Contents

AI705 — ICD 705 → Frontier AI Datacenters

Version 0.1 working draft · May 2026

Authors: Lisa Thiergart, Luis Cosio, Luke Sallmen, Guy

Security Level 5 Task Force · https://ai705.sl5.org

About This Document

AI705 is a proposed gap analysis and technical guidance project for applying ICD 705 and the IC Technical Specifications for ICD/ICS 705 to frontier AI datacenters. Its purpose is practical: give labs, datacenter operators, colocations, facilities teams, and accrediting officials a shared reference for physically secure environments that handle frontier model weights.

The output is a technical guidance document that states, for each source requirement, whether it applies as written, applies with AI/datacenter-specific modification, is inapplicable, or leaves a gap requiring new controls. This follows the same source-to-guidance discipline used in the SL5 Standard for AI Security, but the unit of analysis is an ICD 705 or IC Tech Spec requirement rather than a NIST SP 800-53 control.

Why The Threat Vectors Matter

AI705 treats weight theft, secret theft, and sabotage as separate control outcomes. A facility measure that protects stored checkpoints may not protect construction plans, operational telemetry, credentials, or power and cooling paths from sabotage.

Weight theft still carries three categories: stored weights, training systems, and inference systems. A single facility baseline is useful only if those category differences stay visible while secret theft and sabotage are reviewed as first-class outcomes.

About The Security Level 5 Task Force

The SL5 Task Force is a non-profit cross-industry effort working to ensure frontier AI infrastructure can achieve nation-state-level security by 2028/2029. Founded in March 2025, it is a core team of engineers and security strategists leading a 100-person technical track of security engineers from frontier AI labs, government security specialists, and datacenter colocation providers, alongside an executive track of AI industry security leaders providing steering input.

The Task Force convenes technical work that clarifies what needs to be done early to preserve security optionality. AI705 is one output of that effort, focused on the physical, construction, accreditation, and side-channel questions raised by applying ICD 705 to frontier AI facilities.

Scope & Roadmap

v0.1 — Scope of this draft

v0.1 covers every source requirement in ICD 705, ICS 705-01, ICS 705-02, and the IC Tech Spec v1.5.1. The work is a literature review and expert consultation: each requirement is read against the existing public body of practice, judged against weight theft / secret theft / sabotage, and recorded with the assumptions and counterevidence the reviewers surface.

A subset of the rows is walked in deeper detail and published with individual verdicts — the requirements most likely to change when applied to AI datacenters (security-in-depth, the Construction Security Plan, TEMPEST and RF shielding, perimeter penetrations, intrusion detection and continuity, access control systems, acoustic protection, PED / wireless / RCET, environmental infrastructure, protected distribution systems, and re-accreditation after de-accreditation). These published rows show what the full pipeline looks like end to end; they are not the scope.

v0.1 deliberately does not include new measurements, new test campaigns, or third-party engineering work. Where the literature does not settle a question, v0.1 publishes the gap with an explicit measurement question rather than a synthesized answer.

v0.2 — Planned scope

v0.2 closes the evidence gaps v0.1 surfaces. The plan has three tracks:

1. **Operator review.** Facilities teams, colocation operators, and accrediting officials review the rows whose v0.1 verdict is “Applies with modification” or “Needs evidence” and record which assumptions hold in production.

2. **Measurement campaign.** A targeted set of physical measurements answers the questions v0.1 cannot settle from existing literature: accelerator-rack emanations, acoustic side channels at modern hardware, environmental-infrastructure boundaries on shared datacenter floors, and protected distribution paths for high-rate optical links.
3. **Third-party engagement.** CTTA-credentialed reviewers, TEMPEST contractors, and IDS / BMS vendors are engaged where v0.1 identifies an evidence boundary the project itself cannot cross.

Method

1. Normalize official source documents into requirement JSON.
2. Generate OSCAL-style source catalogs from those normalized rows.
3. Evaluate each source requirement against weight theft, secret theft, and sabotage.
4. For weight theft, preserve stored-weight, training-system, and inference-system category differences.
5. Record applies-as-written, applies-with-modification, inapplicable, gap, or needs-evidence verdicts.
6. Preserve measurement questions where current literature cannot settle the AI/datacenter-specific issue.

Source Corpus

Source	Role	Status
`icd-705`	primary baseline	downloaded
`icd-705-original`	historical context	downloaded
`ics-705-01`	primary baseline	downloaded
`ics-705-02`	primary baseline	downloaded
`ic-tech-spec-v151`	primary baseline	downloaded
`scif-fixed-facility-checklist-v15`	supporting baseline	downloaded
`scif-tempest-checklist-v15`	supporting baseline	downloaded
`scif-preconstruction-checklist-v15`	supporting baseline	downloaded
`construction-security-plan-v15`	supporting baseline	downloaded
`inspectable-materials-checklist-v15`	supporting baseline	downloaded
`scif-ca-checklist-v15`	supporting baseline	downloaded
`cnssi-7003`	adjacent standard	downloaded
`rand-rra2849-1`	threat-model reference	downloaded
`nist-sp-800-53-rev5-oscal`	alignment reference	downloaded

Threat Vectors

AI705 separates the outcome a control must prevent from the technical channel the evidence may use. Weight theft, secret theft, and sabotage are scored as first-class outcomes. Channels like electromagnetic leakage, power, cooling, BMS / OT, wireless, and physical intrusion stay as evidence tags.

Threat vector	Definition
Weight theft	Theft or unauthorized reconstruction of model weights, checkpoints, adapters, key material, or enough model state to reproduce protected capability.
Secret theft	Theft of non-weight secrets: facility design, security procedures, credentials, customer/user data, operational telemetry, procurement details, or sensitive mission information.
Sabotage	Physical or operational disruption, tampering, degradation, or manipulation of AI facility infrastructure, including power, cooling, racks, networks, sensors, and recovery paths.

Weight theft is subdivided because storage, training, and inference create different facility-control questions.

Weight-theft category	Definition
Stored weights	Stored weights, checkpoints, backups, archives, transfer staging, destruction/decommissioning, and associated key custody.
Training systems	Active training clusters, accelerators, schedulers, storage fabric, high-speed interconnect, power, cooling, maintenance, and side-channel exposure during computation.
Inference systems	Serving replicas, request/response paths, customer/user data boundary, caches/logs, online operations, remote administration, availability pressure, and model-update workflows.

Measurement priorities

- **Weight theft (P0):** ICD/ICS 705 and the IC Tech Spec protect SCI facilities, but AI705 must translate those requirements to model-weight custody across storage, active training, and serving replicas.
- **Secret theft (P1):** Traditional SCIF language maps naturally to many secret-theft cases, but AI705 must include datacenter design, operational, vendor, and telemetry secrets that are not model weights.
- **Sabotage (P1):** ICD/ICS 705 contains access, IDS, construction, and environmental controls, but AI datacenters require explicit sabotage review for power, cooling, BMS/OT, remote maintenance, and shared infrastructure.

Gap Matrix

Rows currently published in v0.1, grouped by analysis area. Each row is a single source requirement judged against weight theft, secret theft, and sabotage, with the weight-theft category breakdown (stored / training / inference) and source excerpts.

Physical envelope

Construction-time controls that define what crosses the facility boundary.

Security in depth and shared infrastructure Row ID: `pilot-001-security-in-depth-shared-infrastruc`

Source requirements: `ics-705-01.r0013`, `ic-tech-spec-v151.r0039`, `ic-tech-spec-v151.r0085`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	Shared landlord, loading, Meet-Me Room, contractor, and management spaces can expose non-weight secrets such as facility layout, access procedures, and security operations; SID must explicitly cover them.
Sabotage	Applies with modification	Shared power, cooling, network, logistics, and landlord-controlled layers can be disrupted without entering the protected AI area; SID must account for sabotage paths as well as theft paths.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	SID can reduce construction burden for stored weights only if shared-building, cage, and media-custody layers are explicitly documented.

Category	Verdict	Rationale
Training Systems	Applies with modification	Training facilities depend on power, cooling, loading dock, fiber, and maintenance layers that the SCIF framing does not enumerate.
Inference Systems	Applies with modification	Serving environments may rely on online operations and remote support; SID needs availability-aware assumptions for access paths and failure response.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ics-705-01.r0013` (p. 2, para. 13): 2. Security in Depth a. Security in Depth (SID) is the acceptance of the AO of external and/or internal SCIF factors that…
- `ic-tech-spec-v151.r0039` (p. 19, para. 39): 1. SID describes the factors that enhance the probability of detection before actual penetration to the SCIF occurs. The existence of a…
- `ic-tech-spec-v151.r0085` (p. 24, para. 85): g) Consider SID on USG or USG-sponsored contractor facilities to substitute for standards herein. (SID shall be documented in the CSP and…

Construction Security Plan and design-document control Row ID: `pilot-002-construction-security-`

Source requirements: `ics-705-01.r0018`, `ic-tech-spec-v151.r0100`, `ic-tech-spec-v151.r0101`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	AI facility construction plans reveal sensitive design secrets: rack layout, cooling routes, power topology, fiber paths, security devices, and operational chokepoints.

Threat vector	Verdict	Rationale
Sabotage	Applies with modification	Construction, renovation, supplier staging, and finishing-material control can introduce tamper paths or latent disruption mechanisms, so the CSP must cover sabotage as well as document handling.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Vaults, storage rooms, and transfer staging areas need CSP coverage when constructed or renovated.
Training Systems	Applies with modification	Training build-outs add AI-specific design documents for rack layouts, liquid cooling, power distribution, network paths, and supplier staging.
Inference Systems	Applies with modification	Serving sites need CSP coverage where model-serving infrastructure or weight-handling paths are built or modified.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ics-705-01.r0018` (p. 3, para. 18): 3. For each SCIF construction project, a Construction Security Plan (CSP) shall be developed to address the application of security to the…
- `ic-tech-spec-v151.r0100` (p. 25, para. 100): 1. Prior to awarding a construction contract, a CSP for each project shall be developed by the SSM and approved by the…
- `ic-tech-spec-v151.r0101` (p. 25, para. 101): 2. Construction plans and all related documents shall be handled and protected in accordance with the CSP.

TEMPEST review, RF shielding, and accelerator emanations Row ID: `pilot-003-tempest-rf-shieldi`

Source requirements: `ics-705-01.r0029`, `ics-705-01.r0075`, `ic-tech-spec-v151.r0144`

Threat vector	Verdict	Rationale
Weight theft	Gap	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Needs evidence	CTTA/TEMPEST review protects non-weight secrets too, but accelerator-specific emissions evidence is not yet strong enough to quantify leakage for realistic AI datacenter racks.
Sabotage	Inapplicable	RF shielding and TEMPEST planning are primarily confidentiality controls. Sabotage is handled by access, IDS, BMS/OT, power, cooling, and protected-path rows unless future evidence shows an RF injection or interference control is needed.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Stored weights still implicate key systems, storage controllers, and transfer workstations, but the compute-emissions problem is lower.
Training Systems	Gap	The source requires CTTA/TEMPEST review, but frontier training introduces high-power accelerator emissions and conducted side channels not quantified by ICD 705.
Inference Systems	Needs evidence	Serving replicas may create exploitable emissions, but risk depends on hardware, request patterns, shielding, and distance.

Falsifier: Change this verdict if a source requirement, established control, or source-checked evidence already covers the AI-specific risk.

Source excerpts:

- `ics-705-01.r0029` (p. 4, para. 29): (4) When RF shielding is required by Certified TEMPEST Technical Authority (CTTA) evaluation, it should be planned for installation during initial construction…
- `ics-705-01.r0075` (p. 8, para. 75): 6. CTTAs shall: a. Review SCIF construction or renovation plans to determine if TEMPEST countermeasures are required and recommend solutions. To the…
- `ic-tech-spec-v151.r0144` (p. 28, para. 144): a) RF protection shall be installed at the direction of the CTTA when a SCIF utilizes electronic processing and does not provide…

Perimeter penetrations for power, cooling, ducts, pipes, and conduit Row ID: `pilot-004-perimeter-penetrations`

Source requirements: `ic-tech-spec-v151.r0211`, `ic-tech-spec-v151.r0212`, `ic-tech-spec-v151.r0218`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	Power, cooling, fiber, conduit, ducts, and telemetry penetrations can carry covert sensors, unmanaged links, or leakage paths that expose operational secrets.
Sabotage	Applies with modification	The same penetrations can be used to disrupt cooling, power, fire suppression, sensing, or network service, so each path needs ownership, inspection, and tamper treatment.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Storage areas can usually minimize penetrations, but key custody and transfer rooms still need documented penetrations.
Training Systems	Applies with modification	Training clusters have dense power, cooling, fiber, fire suppression, and monitoring penetrations; minimization needs an AI datacenter interpretation.
Inference Systems	Applies with modification	Serving environments need equivalent treatment for network, cooling, and monitoring penetrations, especially in leased or colo space.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ic-tech-spec-v151.r0211` (p. 31, para. 211): 1. All penetrations of perimeter walls shall be kept to a minimum.
- `ic-tech-spec-v151.r0212` (p. 31, para. 212): 2. Metallic penetrations may require TEMPEST countermeasures, to include dielectric breaks or grounding, when recommended by the CTTA.
- `ic-tech-spec-v151.r0218` (p. 32, para. 218): a) All vents and ducts shall be protected to meet the acoustic requirements of the SCIF. (See Figure 4, Typical Air (Z)…

Acoustic protection and hardware acoustic side channels Row ID: `pilot-007-acoustic-protection`

Source requirements: `ics-705-01.r0030`, `ic-tech-spec-v151.r0968`, `ic-tech-spec-v151.r0974`, `ic-tech-spec-v151.r0988`

Threat vector	Verdict	Rationale
Weight theft	Gap	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.

Threat vector	Verdict	Rationale
Secret theft	Needs evidence	Speech acoustic protection applies to discussions and operations areas, but hardware acoustic, ultrasonic, and vibration leakage of operational secrets needs targeted evidence review.
Sabotage	Inapplicable	Acoustic protection is primarily a confidentiality control. Sabotage should be handled through access, tamper, environmental, and continuity controls unless measurement shows hardware acoustic control has disruption relevance.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Traditional acoustic protection matters for discussion and operations areas; pure storage areas may need less.
Training Systems	Gap	ICD acoustic rules focus on overheard discussions, not fan, pump, coil-whine, ultrasonic, or vibration channels from AI hardware.
Inference Systems	Needs evidence	Serving may expose acoustic or vibration patterns, but the practical leakage risk requires measurement.

Falsifier: Change this verdict if a source requirement, established control, or source-checked evidence already covers the AI-specific risk.

Source excerpts:

- `ics-705-01.r0030` (p. 4, para. 30): (5) SCIFs that require discussions of SCI shall provide acoustic protection to prevent conversations from being inadvertently overheard outside of the SCIF.
- `ic-tech-spec-v151.r0968` (p. 89, para. 968): 1. This establishes DNI guidelines to protect classified conversations from being inadvertently overheard outside a SCIF.

- `ic-tech-spec-v151.r0974` (p. 89, para. 974): 1. Audio tests shall be conducted to verify standards are met. Tests may be instrumental or non-instrumental as approved by the AO….
- `ic-tech-spec-v151.r0988` (p. 90, para. 988): 3. Utility (e.g., power, signal, telephone) distribution shall be surface mounted to a sound-treated wall and shall not completely penetrate the sound-engineered…

Protected Distribution Systems and high-speed AI data paths Row ID: `pilot-010-protected-distribu`

Source requirements: `ic-tech-spec-v151.r1145`, `ic-tech-spec-v151.r1146`, `cnssi-7003.r0011`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	Protected paths need to cover management links, security-system links, operational data, and facility-control communications, not only model-weight transfer.
Sabotage	Applies with modification	Cable, fiber, and management-path tampering can disrupt or alter AI operations, so protected-path inventories should include integrity and availability consequences.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Weight-transfer and key-management cabling need PDS or equivalent protection when outside controlled perimeters.
Training Systems	Applies with modification	Training introduces high-speed fiber, storage fabrics, and cluster interconnects where literal PDS language may not scale cleanly.

Category	Verdict	Rationale
Inference Systems	Applies with modification	Serving environments need PDS interpretation for model-weight distribution paths and management links.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ic-tech-spec-v151.r1145` (p. 102, para. 1145): 1. Unencrypted communication cables transmitting SCI between accredited SCIFs shall be installed in a Protective Distribution System that complies with standards established…
- `ic-tech-spec-v151.r1146` (p. 102, para. 1146): 2. PDS used to protect SCI shall be approved by the CSA AO.
- `cnssi-7003.r0011` (p. 6, para. 11): 6. PDS are used to protect all unencrypted NSI through areas of lesser classification or control. Inasmuch as the NSI is unencrypted,…

Operations

Run-time controls for occupancy, monitoring, and continuity.

Intrusion detection, failure response, and 24/7 operations Row ID: `pilot-005-intrusion-detection-a`

Source requirements: `ics-705-01.r0036`, `ic-tech-spec-v151.r0799`, `ic-tech-spec-v151.r0800`, `ic-tech-spec-v151.r0842`, `ic-tech-spec-v151.r0875`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	IDS and response procedures must detect unauthorized access to non-weight secret-bearing zones such as operations rooms, security panels, design records, and management infrastructure.

Threat vector	Verdict	Rationale
Sabotage	Applies with modification	IDS failure and degraded monitoring can create sabotage windows against racks, power, cooling, and environmental controls, especially in unmanned 24/7 operations.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	IDS requirements apply strongly, with additional focus on backup media and storage-vault occupancy states.
Training Systems	Applies with modification	Training facilities are often continuously operating, so 'occupied' and IDS-failure procedures need datacenter operations semantics.
Inference Systems	Applies with modification	Serving sites need IDS integration that does not create availability-driven bypasses during incidents or maintenance.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ics-705-01.r0036` (p. 5, para. 36): (1) Intrusion Detection System (IDS) shall detect attempted or actual unauthorized human entry into a SCIF.
- `ic-tech-spec-v151.r0799` (p. 74, para. 799): d) If any component of the IDS is disrupted to the extent the system no longer provides essential monitoring service (e.g., loss…
- `ic-tech-spec-v151.r0800` (p. 74, para. 800): e) IDS failure shall be addressed in the SCIF emergency plan.
- `ic-tech-spec-v151.r0842` (p. 78, para. 842): c) If any component of the IDS is remotely programmable, continuous network monitoring is required. Continuous network monitoring includes auditing and reporting…
- `ic-tech-spec-v151.r0875` (p. 80, para. 875): b) Twenty-four hours of uninterruptible backup power is required and shall be provided by batteries, an uninterruptible power supply (UPS), generators, or…

Access control systems, identity factors, and remote release Row ID: `pilot-006-access-control-syste`

Source requirements: `ics-705-01.r0033`, `ic-tech-spec-v151.r0920`, `ic-tech-spec-v151.r0926`, `ic-tech-spec-v151.r0934`, `ic-tech-spec-v151.r0951`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	Access control must distinguish authorization for model systems from authorization for facility secrets, procedures, BMS panels, security closets, and operational records.
Sabotage	Applies with modification	Physical access to racks, power, cooling, BMS/OT, fiber meet points, and emergency controls must be constrained because those zones can enable disruption or tampering even without weight access.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Strong access control applies directly but must distinguish weight vault, transfer room, and key-management roles.
Training Systems	Applies with modification	Training operations need access control for facilities staff, hardware vendors, liquid-cooling maintenance, and emergency responders.
Inference Systems	Applies with modification	Serving operations need access control that accounts for online incident response, remote hands, and model-update workflows.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ics-705-01.r0033` (p. 4, para. 33): (1) Access to SCIFs is restricted to authorized personnel. Access control methods shall be approved by the AO.
- `ic-tech-spec-v151.r0920` (p. 85, para. 920): b) Personnel access control shall be utilized at all SCIFs.
- `ic-tech-spec-v151.r0926` (p. 85, para. 926): (1) Identification (ID) badge or card used in conjunction with the access control device that validates the identity of the person to…
- `ic-tech-spec-v151.r0934` (p. 86, para. 934): 3. ACSs shall not be used to secure an unoccupied SCIF.
- `ic-tech-spec-v151.r0951` (p. 87, para. 951): 1. CCTV may be used to supplement the monitoring of a SCIF entrance for remote control of the door from within the…

Portable electronics, wireless, recording, and embedded technologies Row ID: `pilot-008-ped-wireless-rcet`

Source requirements: `ics-705-01.r0032`, `ic-tech-spec-v151.r1020`, `ic-tech-spec-v151.r1027`, `ic-tech-spec-v151.r1030`, `ic-tech-spec-v151.r1107`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	Phones, cameras, radios, wearable diagnostics, vendor laptops, and embedded devices can capture non-weight secrets such as procedures, layouts, screens, credentials, and incident activity.
Sabotage	Applies with modification	Unapproved wireless, recording, diagnostic, or embedded devices can introduce remote-control, covert-channel, or tamper paths during operations and incident response.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	PED/RCET restrictions apply to weight-handling rooms, key ceremonies, backup handling, and transfer staging.
Training Systems	Applies with modification	Training facilities need device rules for technicians, vendors, wearable diagnostics, phones, radios, cameras, and wireless tools.
Inference Systems	Applies with modification	Serving sites need the same restrictions, with added attention to incident-response and availability tooling.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ics-705-01.r0032` (p. 4, para. 32): 2. Technical Security Standards for SCIFs a. RF transmitters shall not be introduced into a SCIF unless evaluated and mitigated to be…
- `ic-tech-spec-v151.r1020` (p. 93, para. 1020): 5. Any approval for radio frequency transmitters shall require the AO and the Certified TEMPEST Technical Authority (CTTA) collaborate and approve (as…
- `ic-tech-spec-v151.r1027` (p. 94, para. 1027): c) Mitigation shall be applied to PEDs/RCET evaluated to be high and medium risk to reduce the PED/RCET risk to low before…
- `ic-tech-spec-v151.r1030` (p. 94, para. 1030): 1. Personally-owned PEDs/RCETs are prohibited from processing SCI. Connecting personally-owned PEDs/RCETs to an unclassified IS inside SCIFs may only be done when…
- `ic-tech-spec-v151.r1107` (p. 99, para. 1107): 2. Wireless systems shall meet all TEMPEST and TSCM requirements and shall be weighed against the facilities overall security posture (i.e., facility…

Environmental infrastructure and building management systems Row ID: `pilot-009-environmental-i`

Source requirements: `ic-tech-spec-v151.r1110`, `ic-tech-spec-v151.r1113`, `ic-tech-spec-v151.r1128`, `ic-tech-spec-v151.r1129`

Threat vector	Verdict	Rationale
Weight theft	Gap	Weight-theft analysis keeps storage, training, and inference separate because the same source control can apply differently as model weights move, execute, replicate, or are updated.
Secret theft	Applies with modification	BMS/OT, telemetry, remote maintenance, and environmental logs can reveal operational secrets, workload patterns, facility topology, and security-relevant dependencies.
Sabotage	Gap	AI facilities depend on industrial cooling, power, BMS/OT, and remote-maintenance paths in ways not made explicit by office-like SCIF environmental assumptions; sabotage control language needs expansion.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	Storage environments still rely on HVAC, power, alarms, and maintenance systems that can affect custody and availability.
Training Systems	Gap	Training clusters depend on industrial cooling, power, BMS/OT, telemetry, and remote maintenance far beyond office SCIF assumptions.
Inference Systems	Applies with modification	Serving sites need explicit controls for BMS/OT remote access, telemetry, and maintenance paths.

Falsifier: Change this verdict if a source requirement, established control, or source-checked evidence already covers the AI-specific risk.

Source excerpts:

- `ic-tech-spec-v151.r1110` (p. 100, para. 1110): 1. The FFC shall include information on whether or not environmental infrastructure systems (also referred to as building maintenance systems) are located…
- `ic-tech-spec-v151.r1113` (p. 100, para. 1113): 2. The FFC shall identify all external connections for infrastructure systems that service the SCIF. Examples of the purpose of external connections…
- `ic-tech-spec-v151.r1128` (p. 101, para. 1128): 1. Installation and maintenance of unclassified systems and devices supporting SCIF operations may require physical or remote access. The requirements outlined in…
- `ic-tech-spec-v151.r1129` (p. 101, para. 1129): 2. Installation and maintenance personnel requiring physical access shall possess the appropriate clearance and access, or will be escorted and monitored at…

Lifecycle

Accreditation, de-accreditation, and re-use of secured space.

Re-accreditation after de-accreditation or lower-security control Row ID: `pilot-011-reaccreditation`

Source requirements: `ics-705-01.r0009`, `ics-705-02.r0010`, `ics-705-02.r0011`, `ic-tech-spec-v151.r0014`

Threat vector	Verdict	Rationale
Weight theft	Applies with modification	Weight-theft analysis keeps storage, training, and inference separate because reuse of a formerly accredited area can affect stored assets, active compute, and serving operations differently.
Secret theft	Applies with modification	Re-accreditation records and facility history can reveal or conceal assumptions about drawings, procedures, access paths, and security operations; AI705 should preserve accreditation provenance.
Sabotage	Applies with modification	A lower-control interval can permit physical-plant, cabling, BMS/OT, or maintenance changes that matter for disruption or tamper risk, so re-accreditation must include change and tamper review.

Weight-theft categories:

Category	Verdict	Rationale
Stored Weights	Applies with modification	A reused weight vault, archive room, or transfer-staging space needs documented custody history, sanitization, and change review before relying on prior accreditation.
Training Systems	Applies with modification	Training facilities can change materially while held under a lower posture; re-accreditation needs AI-specific review of racks, power, cooling, fabric, and maintenance paths.
Inference Systems	Applies with modification	Serving sites may be recommissioned quickly, but prior accreditation should not substitute for review of model-serving paths, online operations, logs, and remote support.

Falsifier: Change this verdict if source review, operator evidence, or accreditor review shows the requirement applies without AI-specific adaptation or cannot apply even with adaptation.

Source excerpts:

- `ics-705-01.r0009` (p. 2, para. 9): 2. IC elements shall fully implement this Standard within 180 days of its effective date. a. Facilities under construction or renovation as…
- `ics-705-02.r0010` (p. 2, para. 10): 4. Re-accreditation: a. SCIFs that have waivers issued under previous standards shall be re-accredited using the most current standards. b. All SCIFs…
- `ics-705-02.r0011` (p. 3, para. 11): 5. De-accreditation: a. The de-accreditation of a SCIF is a formal notification to the DNI (via the SCIF Repository) that the facility…
- `ic-tech-spec-v151.r0014` (p. 15, para. 14): 1. SCIFs that have been de-accredited but controlled at the SECRET level (IAW 32 Code of Federal Regulations (CFR) parts 2001 and…

References

Source corpus

[1] ODNI, Intelligence Community Directive 705, Sensitive Compartmented Information Facilities.

[2] ODNI/NCSC, ICS 705-01, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities.

[3] ODNI/NCSC, ICS 705-02, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities.

[4] ODNI/NCSC, IC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, v1.5.1.

[5] CNSS, CNSSI No. 7003, Protected Distribution Systems, September 2015.

Adjacent standards

[6] NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

[7] NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations.

[8] NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023.

[9] UL 2050, National Industrial Security Systems for the Protection of Classified Materials, Fourth Edition.

[10] IEC 62443 series, Industrial communication networks — Network and system security.

Frameworks & tooling

[11] NIST, Open Security Controls Assessment Language (OSCAL).

[12] Security Level 5 Task Force, SL5 Standard for AI Security, https://standard.sl5.org.

Methodology

[13] S. Nevo, D. Lahav, A. Karpur, Y. Bar-On, H. A. Bradley, J. Alstott, Securing AI Model Weights: Preventing Theft and Misuse of Frontier Models, RAND Corporation, RR-A2849-1, May 2024.

Acknowledgments

AI705 depends on review from communities that do not always share a common vocabulary: SCIF and facility-security practitioners, frontier AI infrastructure teams, datacenter operators, colocation providers, accrediting officials, side-channel researchers, OSCAL and compliance-tooling specialists, and policy reviewers. Named acknowledgments will appear once contributors approve public attribution.