricted per Tech Spec Chapter 10. Ch. 13

Pre-Construction Checklist

Tech Spec form (added in v1.5) giving the AO project information and the SID starting point. Ch. 4

Reciprocity

Acceptance of a SCIF accredited by one IC element, with no waivers, by all IC elements. Ch. 2, 4

RED

Equipment, wires and signals carrying unencrypted classified information. Ch. 12

SAPF

Special Access Program Facility, governed by DoDM 5205.07 (17 Jan 2025) and built to equivalent Tech Spec criteria. Ch. 1

SAPF Accrediting Official

Appointed in writing by the CA SAPCO to approve SAPF preconstruction plans and accredit SAPFs. Ch. 3

SCI

Sensitive Compartmented Information: classified national intelligence requiring handling within formal access control systems. Ch. 1

SCIF

Sensitive Compartmented Information Facility: a room, suite or building accredited by an AO for SCI. Ch. 1

Security-in-Depth (SID)

Layered controls around a SCIF that the AO accepts; can allow Wall A and a 15-minute response for open storage. Mandatory overseas. Ch. 5

Sound Group 3 / 4

Acoustic performance levels: STC 45 (default perimeter) and STC 50 (amplified audio). Ch. 9

SSM

Site Security Manager: security point of contact for planning, design and construction; writes the CSP. Ch. 3

SSO / SSR / CSO

Operational security officers: Special Security Officer, Special Security Representative, and Contractor Special (SCI) or SAP (SAP) Security Officer. Ch. 3

Sound Transmission Class (STC)

Laboratory rating of airborne sound blocking (ASTM E90/E413). Ch. 9

Secure Working Area (SWA)

Accredited space for discussing, handling or processing SCI with no storage. Ch. 5

T – W**TEMPEST Countermeasures Review (TCR)**

The CTTA's documented recommendations for a facility, requested through the TEMPEST addendum. Ch. 4, 12

Tech Spec

IC Tech Spec for ICD/ICS 705; current public version 1.5.1 (26 Jul 2021). Ch. 2

TEMPEST

A covername, not an acronym: the investigation, study and control of compromising emanations (NIST, citing CNSSI 4009). Ch. 12

TSCM

Technical surveillance countermeasures; for accreditation, conducted by U.S. Government teams through the AO. Ch. 3

Temporary Secure Working Area (TSWA)

SCI use under 40 hours per month; accreditation 12 months or less; no storage. Ch. 5

UL 2050

National Industrial Security Systems, Edition 6 (7 Apr 2025): certifies alarm service companies and their installations. Ch. 10

Vault

Storage room built to Tech Spec 3.C.5 (or FED-STD 832 for collateral) with a GSA Class 5 vault door. Ch. 6

Waiver

Documented, time-bound exception granted by an official who is not the AO; removes mandatory reciprocity. Ch. 4

Wall A / B / C

Tech Spec perimeter wall types: standard, enhanced with expanded metal, enhanced with plywood. Ch. 6

Waveguide-beyond-cutoff

A metal tube sized so RF below its cutoff frequency dies out while air, water or fiber pass. Never put a conductor through one. Ch. 12

CHAPTER 17 REFERENCE

Reference library

Official public sources behind this primer, checked September 2026. Many www.dni.gov links now redirect to archive.dni.gov; where available, the stable DoD Lock Program (NAVFAC EXWC) mirror is listed. Confirm the current version with the issuer before you cite it in a specification.

Document	Issuer	Version / date	Link
INTELLIGENCE COMMUNITY (ODNI / NCSC)			
ICD 705, SCI Facilities	ODNI	26 May 2010	archive.dni.gov/.../ICD/ICD-705-SCIFs.pdf
ICS 705-1, Physical & Technical Security	ODNI / NCSC	17 Sep 2010	exwc.navfac.navy.mil/.../DoD_Locks/PDFs/ICS-705-1.pdf
ICS 705-2, Accreditation & Reciprocal Use	ODNI / NCSC	22 Dec 2016	exwc.navfac.navy.mil/.../DoD_Locks/PDFs/ICS-705-2.pdf
IC Tech Spec for ICD/ICS 705	NCSC	v1.5.1, 26 Jul 2021	exwc.navfac.navy.mil/.../ICD-ICS-705_Tech_Spec.pdf
SCIF Fixed Facility Checklist v1.5 (form)	NCSC	v1.5 forms	archive.dni.gov/.../SCIF-Fixed-Facility-Checklist-V15.pdf
TSG approved telephone endpoints list	NCSC TSG	May 2026	archive.dni.gov/.../May_2026_TSG_AEL_Endpoints.pdf
DEPARTMENT OF DEFENSE			
DoDM 5105.21 Vol. 2, SCI Admin Security Manual	USD(I&S)	2012; Change 2, 2020	esd.whs.mil/.../dodm/510521m_vol2.pdf
DoDM 5205.07, SAP Security Manual	USD(I&S)	17 Jan 2025	esd.whs.mil/.../dodm/520507m1.PDF
UFC 4-010-05, SCIF/SAPF Design & Construction	DoD (WBDG)	26 May 2023	wbdbg.org/FFC/D0D/UFC/ufc_4_010_05_2023.pdf
DoD Lock Program · (800) 290-7607	NAVFAC EXWC	Current	exwc.navfac.navy.mil/DoD-Lock-Program/
FF-L-2740B combination locks	GSA	15 Jun 2011	exwc.navfac.navy.mil/.../DoD_Locks/PDFs/FF-L-2740.pdf
FF-L-2890C lock extensions; QPL	GSA	2019; QPL 2022	exwc.navfac.navy.mil/.../DoD_Locks/PDFs/FF-L-2890C.pdf
NISPOM, DCSA AND CDSE			
32 CFR 117.15, NISPOM safeguarding	DoD / eCFR	Current eCFR	ecfr.gov/current/title-32/.../section-117.15
32 CFR 2001.43, Storage (supplemental controls)	ISOO / eCFR	Current eCFR	ecfr.gov/current/title-32/.../section-2001.43
DoW SAP Security Compliance Checklist	DCSA	Jan 2026, v2	dcsa.mil/.../SAP_Security_Compliance_Checklist_(2026)
CDSE SA501, ICD 705 construction for SAP	CDSE	eLearning	cdse.edu/Training/eLearning/SA501/
UL, IDENTITY AND CRYPTOGRAPHY			
UL 2050 NISS certification (CRZH / CRZM)	UL Solutions	Ed. 6, 7 Apr 2025	ul.com/services/national-industrial-security-...
FIPS 201 Approved Products List	GSA	Current	idmanagement.gov/buy/
NIST SP 800-116 Rev. 1 (PIV for PACS)	NIST	29 Jun 2018	nist.gov/.../sp-800-116-revision-1-guidelines-use-piv
FIPS 140-3 transition (CMVP)	NIST	140-2 sunset 21 Sep 2026	csrc.nist.gov/projects/fips-140-3-transition-effort
STATE DEPARTMENT, LIFE SAFETY AND ACCESSIBILITY			
12 FAM 710 (Chief of Mission SCIFs)	State Dept.	Current FAM	fam.state.gov/fam/12fam/12fam0710.html
NFPA 101 Life Safety Code	NFPA	Edition per AHJ	nfpa.org/.../nfpa-101-standard-development/101
HISTORICAL (CONTEXT ONLY, NEVER CURRENT REQUIREMENTS)			
NSA, “TEMPEST: A Signal Problem”	NSA	Declassified article	nsa.gov/portals/75/.../cryptologic-spectrum/tempest.pdf
IC Tech Spec v1.5	NCSC	2020; superseded	archive.dni.gov/.../IC-Tech-Specs-...-SCIFs-v15.pdf



Build it right the first time.

Secure-space projects succeed when the owner, designer, general contractor, low-voltage integrator and security manager share one accurate vocabulary before the first submittal. This primer is our contribution to that conversation. It is educational and public-level; your Accrediting Official, Cognizant Security Authority and CTTA set the requirements for your facility.

MAIL

PO Box 4327, La Puente, CA 91747

PHONE

1-626-789-2267

WEB

lacctvsupply.com

ESTABLISHED

Since 2009

Do not send classified information, CUI, completed checklists, TEMPEST findings or facility addresses by unencrypted email. Ask your AO for the approved channel.

Not affiliated with or endorsed by ODNI, NCSC, DoD, DCSA, NSA, DIA or UL Solutions. Product and program names belong to their owners and are cited for identification only. © 2026 LA CCTV Supply. September 2026 edition.