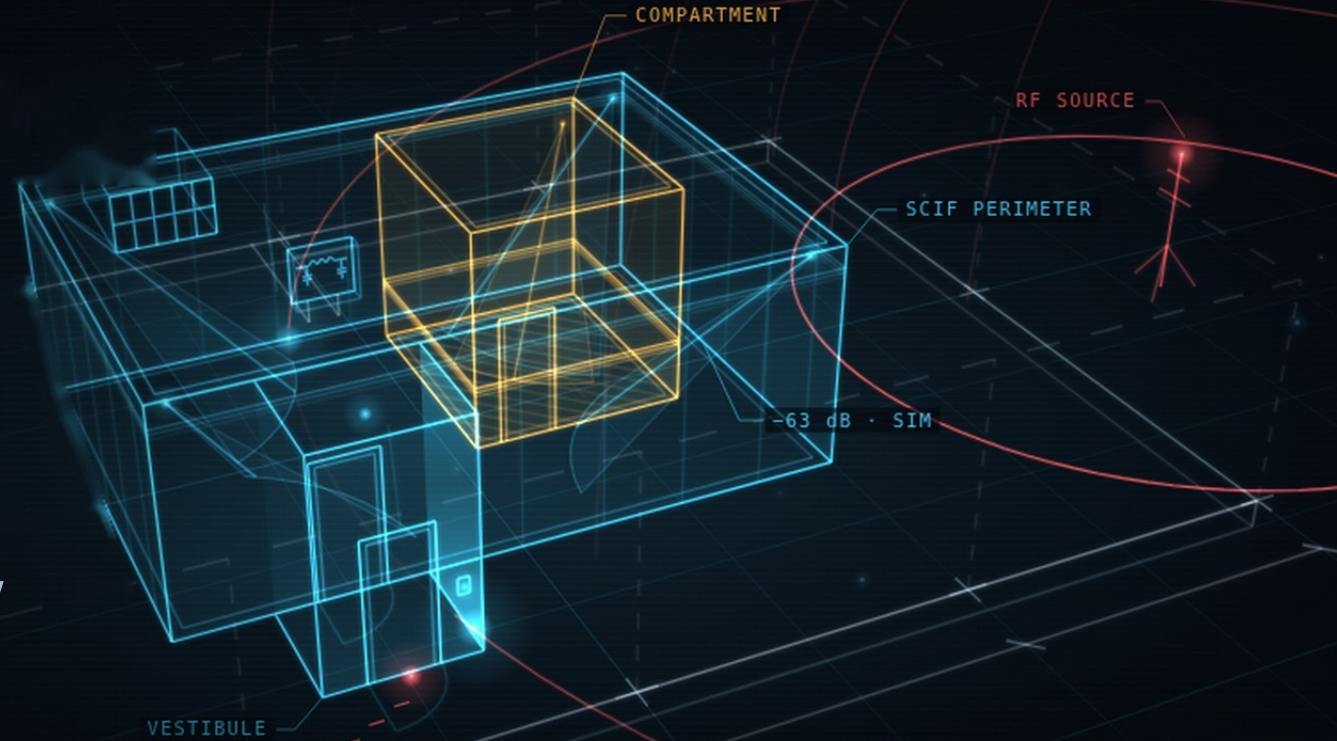


LA CCTV SUPPLY · PUBLIC BRIEFING

Understanding SCIF & SAPF Security

ICD 705, the IC Tech Spec and UL 2050 Extent 3: how secure spaces are approved, built and protected.



Why this matters

THE ONE IDEA

The approval, not the construction, makes it a SCIF.

A room built “to ICD 705” but never accredited is just an expensive room. SCI can’t be discussed or brought in until the Accrediting Official (AO) accredits the space.

Most failures trace back to steps skipped at the start.

WHO NEEDS ONE



Intelligence Community elements and DoD

Anyone handling Sensitive Compartmented Information (SCI) needs an accredited SCIF.



Cleared contractors

A government sponsor is required; DoD SCIFs need a SCIF number or written concept approval.



Special Access Programs

SAP work happens in a SAPF, accredited by a SAPF Accrediting Official.

WHO HAS TO GET IT RIGHT

Owners & sponsors

Architects & engineers

General contractors

Low-voltage integrators

Security managers

SCIF vs SAPF vs open storage area vs GSA container

	SCIF	SAPF	NISPOM open storage area	GSA-approved container
Protects	Sensitive Compartmented Information (SCI)	Special Access Program information	Collateral classified (contractors)	Collateral; SCI only inside a closed storage SCIF
Rules	ICD 705 · ICS 705-1/-2 · IC Tech Spec	DoDM 5205.07 · Tech Spec criteria	32 CFR 117 (NISPOM) · 32 CFR 2001	32 CFR 2001.43 · DoD Lock Program
Approved by	IC element AO (DIA for most DoD)	SAPF Accrediting Official	DCSA	Container must be GSA-approved
Intrusion detection	UL 2050 Extent 3	UL 2050 Extent 3	Extent 3 baseline; Extent 5 only with CSA approval	No IDS sensors on the container itself
Top Secret alarm response	Closed: 15 min · Open: 15 min with SID, 5 without	Same as SCIF	Open storage: 15 min with SID, 5 without	2-hour checks, or IDS + 15 min, or SID + FF-L-2740 lock

 **Trap:** a DCSA-approved open storage area is not a SCIF. Moving SAP into a SCIF, or SCI into a SAPF, needs a Co-Use Agreement first.

The document stack and current versions

DIRECTIVE	● ICD 705	26 May 2010
STANDARD	● ICS 705-1 · physical & technical	17 Sep 2010
STANDARD	● ICS 705-2 · accreditation & reciprocity	22 Dec 2016
BUILD-TO SPEC	● IC Tech Spec for ICD/ICS 705	v1.5.1 · 26 Jul 2021
DOD SCI MANUAL	● DoDM 5105.21 Vol. 2	Change 2 · 2 Nov 2020
DOD SAP MANUAL	● DoDM 5205.07 (Vol. 3 cancelled)	17 Jan 2025
DESIGN CRITERIA	● UFC 4-010-05	26 May 2023
ALARM STANDARD	● UL 2050	Edition 6 · 7 Apr 2025
COLLATERAL RULES	● 32 CFR 117 (NISPOM) · 32 CFR 2001	Current eCFR

● IC ● DoD ● UL ● CFR

Read down
for authority: what must be true

Read up
for method: how to build it

VERSION TRAP

“The 2020 Tech Spec” is out of date: v1.5.1 replaced v1.5 and moved the forms to Chapter 14.

When layers disagree, the stricter rule and your AO’s written direction win.

Who approves what



DECIDERS Approve

Accrediting Official (AO)

Approves design, CSP and final design; accredits the SCIF

SAPF Accrediting Official

Approves SAPF plans and accreditation

Cognizant Security Authority

Oversight and co-use concurrence

CTTA

Recommends countermeasures; AO approves

Authority Having Jurisdiction

Building code, fire and accessibility



SECURITY STAFF Plan and run

Site Security Manager (SSM)

Owens security through construction; writes the Construction Security Plan (CSP)

SSO / SSR / CSSO

Run the accredited space every day: SOPs, logs, change reports

CSTs and escorts

Construction surveillance and site access control

TSCM team

Technical surveillance countermeasures, as required



BUILDERS Produce evidence

Architect-engineer

Drawings and project data for the SSM

General contractor

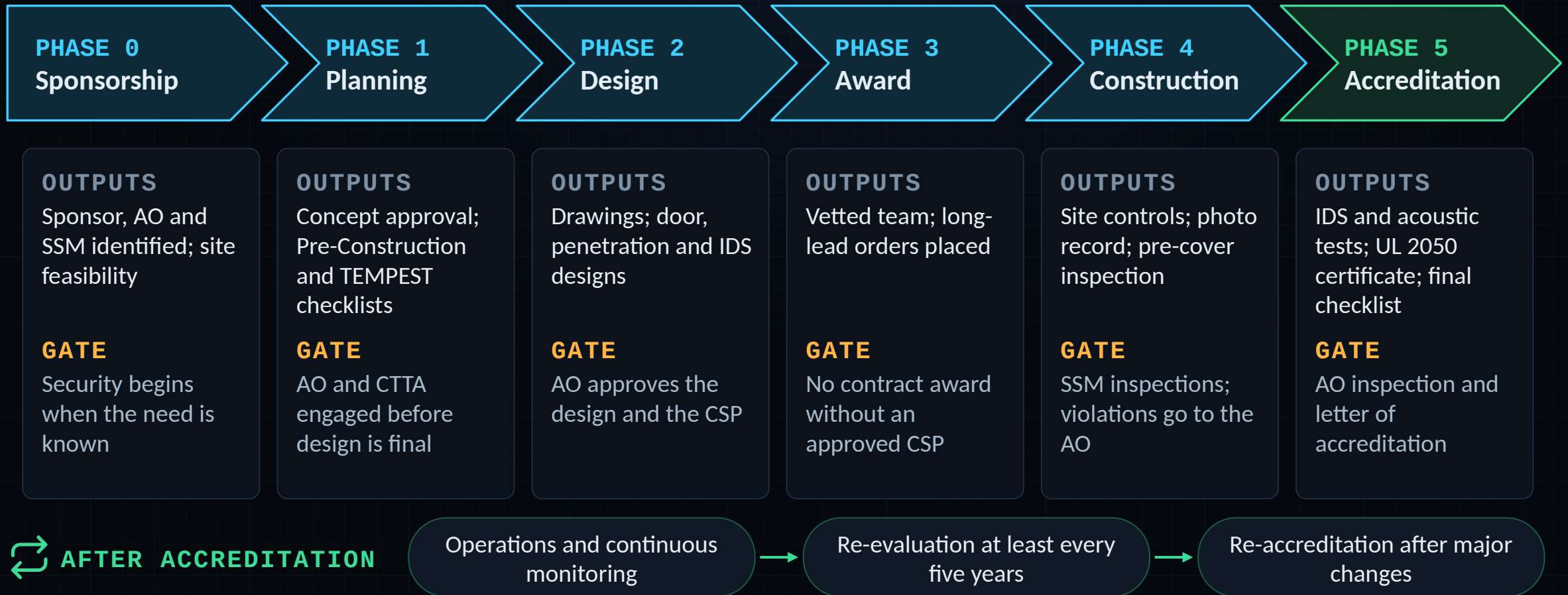
Builds to approved drawings and CSP; keeps the photo record

IDS / low-voltage integrator

UL 2050 certificate, spec sheets and acceptance test results

Builders never approve their own work. Authority flows down from the IC element head; evidence flows up to the AO.

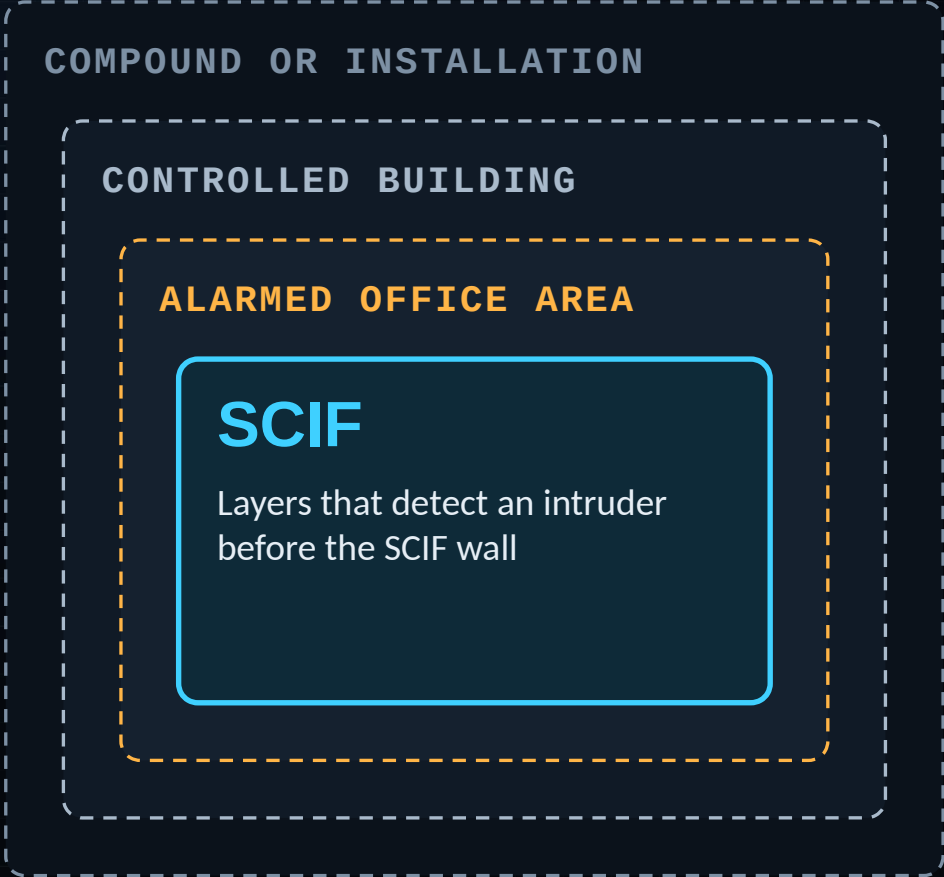
Six phases, each with a security gate



Facility modes and Security-in-Depth

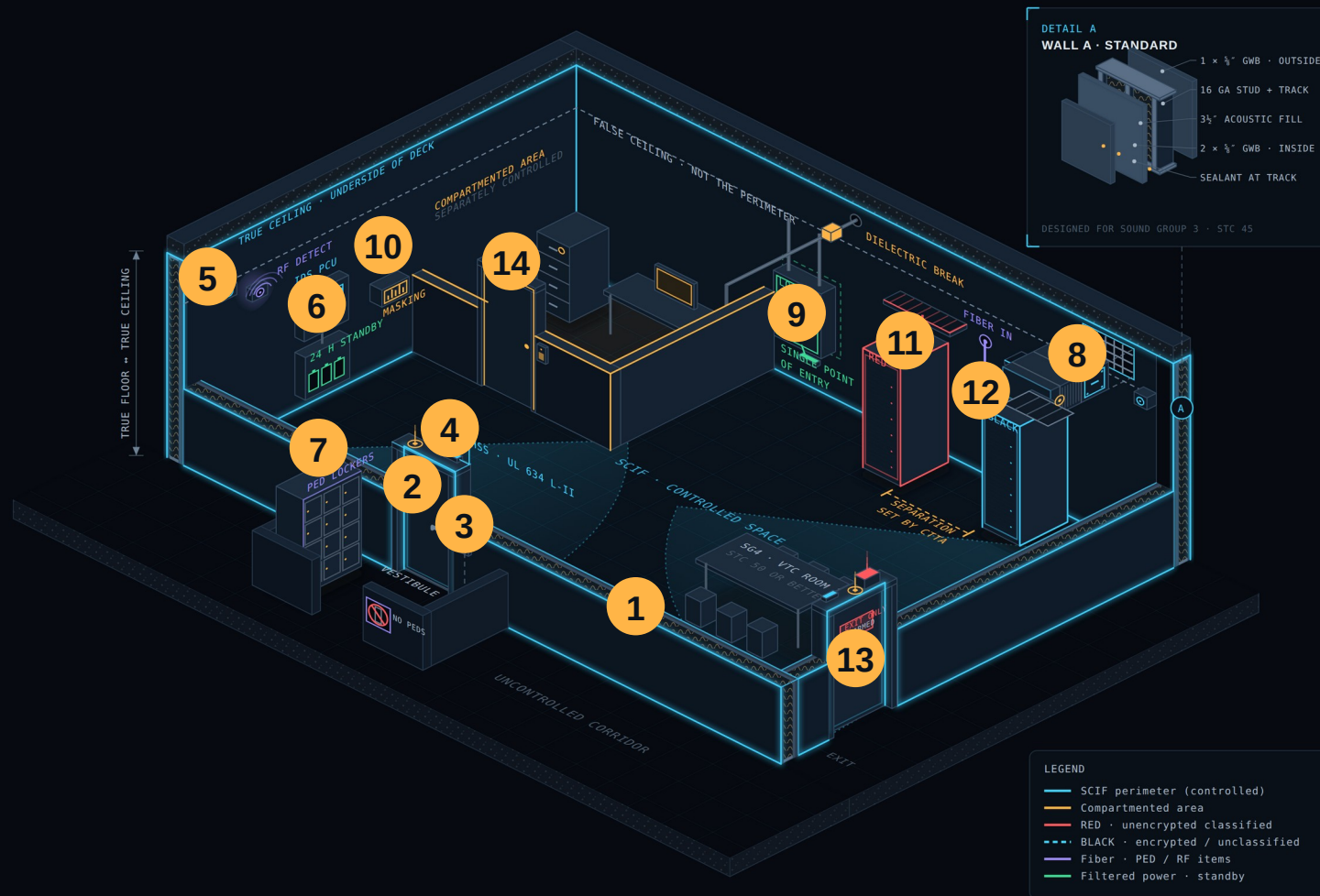
MODE	SCI STORED	WALL	RESPONSE
Closed storage	In GSA containers	Wall A	15 min
Open storage + SID	In the open	Wall A	15 min
Open storage, no SID	In the open	Wall B or C	5 min
Continuous operation	Staffed 24/7	Wall A	Per AO
Secure Working Area	Not stored	Wall A	15 min

Response = initial alarm response force for facilities inside the U.S. (Tech Spec 3.H).
With AO-accepted SID, open storage can use Wall A and a 15-minute response.



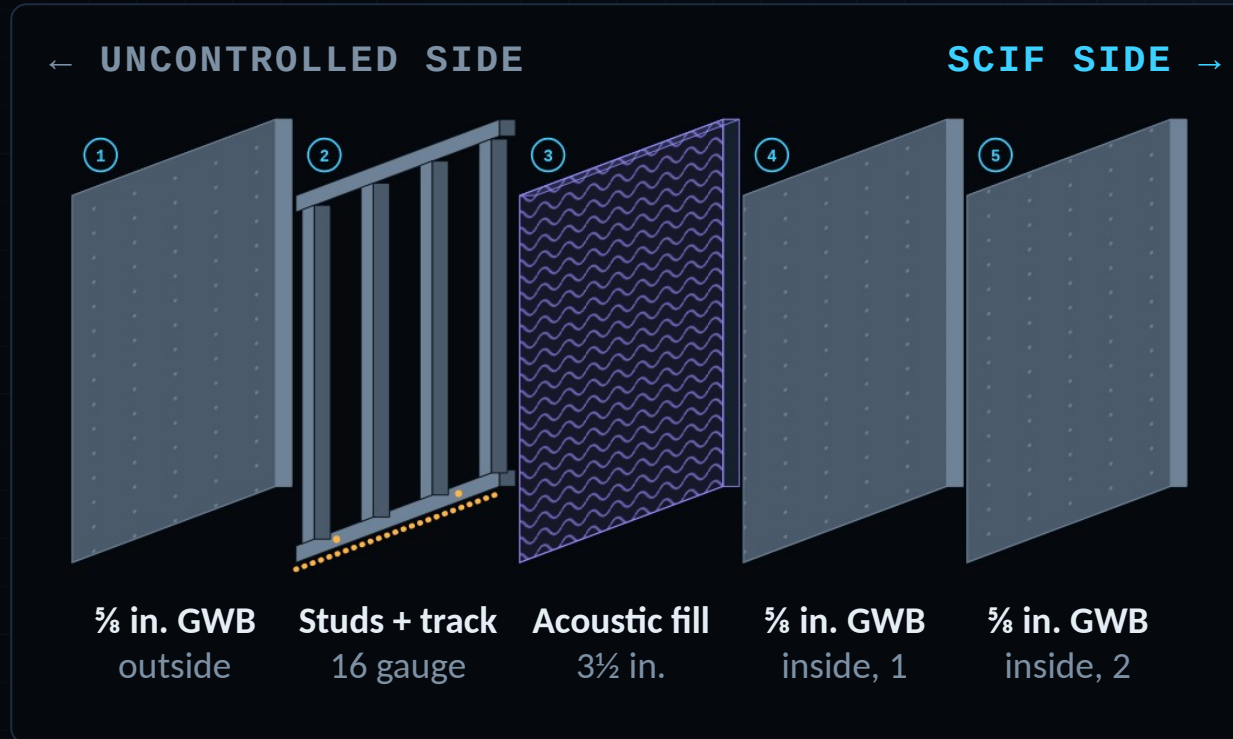
The AO decides. SID is recorded in FFC Section B, and it is mandatory outside the U.S.

Anatomy of a SCIF



- 1 Perimeter, slab to slab
- 2 Primary door + FF-L-2740 lock
- 3 Card reader + PIN
- 4 Door switch, UL 634 Level II
- 5 Motion sensors
- 6 IDS control unit + 24 h power
- 7 Vestibule + PED lockers
- 8 Duct over 96 sq in: bars
- 9 Penetration panel + filter
- 10 Sound masking
- 11 RED vs BLACK equipment
- 12 Fiber entry, no copper
- 13 Egress-only door, alarmed
- 14 Compartmented area

Perimeter walls: A, B and C



EVERY WALL TYPE SHARES

- ✓ True floor to true ceiling, painted
- ✓ 16-ga track in acoustical sealant
- ✓ 3 1/2 in. acoustic fill
- ✓ Staggered board seams

Wall A · Standard

SOUND GROUP 3

Three layers of 5/8 in. gypsum board: one outside, two on the SCIF side.

Use: closed storage, SWA, continuous ops, open storage with SID

Wall B · Enhanced

FORCED-ENTRY LAYER

Wall A plus #9 expanded metal on the SCIF side of the studs.

Use: open storage without SID (5-minute response)

Wall C · Enhanced

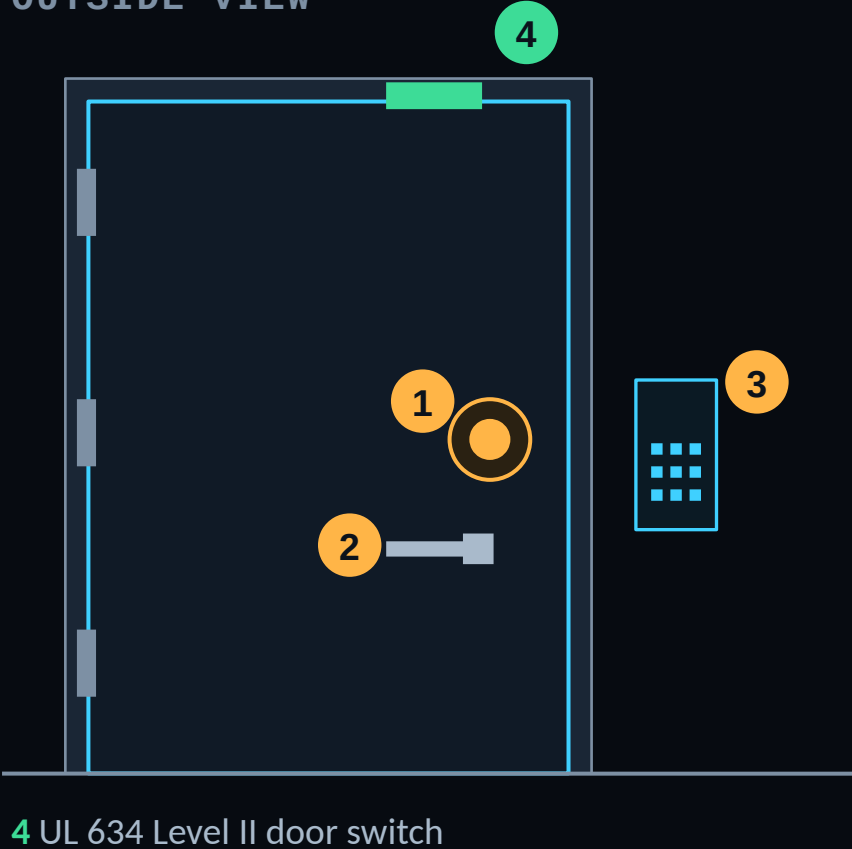
FORCED-ENTRY LAYER

1/2 in. plywood on the SCIF side under one board layer; two layers outside.

Use: open storage without SID (5-minute response)

Doors and locks: three layers, two jobs

OUTSIDE VIEW



1 FF-L-2740B combination lock

Secures the empty SCIF. 20 man-hours surreptitious entry resistance; at least 1,000,000 combinations. Current models: Kaba Mas X-10, S&G 2740B.

2 FF-L-2890C lock extension

Ten device types: primary doors use Types I-IV, secondary VII-VIII, exit-only IX-X. Buy only from the current QPL, and check with the AHJ first.

3 Access control, duty hours only

At least two technologies, such as card + PIN, with a UL 1034 fail-secure strike. Never used to secure an unoccupied SCIF.

PRIMARY

One per SCIF; visitor control happens here

SECONDARY

Needs AO approval; ACS off when unoccupied

EMERGENCY EXIT

No outside hardware; alarmed 24/7

Penetrations: size, bars and a single point of entry

96 sq in

Vent or duct openings larger than this need permanently affixed bars or grilles...

< 6 in.

...unless one dimension is under six inches.

WORKED EXAMPLES

✗ $12 \times 10 \text{ in.} = 120 \text{ sq in}$

Bars required

✓ $24 \times 5 \text{ in.} = 120 \text{ sq in}$

No bars: 5 in. side

✓ $8 \times 8 \text{ in.} = 64 \text{ sq in}$

No bars: under 96

✓ $12 \times 8 \text{ in.} = 96 \text{ sq in}$

No bars: not over 96

DUCT OPENING AT THE PERIMETER



Man-bars: ½ in. steel, welded both ways at 6 in. on center

Or: expanded metal, welded wire fabric, or metal baffles 6 in. apart



Every crossing is a problem to solve on paper first

- Utilities enter at a single point; nothing for other areas transits the SCIF
- Spare conduit filled with acoustic fill and capped
- Bars don't stop sound: every duct still needs acoustic treatment

Acoustics: Sound Group 3 vs Sound Group 4

SOUND GROUP 3

STC 45



FIELD TEST

NIC 40

LAB-RATED PARTS

STC 50

“Loud speech ... can be faintly heard but not understood outside the SCIF.”

Default SCIF perimeter • Wall A

SOUND GROUP 4

STC 50



FIELD TEST

NIC 45

LAB-RATED PARTS

STC 55

“Very loud sounds ... such as ... a radio at full volume, can be heard ... faintly or not at all outside the SCIF.”

VTC, conference and amplified-audio rooms

SOUND MASKING, WHEN THE AO APPROVES IT

- ✓ Generator fixed inside the SCIF
- ✓ No AM/FM receiver; recording disabled
- ✓ Volume set by listening outside

IDS essentials: the numbers every installer should know

Extent 3

UL 2050 installation level

7.A.2.b

Level II

UL 634 switch and motion at each perimeter door

7.A.2.d

≤ 30 s

Entry delay at the primary door

7.A.3.a(6)

24 h

Uninterruptible backup power

7.B.5

15 min

Response force; 5 min for open storage without SID

3.H

60 min

SCI-indoctrinated person on site, or AO-approved time

7.C.1.c

≤ 1

False alarm per 30 days per IDS partition

7.A.2.p

4 h

Service must start after a trouble signal

7.C.2

Also: semiannual testing · IDS separate from fire and other systems · IDS alarms outrank access control events · control unit inside the SCIF

UL 2050 and “Extent 3” explained

“Extent” = how much of a space an alarm covers.

Tech Spec 7.A.2.b: “Installation shall comply with an Extent 3 installation as referenced in UL 2050.”

✓ Extent 3

- Required for every SCIF and SAPF
- The highest level for National Industrial Security Systems
- ICD 705 adds Level II door switches plus motion, 24 h power and encrypted signals

✗ Extent 5

- A reduced level based on patrols and Security-in-Depth
- Needs CSA approval under 32 CFR 117.15
- No Extent 5 option in the Tech Spec: never for a SCIF or SAPF

CERTIFIES THE COMPANY

UL 2050 certifies the alarm company, not a product.

Edition 6

7 Apr 2025

CRZH

Alarm service company listing

CRZM

Monitoring station listing

Certificate

Kept current; renewed after any IDS change

Trap: web glossaries that rank “Extent 1–5” with 5 as complete coverage are wrong. Extent is not a TEMPEST, RF or acoustic rating.

Access control and identity



RULES THAT FAIL INSPECTIONS

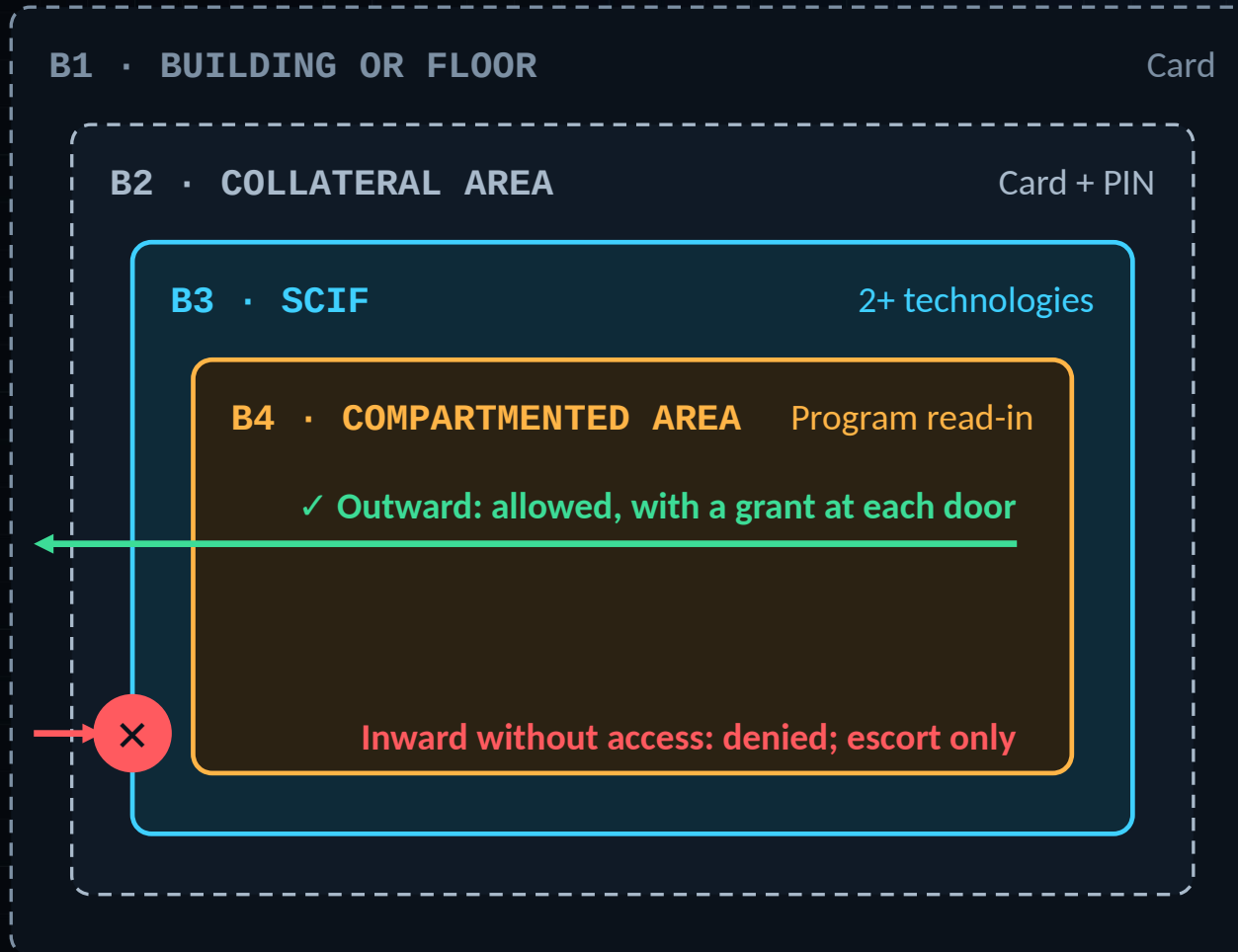
- Two technologies at the door. “Card only” mode is single-factor, whatever the reader can do.
- Access control never secures an empty SCIF.
- ID data and PINs restricted to SCI-indoctrinated staff.
- FIPS 140-2 moves to NIST’s historical list on 21 Sep 2026: ask for FIPS 140-3.

PLATFORM EXAMPLE · HIRSCH

- Mx controllers: UL 294 and UL 1076 listed
- FIPS 140-3 certified cryptography with TLS 1.3 (per Hirsch)
- TS ScramblePad readers scramble digits on every use
- Two-person rule, occupancy counting, door interlocks
- Velocity integrates with DMP XR-series intrusion panels

Manufacturer claims, not AO approvals.

Nested access: higher → lower, never lower → higher



Higher → lower: allowed

People cleared for an inner area may use outer doors, with an explicit grant at each one.



Lower → higher: never

An outer-area grant opens nothing inside. Visitors are escorted.

DESIGN RULES

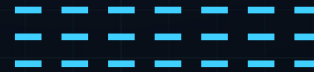
- Put high inside low: never enter a lower area through a higher one
- Authentication factors never decrease going inward
- Clearance isn't access: eligibility, NDA, need-to-know
- Compartmented area doors: no spin-dial locks, no separate alarm

RED/BLACK basics

RED

Classified information in the clear

- Classified computer and monitor
- The cable between them
- Unencrypted classified circuits



SEPARATION SET BY YOUR CTTA

Keep RED physically and electrically apart from anything BLACK that leaves the room.

BLACK

Encrypted or unclassified only

- Building power and phones
- Unclassified LAN, fire alarm, building controls
- IDS, access control, CCTV



Label everything

Cabling, patch panels, outlets and connectors marked by classification



Separate pathways

Never share a bundle, tray or patch panel. Don't improvise reroutes.



Keep crypto close

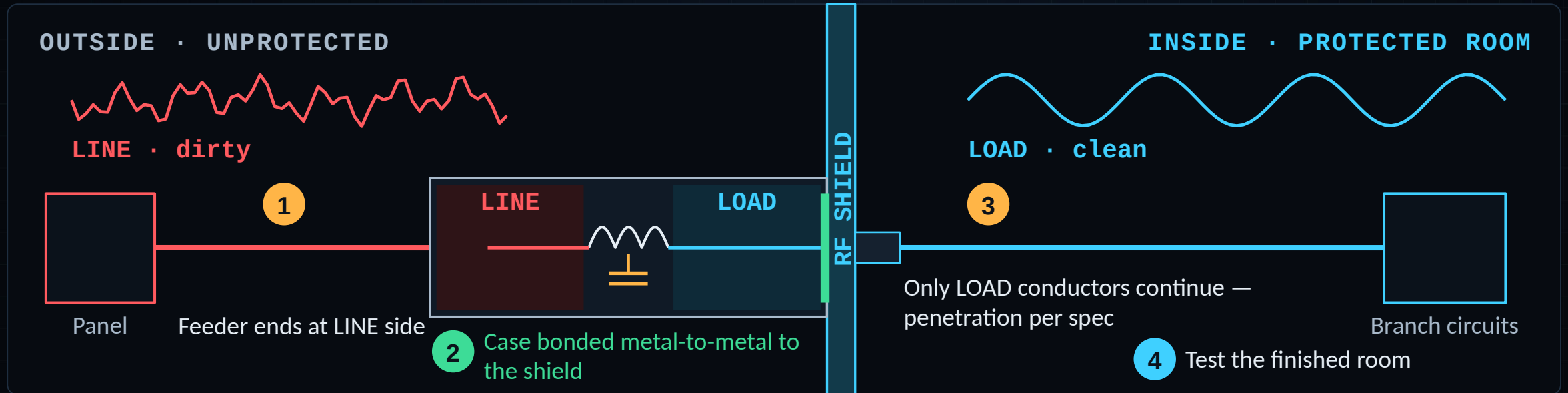
Encryption gear in telecom rooms within or next to the secure area



Review first

The CTTA decides countermeasures; grounding is engineered, not improvised

EMI filters: the case is the boundary



Backwards fails

Unfiltered conductors end up inside the room, where RF radiates and signals can couple onto them.



A shared box fails

Dirty and clean wires in one box or raceway let RF jump around the filter entirely.



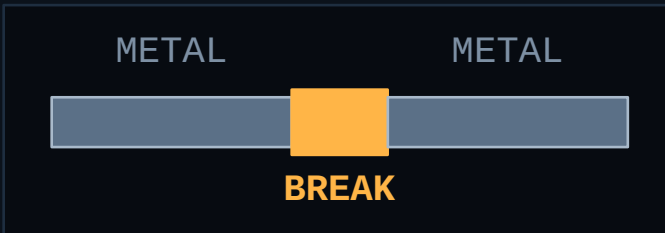
Filters store charge

Lock out and tag out, wait, verify with a meter, then use a shorting stick.

Shield penetrations: breaks, waveguides and fiber

Non-shielded perimeter: break the metal path, only if the CTTA directs

RF-shielded room: bond metal to the shield; size openings as waveguides



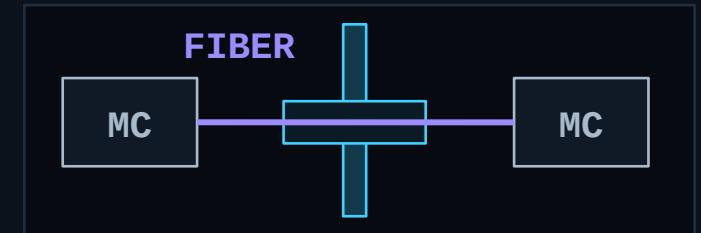
Dielectric break

- A short, listed non-metal section: union, flange kit or duct connector
- Stops metal acting as a long wire out of the room
- Length and location come from the CTTA and drawings
- Listed and firestopped for the system it serves



Waveguide-beyond-cutoff

- A narrow metal tube passes air, water or fiber; RF below cutoff dies out
- Opening size sets the cutoff; length sets the attenuation
- Never a conductor through it: that makes a coax with no cutoff
- Honeycomb vents apply the same idea to HVAC air



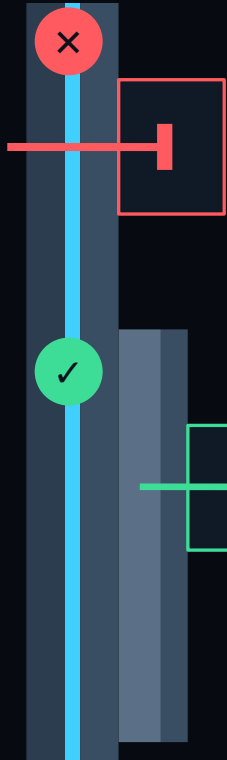
Fiber entry

- Convert to light; run all-dielectric fiber through a waveguide
- No armor, steel strength member or tracer wire
- Converters inside on filtered power; never PoE or copper
- Size tubes for spares: adding one later means a retest

Never fasten through the shield

WALL SECTION

OUT SCIF



Wrong: a screw, anchor or hanger through the shield leaves a hole RF leaks through

Right: a furred wall on stand-offs, or surface raceway; fasteners stop short of the shield

Leaks can't be seen, only measured. Any new penetration means review, then retest.



Do

- Surface-mount, use raceway, or build a furred wall
- Mount door switches on maker brackets on the protected side
- Route low-voltage cable to the single entry point
- Report an accidental hole: vendor repair, then retest



Don't

- Drive screws, anchors, powder pins or hanger rods through foil or steel
- Recess boxes or panels in a perimeter wall
- Caulk over a shield hole
- Pass copper, PoE or steel-member fiber through a waveguide

PEDs, detection and telecom



Portable devices

- PEDs pose a risk to SCI; the AO approves any exception
- No RF transmitters inside unless evaluated, mitigated and AO-approved
- Lockers outside the primary entrance, at least 10 ft from unencrypted classified processing
- Medical devices get an individual review



Device detection

- DoD directed SCIFs and SAPFs to program for detection systems (SECDEF memo, June 2023)
- RF detectors only see devices that are transmitting
- Powered-off phones are invisible; airplane mode can leave Wi-Fi and Bluetooth on
- Detection feeds access control and must never block egress



Telecom and CCTV

- Unclassified phones: TSG-6 (CNSSI 5006) approved phone or disconnect device
- Speakerphones and microphones disabled unless AO-approved
- PA and notification: no audio back feed
- Cameras stay outside and never view inside; keypads out of frame



Integrator note: detectors, sensors and speakers are equipment too. Anything inside the SCIF or crossing the perimeter needs AO review, and CTTA review where TEMPEST applies.

Top traps that fail inspections

⚠️ TRAP 01

AO engaged after design or contracts

→ Coordinate first; no award without an approved CSP

⚠️ TRAP 02

Walls stop at the drop ceiling

→ Build true floor to true ceiling, sealed

⚠️ TRAP 03

Wall A for open storage, assuming SID

→ Settle the SID decision before drawing walls

⚠️ TRAP 04

“Card only” mode on a card + PIN reader

→ Configure and document two factors

⚠️ TRAP 05

Access control server in unsecured space

→ Head-end in the SCIF or an alarmed SECRET area

⚠️ TRAP 06

VTC added to a Sound Group 3 room

→ Zone Sound Group 4 rooms during design

⚠️ TRAP 07

Filter reversed, or wires sharing a box

→ Dirty side outside, clean side inside, kept apart

⚠️ TRAP 08

A new penetration after the shield test

→ Freeze the schedule; review and retest

How to start a SCIF project

1

Confirm the mission need and sponsor

DoD SCIFs need a SCIF number or written concept approval.



2

Identify the AO and appoint an SSM

Talk to the AO before design, orders or contracts.



3

Profile the facility

Storage mode, Security-in-Depth, U.S. or overseas.



4

Zone every room

Sound Group 3, Sound Group 4 or non-discussion.



5

Get the CTTA's review early

Submit the TEMPEST checklist; buy no filters or shielding before the review.



6

Build a penetration schedule

Every duct, pipe, conduit and cable, entering at a single point.



7

Bring in your IDS and ACS integrator

Verify UL 2050 listings (CRZH and CRZM) in UL Product iQ.



8

Approve the CSP before award

Then build under surveillance and photograph everything before cover.



Resources and contact

PUBLIC REFERENCES

ICD 705 · ICS 705-1 · ICS 705-2

ODNI / NCSC

IC Tech Spec v1.5.1 and forms

ODNI / NCSC

UFC 4-010-05 (2023)

DoD design criteria

DoDM 5205.07 (2025)

DoD SAP security manual

FF-L-2740B · FF-L-2890C · QPL

DoD Lock Program

UL 2050 certificates

UL Product iQ



SCIF ANSWERS KNOWLEDGE BASE

lacctvsupply.com/scif-answers.php

Call 1-626-789-2267 · lacctvsupply.com

Low-voltage scope for secure spaces: intrusion detection, access control, entrance video and cabling.

 Public-level educational information only. It does not replace the direction of your Accrediting Official, Cognizant Security Authority or CTTA, engineered drawings, the NEC or your AHJ. No product is “ICD 705 certified”: the AO accredits the facility. Final system design, IDS/access control integration and door hardware are subject to AO/CSA approval, and CTTA approval where TEMPEST applies.