SCIF / SAPF Project Readiness Questionnaire

& Pre-Design Checklist

A fillable intake template for owners, program security staff, designers, general contractors and low-voltage integrators. Use it before design starts to find out what is decided, what is unknown, and what your Accrediting Official (AO), Cognizant Security Authority (CSA) and Certified TEMPEST Technical Authority (CTTA) still need to rule on.

IMPORTANT: PUBLIC-LEVEL PLANNING DOCUMENT

Do not enter classified information, CUI, or facility street addresses in this document. Share completed questionnaires only through channels your security officer approves.

A completed questionnaire can describe a real facility's security posture. Keep answers general (types, yes/no, roles), leave out locations, room numbers and vulnerabilities, and follow the document-handling rules in your Construction Security Plan.

Project identification (non-sensitive)

Project nickname	*Use a code name. No facility name or street address.*	**Prepared by (role)**	
Date prepared		**Revision**	
Your organization type	☐ Government ☐ Contractor ☐ Owner / landlord ☐ Designer (A-E) ☐ General contractor ☐ Integrator		

How to use this template

- Tick **Yes**, **No** or **Unk.** (unknown) for each item, then add short notes. Checkboxes are clickable in Microsoft Word; on paper, mark them by hand.
- Every **Unknown** is an action item. Collect them in the open-items log in Section N and take them to your first AO / CSA / CTTA meeting.
- This is not a government form. It does not replace the IC Tech Spec forms (Pre-Construction Checklist, Fixed Facility Checklist, TEMPEST Checklist, Construction Security Plan) or DoD, DCSA and program equivalents.
- References are to public documents: ICD 705 (2010), ICS 705-1 (2010), ICS 705-2 (2016), IC Tech Spec v1.5.1 (26 Jul 2021), UFC 4-010-05 (26 May 2023), DoDM 5205.07 (17 Jan 2025), 32 CFR Parts 117 and 2001, and UL 2050 Edition 6 (7 Apr 2025). Many items are left to AO or CSA determination; exceeding a published standard requires a waiver.
- Sections: A Program · B Space & site · C Operating mode · D Perimeter · E Doors · F Penetrations & utilities · G Acoustics · H Intrusion detection · I Access control · J TEMPEST · K PEDs, telecom & CCTV · L Life safety · M Construction security · N Documents & schedule · O Sign-off.

A Program & sponsorship

Who needs the space, under what authority, and who approves it. Security planning starts when the requirement is known, not when construction starts.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
A1	A government sponsor has documented the requirement for the space (contract, agency requirement or program need).	☐	☐	☐	☐ IC element ☐ DoD component ☐ Other federal ☐ Contractor under sponsorship	Accreditation needs a sponsor. Tech Spec 2.A: coordinate with the AO before design, material ordering or contracts are finalized.
A2	A contract vehicle and funding line cover design, construction, testing and accreditation (not just build-out).	☐	☐	☐	*Vehicle type / funding notes*	Escorts, badging, document control, UL 2050 certification, acoustic and IDS testing are real costs. Bidders who don't see them won't price them.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
A3	The information to be protected is known.	☐	☐	☐	☐ SCI ☐ SAP ☐ Collateral only ☐ More than one	SCI follows ICD 705 and the IC Tech Spec; SAP follows DoDM 5205.07 with a SAPF-AO; collateral follows 32 CFR 117 / 2001. This sets the rulebook and the approver.
A4	The Accrediting Official (AO) or Cognizant Security Authority (CSA) is identified and has been contacted.	☐	☐	☐	*Office / role only*	The AO approves the design concept, the Construction Security Plan (CSP) and the final design before construction starts. Requirements vary by AO.
A5	A Site Security Manager (SSM) or Special Security Officer (SSO) is assigned to the project.	☐	☐	☐	*Role / organization*	The SSM develops the CSP, runs periodic security inspections during construction and is the point of contact for field changes.
A6	Co-use or joint use by another agency, program or tenant is expected.	☐	☐	☐	☐ Co-Use Agreement ☐ Shared IDS partition ☐ None expected	Co-use is handled under ICS 705-2. Exceeding a standard without a waiver can cost the SCIF its reciprocity with other agencies.
A7	The project intends to meet the standard as written (no planned waivers or "extra" features).	☐	☐	☐		Tech Spec 2.A: exceeding a standard, even based on risk, requires an approved waiver. A waiver removes mandatory reciprocal use.

B Space & site

What kind of space you have, what surrounds it, and whether it can physically become a SCIF or SAPF.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
B1	Tenure of the space is known.	☐	☐	☐	☐ Leased ☐ Owned ☐ Government-furnished	Perimeter walls to the true deck, reinforced doors and sealed penetrations are permanent alterations. The lease must allow them.
B2	The lease or building rules allow slab-to-slab walls, perimeter penetrations and changes to shared building systems.	☐	☐	☐		Walls must run true floor to true ceiling. Landlord approvals discovered late stall design.
B3	The floor level and adjacent spaces (above, below, beside) are identified in general terms.	☐	☐	☐	☐ Other tenants ☐ Public areas ☐ Controlled space	Adjacent spaces and their risk are CSP inputs. Alarmed, access-controlled office space around the SCIF can count toward Security-in-Depth.
B4	The facility is located inside the United States.	☐	☐	☐	☐ Inside the U.S. ☐ Outside the U.S. *No country name needed*	Outside the U.S., Security-in-Depth is mandatory and threat Category drives construction, surveillance, material controls and cleared finish workers (Tech Spec Ch. 2, 4, 5).
B5	The space is, or was, an accredited SCIF / SAPF that will be reused or modified.	☐	☐	☐	☐ Currently accredited ☐ Previously accredited	Modifications can trigger re-accreditation. Legacy items (Level I switches, older locks, expired certificates) may need replacement at the next major change.
B6	Building utilities that serve other areas (sprinkler mains, ducts, drains, conduit) currently cross the planned space.	☐	☐	☐		Tech Spec 3.G.3: utilities serving other areas shall not transit the SCIF unless mitigated with AO approval. Rerouting is a landlord and budget issue.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
B7	There is room for a vestibule and PED lockers outside the primary entrance, and a telecom room within or adjacent to the space.	☐	☐	☐		A vestibule is recommended. UFC 3-4.7: PED lockers not recessed in the perimeter or within 10 ft of unencrypted NSI processing. Adjacent telecom rooms reduce PDS needs.

C Operating mode

How the space will run. Storage mode and Security-in-Depth drive wall type and alarm response time.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
C1	The storage / operating mode is decided.	☐	☐	☐	☐ Closed storage ☐ Open storage ☐ Secure Working Area (no storage) ☐ Continuous operation	Closed storage and Secure Working Areas use Wall A with a 15-minute response. Open storage depends on Security-in-Depth (see C3–C4).
C2	The space will be staffed 24 hours a day, 7 days a week.	☐	☐	☐		Tech Spec 3.H sets no separate IDS response time for continuous operation. Get the AO's decision in writing.
C3	Security-in-Depth (SID) layers exist around the space (tick all that apply).	☐	☐	☐	☐ Military / government / contractor compound with response force ☐ Controlled building: separate access control, alarms, elevator control ☐ Alarmed, controlled office areas around the SCIF ☐ Fenced compound with access-controlled gates	Tech Spec 2.B.3 primary means. AO-accepted SID can allow Wall A and a 15-minute response for open storage. Without SID: Wall B or C and a 5-minute response.
C4	The AO has accepted the SID layers in writing.	☐	☐	☐		SID is documented (FFC Section B, CSP SID block), not assumed. Designing Wall A for open storage before acceptance is a common redesign trigger.
C5	The SID systems (lobby access control, building alarms, CCTV) are under change control, even if the landlord runs them.	☐	☐	☐		If a landlord removes lobby access control, open storage can suddenly need a 5-minute response it cannot meet. Report SID changes to the AO first.
C6	The number and type of GSA-approved security containers is estimated.	☐	☐	☐	*Class 5 / Class 6 estimate*	Closed storage relies on containers. Confirm containers are current GSA-approved models and plan replacement of phased-out black-label units.

D Perimeter & construction

The physical boundary: walls, ceilings, floors, windows and any vault.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
D1	Perimeter walls can run true floor to true ceiling (slab to slab) on every side.	☐	☐	☐		Required for the SCIF perimeter. Walls that stop at a drop ceiling fail and can drive AO requirements for plenum motion detection.
D2	The expected perimeter wall type is known.	☐	☐	☐	☐ Wall A ☐ Wall B (expanded metal) ☐ Wall C (plywood) ☐ Existing masonry / concrete ☐ TBD	Tech Spec 3.C: Wall A is the standard (designed for Sound Group 3). Walls B and C add forced-entry hardening for open storage without SID.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
D3	False ceilings or raised floors in the space connect to non-SCIF space.	☐	☐	☐		An AO may require plenum motion detection or another fix. Floor and ceiling penetrations must be kept to a minimum (Tech Spec 3.D).
D4	The perimeter has windows. If yes, some are within 18 ft of the ground or an accessible platform (roof, ledge, canopy).	☐	☐	☐		Windows are non-opening with visual and acoustic protection; RF treatment if the CTTA recommends. Within 18 ft: perimeter-standard forced-entry protection plus IDS (Tech Spec 3.F).
D5	A vault is required by the sponsor, program or AO.	☐	☐	☐		A vault changes structure, schedule and door procurement. A vault door cannot be the day-access door; UFC calls for a GSA-approved Class 5 vault door meeting ABA.
D6	Devices on perimeter walls will be surface-mounted, in raceway, or on a furred wall (no recessed boxes or cabinets).	☐	☐	☐		Tech Spec 3.G.5 and UFC 3-4.4.7. Recessed outlet boxes, panels and extinguisher or PED cabinets in treated perimeter walls are recurring findings.
D7	Some perimeter walls or doors are also fire-rated assemblies.	☐	☐	☐		Acoustic door assemblies on rated corridors must also carry the fire label, and penetrations need listed firestop systems. Coordinate early.

E Doors & hardware

Every perimeter door is Primary, Secondary or Emergency egress-only. The category decides the hardware.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
E1	The primary entrance location is set (one primary entrance unless the AO approves otherwise).	☐	☐	☐		Primary door: FF-L-2890 deadbolt plus FF-L-2740 combination lock plus an approved access control device. Visitor control happens here.
E2	Secondary (entry and exit) doors are needed and the AO has authorized them.	☐	☐	☐	*Count*	Secondary doors need AO authorization, use an FF-L-2890 egress device with deadbolt, and their ACS must be deactivated when the SCIF is unoccupied (Tech Spec 3.E.3).
E3	Emergency egress-only doors are required by code or the AHJ.	☐	☐	☐	*Count*	Exit-only FF-L-2890 device, no exterior hardware, alarmed 24/7 with a local audible annunciator (Tech Spec 3.E.4).
E4	An FF-L-2740B combination lock model is selected and a buyer eligible to purchase it is identified.	☐	☐	☐	☐ Kaba Mas X-10 ☐ S&G 2740B ☐ Existing lock to evaluate	FF-L-2740B sales are restricted to the government and authorized contractors. X-07/X-08 are past expected service life; X-09 is no longer made.
E5	An FF-L-2890 device type from the current QPL is chosen for each door.	☐	☐	☐	☐ Types I–IV (primary) ☐ VII–VIII (secondary) ☐ IX–X (exit-only)	Hardware called "SCIF" or "2890-style" that is not on the current QPL is not an FF-L-2890 device; alternates need AO approval. The DoD Lock Program says to check with the AHJ before procurement.
E6	A vestibule is planned at the primary entrance. If interlocked, the AHJ has been consulted.	☐	☐	☐		Tech Spec 3.E.5 recommends a vestibule to preclude visual observation and improve acoustics. Interlocks are not covered by model codes and need AHJ approval.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
E7	Door assemblies will be factory STC-tested assemblies with 7-, 10- and 12-gauge reinforcement shown on the door schedule.	☐	☐	☐		UFC 3-4.6.1: tested to at least STC 50 for an STC 45 perimeter, STC 55 for STC 50. Hinge 7-ga, lock area 10-ga, closer 12-ga reinforcement are factory items.
E8	Double-leaf, roll-up or adjoining-SCIF doors are part of the design.	☐	☐	☐		Double doors: each leaf has its own alarm contact; fixed leaf bolted top and bottom. Roll-up doors: 18-ga steel, deadbolts both sides, alarmed (Tech Spec 3.E.6).
E9	Electrified hardware will be positive-engagement, fail-secure and UL 1034 listed (no magnetic locks); REX devices inside only.	☐	☐	☐		UFC 3-4.6.5. Maglocks are fail-safe. A REX that shunts the door's alarm switch or can be triggered from outside defeats both ACS and IDS.

F Penetrations & utilities

Every duct, pipe, conduit and cable that crosses the perimeter needs a reason, a location and a treatment.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
F1	A penetration schedule exists (one line per duct, pipe, conduit, sleeve and cable bundle, with size and treatment).	☐	☐	☐		Tech Spec 3.G.1: keep penetrations to a minimum. The schedule becomes the pre-cover inspection checklist and part of the accreditation evidence.
F2	Any duct or vent opening through the perimeter exceeds 96 sq in with no dimension under 6 in.	☐	☐	☐		Tech Spec 3.G.7: bars (½-in steel, 6 in on center), approved grilles or metal baffles, plus an inspection port. Acoustic treatment applies to every duct regardless of size.
F3	A sprinkler main or other fire-protection line that serves other areas would cross the space.	☐	☐	☐		Only lines serving the SCIF should enter (3.G.3). Metallic pipe may need grounding or a dielectric break, but only when the CTTA recommends it (3.G.2).
F4	Plumbing, drains, condensate or refrigerant lines run in or through the space.	☐	☐	☐		More penetrations, more maintenance access by uncleared workers, and possible TEMPEST treatment. Relocate where you can.
F5	Power and signal can enter the space at a single point.	☐	☐	☐	*General location (e.g., "near telecom room")*	Tech Spec 3.G.4 and UFC 3-4.19: single point of entry, cables labeled at the entry point. Late additions from other walls break this concept.
F6	Spare conduit for future growth is planned, filled with acoustic fill and capped.	☐	☐	☐		Tech Spec 3.G.6. An open spare sleeve is an acoustic leak and an unmonitored path into the space.
F7	Filtered power or signal lines are required.	☐	☐	☐	☐ CTTA has directed ☐ Not directed ☐ Review pending	Filters are a CTTA or shield-designer decision, not a default. When used: unfiltered conductors terminate outside and never cross, only filtered conductors continue in, case bonded into the shield plane; check generator kVAR and GFCI leakage.
F8	Standby power (UPS and/or generator) is available for IDS, ACS and communications equipment.	☐	☐	☐		IDS needs 24 hours of uninterruptible backup power (Tech Spec 7.B.5). DoD: with a generator, IDS batteries still provide at least 4 hours.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
F9	Air handlers, mechanical and electrical rooms will sit outside the space.	☐	☐	☐		UFC 3-3.3.2 keeps building support spaces outside secure areas. Acoustic Z-ducts and silencers also need above-ceiling space.
F10	Building automation (BAS/HVAC controls, sensors) will have devices inside the space.	☐	☐	☐		Automated environmental systems are declared on the Fixed Facility Checklist, with countermeasures against intrusion and exploitation.

G Acoustics

Which rooms are discussion areas, which use amplified audio, and how sound is kept in.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
G1	Every room is marked as Sound Group 3, Sound Group 4, or non-discussion on the plan.	☐	☐	☐		Sound Group 3 = STC 45 (perimeter minimum). Sound Group 4 = STC 50 for amplified audio. Zone rooms before wall types are drawn.
G2	VTC, speakerphones, conference or presentation audio are planned.	☐	☐	☐	*Which room types*	UFC 3-4.3.2: rooms with amplified audio such as VTC must meet Sound Group 4. Adding VTC to a Sound Group 3 room later can take it out of compliance.
G3	Sound masking is anticipated to cover weak paths (doors, windows, ducts).	☐	☐	☐		Masking needs AO approval. Generator permanently inside the SCIF, no AM/FM receiver, recording disabled, wiring inside, subject to TSCM review.
G4	PA, background music or voice-evacuation speakers will be inside the space.	☐	☐	☐		The Fixed Facility Checklist asks for fiber isolation, self-amplified speakers or another method to ensure no audio back feed.
G5	The acoustic test approach is known (audio test vs. instrumented test).	☐	☐	☐		Field equivalents: NIC 40 for Sound Group 3 and NIC 45 for Sound Group 4. Doors, glazing and ducts are the usual weak points.

H Intrusion detection (IDS)

UL 2050 Extent 3 and IC Tech Spec Chapter 7. These are the core Chapter 7 items. Chapter 7 wording here is quoted from the public v1.4-era copy; confirm against v1.5.1.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
H1	The alarm company is listed by UL for National Industrial Security Systems (CCN CRZH), verified in UL Product iQ.	☐	☐	☐	*UL file number*	SCIF and SAPF work needs a UL 2050 National Industrial Security System certificate. A mercantile (CVSG) "Extent 3" certificate is not UL 2050.
H2	The design is an Extent 3 installation (no Extent 5).	☐	☐	☐		Tech Spec 7.A.2.b: "Installation shall comply with an Extent 3 installation as referenced in UL 2050." Extent 5 never applies under ICD 705.
H3	The monitoring station is identified and its operators are U.S. citizens eligible for SECRET.	☐	☐	☐	☐ Government ☐ GCMS ☐ NIMS (CRZM) ☐ UL central station	Tech Spec 7.B.6 lists the allowed station types and operator requirements. UL 2050 Edition 6 may change earlier station rules; confirm with your CSA.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
H4	A response force is identified under a written agreement that meets the required time.	☐	☐	☐	☐ 15 min (closed / open with SID) ☐ 5 min (open, no SID)	Tech Spec 3.H. The FFC asks who responds, whether they are cleared, the written agreement, and the response time in minutes.
H5	An SCI-indoctrinated person can reach the space within 60 minutes (or an AO-approved time) after an alarm.	☐	☐	☐		Tech Spec 7.C.1.c. That person inspects, finds the cause and resets the IDS before the response force leaves.
H6	Panel-to-station communication uses a FIPS-validated encryption module, with its CMVP certificate on file.	☐	☐	☐	☐ FIPS 140-3 ☐ FIPS 140-2 only ☐ Unknown	Tech Spec 7.A.3.b(10). FIPS 140-2 validations move to NIST's Historical List on 21 Sep 2026; ask the AO before specifying a 140-2-only module.
H7	A 24-hour standby battery calculation will include the communicator, encryption and network equipment.	☐	☐	☐		Tech Spec 7.B.5. A frequent miss: the panel stays up but the IP or cellular path to the station goes dark.
H8	Every perimeter door gets a UL 634 Level II high-security switch AND UL 639 motion; the PCU and arming station are inside; entry delay is 30 s or less.	☐	☐	☐		Tech Spec 7.A.2.d, 7.A.3.a(6)–(7), 7.A.3.b(1). Keypads on the corridor side let people change modes from outside the SCIF.
H9	The IDS will be separate from fire, smoke, water and other systems, with no video-verified sensors or microphones unless the AO approves.	☐	☐	☐		Tech Spec 7.A.2.h and 7.A.2.l. Shared panels and audio/video-capable devices are common findings.
H10	IDS cabling that leaves the space will be encrypted or in sealed ferrous conduit (no set screws) with locked boxes.	☐	☐	☐		Tech Spec 7.A.2.e. A sensor cable above a corridor ceiling in set-screw EMT with an unlocked box breaks three rules at once.
H11	Installers and testers are a U.S. company using U.S. citizens; maintenance staff are TOP SECRET-cleared or escorted; service starts within 4 hours.	☐	☐	☐		Tech Spec 7.D.1 and 7.C.2. Put the 4-hour service start and escort arrangements in the contract.
H12	If the IDS is networked: the host is in a physically protected space, passwords are 12+ characters changed every 6 months (or PIV/CAC), and remote programming is monitored.	☐	☐	☐		Tech Spec 7.A.3.c. Only SCI-indoctrinated U.S. personnel may change system variables and passwords.

I Access control (ACS)

Who may enter during duty hours. Access control never secures an unoccupied SCIF; the combination lock and IDS do.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
I1	The existing or planned PACS platform is documented (make, software version, controller and reader models, firmware).	☐	☐	☐	☐ Hirsch Velocity ☐ Other enterprise PACS ☐ Standalone ☐ None	Record every controller and reader and its crypto module certificate in the accreditation package. A GSA FIPS 201 APL listing does not by itself make a PACS "SCIF-approved".
I2	The ACS head-end, server and database will be inside the SCIF or an alarmed area controlled at the SECRET level (or an AO-approved architecture).	☐	☐	☐		FFC §C.1 asks exactly this. "One server for the whole building" or cloud hosting in unsecured space needs AO approval before bid.
I3	Credentials in use are known.	☐	☐	☐	☐ PIV ☐ CAC ☐ Other card	ICS 705-1 G.2.b: automated entry uses at least two technologies. UFC: card reader with keypad at the primary and secondary entrances.
I4	SCIF doors will be configured for card + PIN at all times (not just capable of it).	☐	☐	☐		A keypad reader set to "card only" during business hours is a single-factor door. Lock the PIN requirement into the door schedule and SOP.
I5	Reader and panel lines leaving protected space are encrypted (FIPS), outside readers are tamper-protected, and wiring is reachable only from inside.	☐	☐	☐		FFC §C.1 and Tech Spec Ch. 8. An unencrypted Wiegand run from a corridor reader to a panel outside the perimeter does not meet the question.
I6	Compartmented areas or nested spaces are planned inside the SCIF.	☐	☐	☐		Tech Spec 2.C.4: no spin-dial combination locks on CA doors and no independent alarm systems in a CA. UFC: entry into a lower area cannot be through a higher one.
I7	A visitor process is defined at the primary entrance (sign-in, PED check, escort, uncleared-presence warning light).	☐	☐	☐		UFC 3-4.6.7 one primary entrance for visitor control; UFC 3-4.15 flashing or rotating light with controls inside each entrance.
I8	ACS enrollment, PIN resets, backups and remote support are limited to SCI-indoctrinated personnel.	☐	☐	☐		FFC §C.1 asks whether ID data and PINs are restricted to SCI-indoctrinated staff. Routine remote support by uncleared vendor technicians is ruled out.
I9	Secondary-door readers will be disabled as part of the closing procedure, and the ACS log retention period is agreed with the AO.	☐	☐	☐		Tie deactivation to the IDS arming sequence rather than a clock schedule. Confirm retention against Tech Spec 8.D and 12.L.

J TEMPEST & RF

Status questions only. Separation distances and countermeasure details come from your CTTA and never belong in this document.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
J1	Classified information will be processed electronically in the space.	☐	☐	☐		If yes, a TEMPEST Checklist is completed (FFC §I). DoD programs submit it as the TEMPEST Addendum.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
J2	CTTA review status is known.	☐	☐	☐	☐ Not started ☐ Checklist submitted ☐ Recommendations received	A late CTTA review can force redesign. ICS 705-1: RF shielding required by CTTA evaluation should be planned during initial construction.
J3	RED equipment (processes unencrypted classified information) and BLACK equipment are identified by type.	☐	☐	☐	*Types only. No room locations.*	The CTTA needs equipment types to plan countermeasures. Keep pathways separate and labeled; take specifics only from the stamped drawings.
J4	Signals will enter the space on fiber rather than copper.	☐	☐	☐	☐ All-dielectric fiber ☐ Copper ☐ Mixed	Non-conductive fiber avoids a conductive path across the perimeter. Specify all-dielectric cable: no armor, steel strength member or tracer wire.
J5	The RF shielding scope is known, and the test method and acceptance criteria are written into the contract.	☐	☐	☐	☐ None ☐ Architectural foil ☐ Shielded racks ☐ Full enclosure	Every penetration added after a shield test needs review and a retest. Schedule test and retest time in the baseline.
J6	Radio transmitters or receivers are planned in or near the space (wireless IDS, Wi-Fi, cellular communicators, wireless locks, BAS radios).	☐	☐	☐		RF transmitters need CTTA evaluation and AO approval. The TEMPEST Checklist asks about radios in and near the SCIF. Design wired first.
J7	Encryption equipment will be located so Protected Distribution Systems (PDS) are avoided.	☐	☐	☐		UFC 3-3.3.2: telecom spaces with encryption equipment within or adjacent to the secure area. UFC 3-4.20: avoid PDS whenever possible.
J8	Completed TEMPEST documents will move only through AO-designated channels.	☐	☐	☐		A completed TEMPEST Checklist describes a real facility's vulnerabilities. Never post it to bid sites, shared drives or email lists.

K PEDs, telecom & CCTV

Personal devices, phones and cameras are frequent late additions. Decide them now.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
K1	PED policy is set and lockers will be outside the primary entrance.	☐	☐	☐		UFC 3-4.7: no recessed PED cabinets on the perimeter; not within 10 ft of equipment processing unencrypted national security information.
K2	PED / wireless detection is planned.	☐	☐	☐	☐ Fixed RF detector at entry ☐ WIDS sensor network ☐ Handheld detector ☐ Ferrous / metal screening ☐ Not planned	RF detection only sees transmitting devices; powered-off phones are invisible. Sensors inside the SCIF need AO/CTTA review; detectors must never block egress.
K3	Medical devices or other PEDs will need approval for use inside.	☐	☐	☐		Approvals must be obtained before the device is introduced (DCSA SAP checklist F-10; Tech Spec Ch. 10).
K4	Unclassified phones will be CNSSI 5006 (TSG-6) approved instruments or use approved disconnect devices.	☐	☐	☐	☐ Analog / PSTN ☐ CTS / PBX (CNSSI 5002) ☐ VoIP (CNSSI 5000)	The FFC asks about on-hook protection, whether a CTS can force a phone off-hook, and whether speakerphones and microphones are enabled.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
K5	Cameras will be outside only, viewing the entrance, with no view into the space and no view of keypads or lock dials.	☐	☐	☐		UFC 3-4.17.2: cameras are not allowed within the perimeter or to enable observation within it. Use cameras without microphones.
K6	Entrance video intercom or remote door release will be controlled from inside by SCI-indoctrinated staff.	☐	☐	☐		Tech Spec 8.E: CCTV may supplement entrance monitoring, with the remote control device inside the SCIF.
K7	Copiers / MFDs, VTC, commercial TV and other connected equipment are listed for the Fixed Facility Checklist.	☐	☐	☐		The FFC has questions for each (memory, hard drives, voice capability, CATV floor plan). Undeclared equipment surfaces at inspection.

L Life safety & AHJ

The Authority Having Jurisdiction (AHJ) and the AO both have jurisdiction. Occupants must always be able to get out.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
L1	The AHJ (building official / fire marshal) is identified and an early meeting is scheduled.	☐	☐	☐		Panic hardware, delayed egress, fire-rated openings and interlocks are AHJ decisions. Conflicts found at the final inspection force hardware changes.
L2	The egress plan is known: number of exits, egress-only doors, and whether occupancy requires panic hardware.	☐	☐	☐		FF-L-2890C Types III, IV, VIII and X include panic hardware. Types V and VI are for rooms not regularly occupied.
L3	Delayed egress is proposed.	☐	☐	☐		UFC 3-4.6.10 recommends delayed egress with NFPA 101 compliance, where permitted. Get AHJ and AO approval before ordering hardware.
L4	The fire alarm notification approach inside the space is agreed with the AHJ, AO and CTTA.	☐	☐	☐	☐ Isolation inside SCIF ☐ Visual-only where permitted ☐ TBD	Speakers can act as microphones; wiring back to the building panel is an audio path. The FFC asks how audio back feed is prevented.
L5	Fire alarm and sprinkler monitoring panels will be outside the space, with only field devices inside.	☐	☐	☐		UFC 3-3.3.2: utilities and building support spaces should remain outside the secure area. Tech Spec 7.A.2.h also keeps the IDS independent of fire and other systems.
L6	Accessibility items are reviewed: hardware and reader heights, vestibule clearances, RF or acoustic door thresholds.	☐	☐	☐		FF-L-2890C hardware is one-hand operable. Raised thresholds on shielded doors and tight vestibules can conflict with accessibility rules.
L7	Emergency responder access and a post-emergency security inspection will be written into the SOP.	☐	☐	☐		Responders may enter during an emergency. The SOP defines who inspects the space afterward and how the event is reported.

M Construction security

The Construction Security Plan (CSP) is the AO-approved rulebook from design through turnover.

#	Question / item	Yes	No	Unk.	Response / notes	Why it matters
M1	A CSP will be developed by the SSM and approved by the AO before the construction contract is awarded.	☐	☐	☐		Tech Spec 3.B.1. UFC: "Do not award a construction contract without an approved CSP."
M2	The AO has decided whether Construction Surveillance Technicians (CSTs) or cleared escorts are required.	☐	☐	☐	☐ CSTs ☐ Cleared escorts ☐ Neither ☐ Pending	Inside the U.S., CST use is threat- and AO-driven and recorded in the CSP. Outside the U.S., CSTs hold TOP SECRET clearances.
M3	Workforce rules are flowed down to every trade (U.S. companies using U.S. citizens, or U.S. persons with AO mitigations).	☐	☐	☐		Tech Spec 3.B.5. IDS installation and testing is stricter: U.S. companies using U.S. citizens. Citizenship is not a clearance.
M4	Site access controls are defined: identity checks, random searches, prohibited-item signage, barriers, vehicle inspections.	☐	☐	☐		Tech Spec 3.B.6 considerations. Plan one controlled entry to the work area, a sign-in log and a delivery inspection point.
M5	Material procurement, receiving inspection and secure storage procedures are set for materials concealed in the perimeter.	☐	☐	☐		UFC 4-3: the AO may impose procurement, shipping and storage procedures. Locks, STC doors, 2890 devices and shielding have long lead times.
M6	A photographic construction surveillance record will cover penetrations, door installations and wall assemblies before cover.	☐	☐	☐		UFC 4-7. Photos of bars, grounds, seals and hardening layers before ceilings close are the evidence reviewers ask for.
M7	Drawings, penetration schedules and test reports will be handled per the CSP (not on public bid portals or open shares).	☐	☐	☐		Tech Spec 3.B.2; UFC 4-2 protects SCIF location and identity at minimum as CUI.
M8	A procedure exists to report security violations to the AO within 3 business days.	☐	☐	☐		Tech Spec 3.A. Name who reports, how, and where records are kept.

N Documents to gather & schedule

Track the approval documents and milestones. Tick one status per row. Record owner by role, not by name, in any shared copy.

Document	Not started	Draft	Submitted	Approved	Owner (role)	Target date	Notes
Sponsorship / concept approval	☐	☐	☐	☐			Starts AO coordination
Pre-Construction Checklist	☐	☐	☐	☐			Tech Spec Ch. 14 form
Fixed Facility Checklist (FFC)	☐	☐	☐	☐			Living document through accreditation
TEMPEST Checklist / TEMPEST Addendum	☐	☐	☐	☐			Requests CTTA review
Construction Security Plan (CSP)	☐	☐	☐	☐			Approved before contract award

Document	Not started	Draft	Submitted	Approved	Owner (role)	Target date	Notes
Design drawings & specifications	☐	☐	☐	☐			Include penetration and door hardware schedules
UL Form CS-ASD-NISS (alarm system description)	☐	☐	☐	☐			CSA signs prior-approval items
Monitoring contract & response force agreement	☐	☐	☐	☐			Response time, duties, POCs
IDS acceptance test plan & 24 h battery calculation	☐	☐	☐	☐			Walk test, HSS, tamper, power
Acoustic test plan	☐	☐	☐	☐			Sound Group 3 / 4 rooms
RF shielding test plan (if any)	☐	☐	☐	☐			Method, frequencies, criteria
SOP drafts: opening/closing, IDS, visitors, PEDs, emergencies	☐	☐	☐	☐			Walk the AO through at acceptance
Co-Use Agreement (if any)	☐	☐	☐	☐			ICS 705-2
Waiver requests (if any)	☐	☐	☐	☐			Affects reciprocity

Key milestones

Milestone	Target date	Dependency / note
AO / CSA kickoff meeting		Bring every "Unknown" from this questionnaire
CTTA recommendations received		Before shield, filter or cable procurement
Design approval		AO approves concept, CSP and final design before construction
Construction contract award		Only after the CSP is approved
Pre-cover inspection (walls, penetrations, grounds, bars)		Photo record complete before ceilings close
RF shielding test (if any)		After all penetrations, filters, waveguides and doors
IDS acceptance test & UL 2050 certificate		Certificate renewed after any later IDS change
Acoustic testing		Leave time to fix doors, glazing and ducts
Final inspection, TSCM and accreditation target		Do not schedule the shield test the day before

Open-items log (collect every "Unknown")

#	Open item (keep it general)	Owner (role)	Needed by	Resolution
1				
2				
3				
4				
5				
6				
7				
8				

O Sign-off

Signatures record that the people below reviewed this planning template. They are not approvals. Only the AO / CSA, CTTA and AHJ approve designs, countermeasures and life-safety features.

Role	Name (optional in shared copies)	Signature	Date
Program / sponsor representative			
Site Security Manager / SSO			
Facility owner or landlord representative			
Designer of record (architect-engineer)			
General contractor			
Low-voltage / IDS integrator			
Prepared by			

Additional notes (non-sensitive)

About this template

Educational template published by LA CCTV Supply for SCIF and SAPF project planning. It summarizes public requirements as of September 2026 and is not an official government form. It does not grant, imply or replace accreditation, certification or clearance decisions. Requirements for your project are set by your AO / CSA, CTTA and AHJ; where this template and their direction differ, follow their direction.

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