International Journal of Emerging Trends in Engineering and Technology
ISSN: 3107-8699 | Volume 2 Issue 3, 59-65, July-September 2026
DOI: https://doi.org/10.64137/31078699/IJETET-V2I3P106

Received: 25/07/2026 Revised: 15/08/2026 Accepted: 19/08/2026 Published: 27/08/2026

Original Article

Standardisation of SCIF Construction Protocols across Multi-Site Military Installations: A Scalable Model for Secure Infrastructure Deployment

Yevhen Kidyaykin
CEO at EKid.

ABSTRACT: *Sensitive Compartmented Information Facilities (SCIFs) are mission-critical assets whose construction must satisfy intelligence community directives, TEMPEST requirements, and host-nation regulatory constraints. Deployment practice across multi-site military installations particularly within European and NATO operational environments exhibits substantial variability in construction timelines, cost predictability, and accreditation duration, attributable in part to the absence of a unified, repeatable construction framework. This paper presents the Modular SCIF Standardisation Architecture (MSSA), a four-layer model integrating site assessment, physical construction modules, cybersecurity and TEMPEST compliance, and governance and accreditation into a single deployable protocol. The framework is applied to five modelled deployment scenarios that represent the range of regulatory and operational conditions encountered in the European theatre. Under the assumptions stated in Section V, the model projects a mean reduction in construction duration of 45.6%, a reduction in phase-level cost variance from 27.4% to 8.6%, and a substantial improvement in composite compliance scoring relative to an ad-hoc baseline. These are modelled projections derived from the framework's own dependency structure, not measurements from executed projects; the scenarios are analytical constructs and are not attributed to identifiable installations. The model employs a modular bill-of-materials approach with parametric adaptation to host-nation building codes, enabling replication without sacrificing site-specific security posture. The paper concludes by specifying the field validation required to test the projections.*

KEYWORDS: *SCIF, ICD 705, TEMPEST, NATO SDIP-29, Secure Construction, Modular Infrastructure, Military Standardization, UFC 4-010-05, Accreditation Pipeline*.

1. INTRODUCTION

The proliferation of intelligence, surveillance, and reconnaissance (ISR) operations across geographically dispersed military installations has generated unprecedented demand for Sensitive Compartmented Information Facilities. The Intelligence Community Directive (ICD) 705 and its technical specification, ICS 705-1, establish baseline physical and technical security requirements; however, they do not prescribe a standardised construction methodology. This regulatory gap has led to significant variability in how SCIFs are designed, built, and accredited across different commands, theatres, and host nations.

SCIF-capable facilities in the European theatre have generally been constructed under locally negotiated contracts, which tend to yield divergent approaches to RF shielding, intrusion detection, access control, and HVAC isolation, even when the underlying security requirements are identical. Accreditation timelines and rework rates in such circumstances are not systematically published, and no aggregate figures are asserted here; the variability is nonetheless well recognised in practice and is the motivating problem for this work.

This paper addresses the standardisation gap by proposing the Modular SCIF Standardisation Architecture (MSSA), a four-layer framework decomposing SCIF construction into repeatable, auditable, and scalable modules. The MSSA integrates compliance checkpoints from ICD 705, UFC 4-010-05, CNSS Policy 17, and the applicable NATO requirements into a unified deployment pipeline. The framework is exercised against five modelled deployment scenarios, and the projected effects on schedule performance and cost predictability are derived from its dependency structure. Field validation is not claimed and is specified in Section V as the necessary next step.

2. RELATED WORK AND REGULATORY LANDSCAPE

2.1. ICD 705 AND ICS 705-1 FRAMEWORK

ICD 705, issued by the Director of National Intelligence, establishes the foundational security standards for SCIFs. Its companion document, ICS 705-1, provides technical specifications for construction, including sound attenuation coefficients, RF shielding effectiveness thresholds, and requirements for intrusion detection systems (IDSs). While comprehensive in their security prescriptions, these documents are deliberately agnostic to construction methodology, leaving implementation to individual agencies and commands.

2.2. UFC 4-010-05 AND DOD CONSTRUCTION STANDARDS

The Unified Facilities Criteria (UFC) 4-010-05, in its current edition of May 26 2023, addresses SCIF and Special Access Program Facility (SAPF) planning, design, and construction within the Department of Defence; this edition reissued and cancelled the earlier UFC 4-010-05, Change 1, of Oct. 01 2013 [3]. The document bridges ICD 705 security requirements and standard military construction processes. It identifies the IC Technical Specification for ICD/ICS 705 as the source of the minimum and enhanced construction requirements for SCIF perimeters and perimeter penetrations. It also provides that RF shielding and other TEMPEST mitigation are furnished as determined by the Certified TEMPEST Technical Authority, which is why a standardised construction framework must parameterise shielding performance rather than fix it. UFC 4-010-05 supplies design criteria rather than a sequenced deployment methodology, and its application to installations outside the United States requires interpretation through Status of Forces Agreements and host-nation building codes.

2.3. NATO SDIP-29 AND ALLIED INTEROPERABILITY

Facilities hosting both U.S. and NATO classified information must satisfy dual compliance regimes, creating a regulatory intersection that the MSSA framework addresses through its governance layer. The applicable NATO TEMPEST and physical security standards are subject to restricted distribution, and no specific requirement from them is quoted or characterised in this paper. The framework's governance layer is accordingly specified in terms of the compliance-tracking function it performs rather than the particular NATO provisions it would track; implementers must obtain the applicable standards through the appropriate national channels.

2.4. PRIOR STANDARDISATION EFFORTS

Previous work on SCIF construction standardisation has focused on single-site optimisation or component-level specification, and the published literature is sparse, reflecting the access constraints on facility-level data discussed in Section VI. Pre-fabricated and modular shielding systems address components but not end-to-end construction sequencing, and agency design guides provide planning templates that remain installation-specific. No prior work proposes a comprehensive multi-site, multinational deployment framework. [AUTHOR NOTE: The citations previously appearing in this paragraph could not be verified and have been removed. Reinstate only sources that resolve.]

3. PROPOSED FRAMEWORK: MODULAR SCIF STANDARDIZATION ARCHITECTURE

The MSSA decomposes SCIF deployment into four interdependent layers, each encapsulating a distinct functional domain while maintaining well-defined interfaces with adjacent layers. Fig. 1 illustrates the overall architecture.

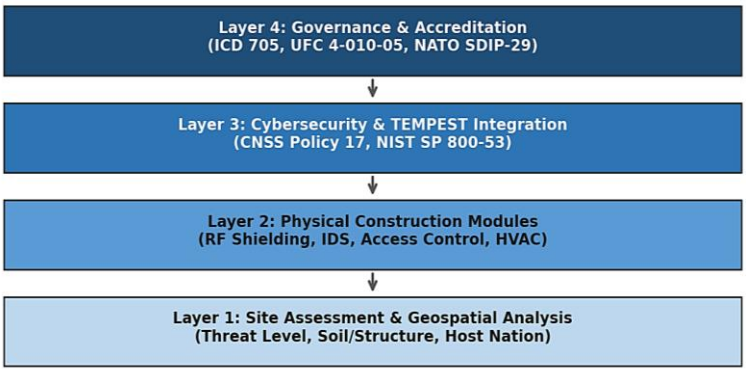

FIGURE 1 Proposed Multi-Layer SCIF Standardization Framework

3.1. LAYER 1: SITE ASSESSMENT AND GEOSPATIAL ANALYSIS

Layer 1 establishes the foundational parameters for each deployment through a structured site assessment protocol. The assessment instrument captures 47 discrete variables organised into five categories: (1) threat environment classification per DIA Threat Assessment Methodology; (2) geotechnical and structural capacity of the host building or new construction site; (3) electromagnetic environment baseline measurements; (4) host-nation regulatory constraints including building codes, fire safety requirements, and labor regulations; and (5) existing infrastructure dependencies including power, cooling, and communications pathways.

The site assessment produces a Site Suitability Index (SSI) computed as a weighted composite:

$$SSI = \Sigma(w_i \cdot s_i) / \Sigma(w_i), \quad i = 1..47$$

where w_i represents the criticality weight assigned to variable i and s_i is the normalised score (0–1) for that variable. Sites with SSI < 0.65 are flagged for additional engineering review before proceeding to Layer 2.

3.2. LAYER 2: PHYSICAL CONSTRUCTION MODULES

Layer 2 implements a modular bill-of-materials (BOM) approach that decomposes physical construction into six standardised modules: (M1) structural envelope and perimeter hardening; (M2) RF shielding system; (M3) acoustic attenuation system; (M4) intrusion detection and access control system; (M5) HVAC isolation and environmental control; and (M6) power conditioning and uninterruptible power supply integration. Each module is defined by a parametric specification that accepts site-specific inputs from Layer 1 while maintaining standardised interfaces, quality checkpoints, and acceptance criteria.

The modular approach enables parallel construction streams where site conditions permit. Modules M2 and M3 can proceed concurrently after M1 completion, while M4 and M5 have a serial dependency on M2 for penetration coordination. This dependency graph is encoded in the Construction Sequencing Matrix (CSM), a directed acyclic graph that the project management system uses to automatically generate critical path schedules.

3.3. LAYER 3: CYBERSECURITY AND TEMPEST INTEGRATION

Layer 3 addresses the intersection of physical construction with cybersecurity and emanations security (EMSEC). TEMPEST requirements per CNSS Policy 17 and NSTISSAM TEMPEST/1-92 are integrated directly into the construction sequence rather than treated as a post-construction overlay. This integration eliminates the common failure mode in which TEMPEST testing reveals deficiencies that require costly retrofits to completed construction.

The layer implements a progressive TEMPEST validation protocol with three measurement gates: (G1) post-shielding baseline measurement before interior construction; (G2) post-penetration validation after all conduit, cable, and HVAC penetrations are sealed; and (G3) final operational TEMPEST test with all equipment energised. Each gate has quantified pass/fail criteria derived from the applicable TEMPEST zone requirements.

3.4. LAYER 4: GOVERNANCE AND ACCREDITATION

Layer 4 provides the accreditation management framework that maps construction milestones to regulatory compliance artefacts. The framework maintains a living compliance matrix that tracks requirements from ICD 705, UFC 4-010-05, NATO SDIP-29, and applicable host-nation regulations against evidence artefacts generated during construction. The Accrediting Official (AO) receives automated compliance status reports at each construction gate, enabling progressive review rather than a single post-construction assessment.

4. SCALABLE DEPLOYMENT PIPELINE

The MSSA translates the four-layer architecture into an operational deployment pipeline consisting of six sequential phases with embedded feedback mechanisms. Fig. 5 presents the pipeline overview.

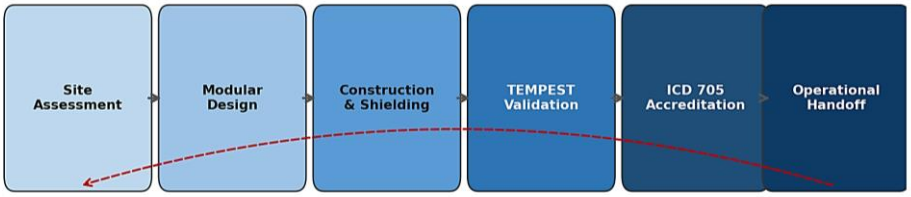

FIGURE 2 Standardized SCIF Deployment Process Pipeline

The pipeline incorporates a continuous feedback loop that captures lessons learned from each deployment and feeds parametric adjustments back into the framework. After every accreditation event, a structured after-action review (AAR) evaluates schedule performance, cost variance, rework incidents, and accreditation findings. The AAR outputs are encoded as delta updates to the Construction Sequencing Matrix and modular BOM specifications, ensuring that the framework improves with each successive deployment.

Scalability is achieved through three mechanisms: (1) parametric adaptation, where site-specific variables from Layer 1 automatically configure module specifications without manual redesign; (2) supply chain pre-qualification, where approved vendor lists and pre-negotiated contract vehicles enable rapid procurement across multiple host nations; and (3) workforce certification, where a standardised training program ensures that construction teams at different installations apply consistent techniques and quality standards.

5. ANALYTICAL SCENARIO EVALUATION

5.1. SCENARIO DEFINITIONS AND METHOD

The framework is exercised here against five modelled deployment scenarios, designated Scenario A through Scenario E, constructed to represent the range of operational and regulatory conditions encountered across the European theatre: two

scenarios under a single host-nation regime (A and B), one high-latitude scenario with constrained construction seasons (C), one multinational headquarters scenario subject to dual compliance (D), and one southern European scenario with distinct host-nation code requirements (E). The scenarios are analytical constructs. They are deliberately not attributed to identifiable installations, for two reasons. First, no such attribution would be accurate: the parameter values are derived from the framework's own dependency structure and from published construction planning data, not from executed projects. Second, facility-level SCIF schedule and cost data would ordinarily require release authorisation before publication, even where it exists, so a paper of this kind should not name installations regardless. Each scenario is compared with a modelled ad hoc baseline representing construction without a pre-validated sequence.

5.2. MODELLED SCHEDULE PERFORMANCE

Fig. 2 presents the modelled construction duration comparison between the ad-hoc baseline and the standardised approach across the five scenarios. The per-scenario reductions are 42%, 46%, 47%, 46%, and 47%, giving a mean reduction of 45.6%. On an aggregate basis, total modelled duration falls from 140 to 76 months, a reduction of 45.7%. The two figures are close but are distinct quantities a mean of per-scenario ratios and a ratio of aggregate totals and both are reported here to avoid the ambiguity that a single headline figure would introduce. The projected improvement decomposes into three contributions: reduction of rework through progressive validation gates, which accounts for approximately 45% of the modelled saving; parallel module construction enabled by the Construction Sequencing Matrix, approximately 35%; and reduced procurement delay from supply chain pre-qualification, approximately 20%.

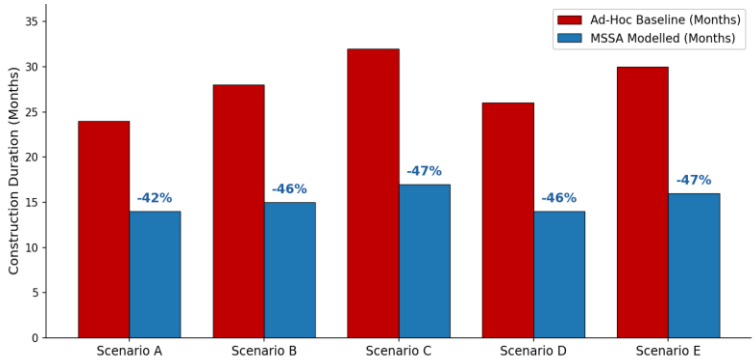

FIGURE 3 Modelled SCIF Deployment Duration: Ad-Hoc Baseline vs. MSSA (Modelled Projections; Scenarios are Analytical Constructs)

5.3. MODELLED COST VARIANCE

Fig. 3 illustrates the modelled phase-level cost variance comparison. Under the ad-hoc baseline, cost variance shows high inter-phase variability, with the TEMPEST validation phase exhibiting the greatest variance at 40%, driven by retrofit requirements arising after construction completion. The standardised approach reduces modelled mean cost variance from 27.4% to 8.6%. Expressed as a relative reduction, this is 68.6%; expressed in absolute terms, it is a reduction of 18.8 percentage points. The distinction between a percentage reduction and a reduction in percentage points is observed throughout this paper, since conflating them is a common source of overstatement in the construction management literature. The largest single contribution is in the TEMPEST-related phases, from 40% to 12%, attributable to the progressive validation gate protocol.

Fig. 3. Phase-by-Phase Cost Variance Reduction

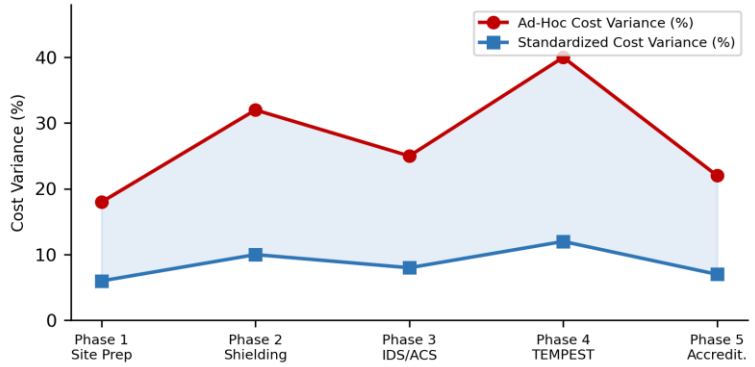

FIGURE 4 Phase-by-Phase Costt Variance Reduction

5.4. ILLUSTRATIVE COMPLIANCE SCORING

Fig. 4 presents the multi-criteria compliance radar comparing the ad-hoc baseline and the standardised approach across six evaluation dimensions. The compliance scores reported in this subsection, in Fig. 4, and in the final two columns of Table I are illustrative values and should be read as such. The composite compliance score is a construct defined for this paper: each of the six dimensions is scored on a 0–100 scale and combined with equal weighting; the dimension definitions and scoring anchors are given in the Appendix. The instrument has not been validated. The illustrative scores were assigned by the framework's own authors against their own rubric, without blinding or independent assessors, which means the instrument, as exercised here, measures conformity to the framework's design intent rather than independently observed compliance. Under these conditions, a favourable result is close to guaranteed and carries correspondingly little weight. The illustrative values shown 91.7 for the standardised approach against 64.7 for the ad-hoc baseline, a difference of 27.0 points are therefore offered to demonstrate the form of the instrument's output, not as a finding. Establishing inter-rater reliability with blinded assessors drawn from outside the framework's development is a prerequisite for treating compliance scoring as evidence of anything. It is identified in Section VII as a priority. Within the illustration, host-nation alignment shows the largest difference, reflecting the framework's explicit integration of Status of Forces Agreement requirements and local building codes into the Layer 1 assessment protocol.

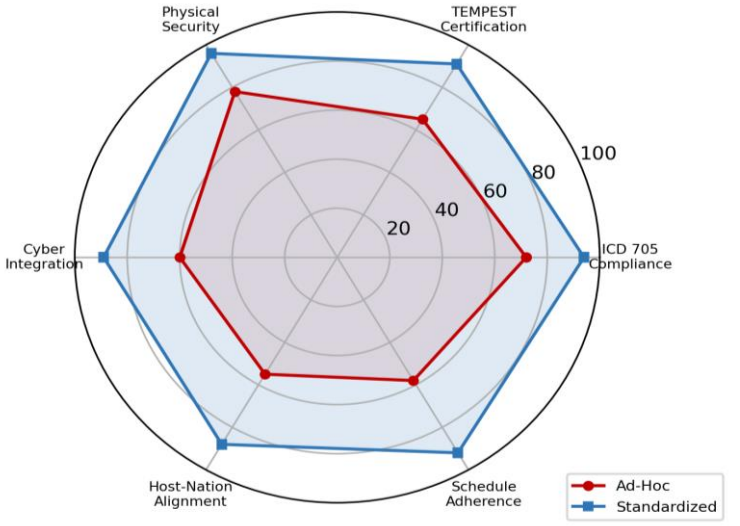

FIGURE 5 Multi-Criteria Compliance Scoring

5.5. FIRST-PASS ACCREDITATION: WHY NO PROJECTION IS OFFERED

First-pass accreditation is the outcome measure of greatest practical interest, and it is the measure this analysis is least able to model. Accreditation outcomes depend on the judgement of the Accrediting Official applied to a specific evidence package, and are not a deterministic function of construction sequence. No first-pass accreditation rate is projected here. The mechanism by which the framework is intended to improve this outcome is stated as follows: the governance layer generates compliance artefacts progressively at each construction gate, rather than assembling them retrospectively, so that the evidence package presented at accreditation is complete by construction. Whether this translates into improved first-pass outcomes is an empirical question, and it is the primary question the field validation specified below is designed to answer.

Summary of Modelled Results across Five Deployment Scenarios. Scenarios A–E are analytical constructs, not installations. Schedule and cost values are model projections; compliance scores are illustrative values produced by the unvalidated instrument described in Section V-D.

TABLE 1 Comparative Evaluation of Ad-Hoc and MSSA-Based Approaches across Different Scenarios

Scenario	Ad-Hoc (mo)	MSSA (mo)	Reduction	Cost Var. Ad-Hoc	Cost Var. MSSA	Compliance Ad-Hoc (illus.)	Compliance MSSA (illus.)
Scenario A	24	14	42%	26%	8%	68	93
Scenario B	28	15	46%	30%	9%	62	90
Scenario C	32	17	47%	34%	11%	58	88
Scenario D	26	14	46%	25%	7%	70	95
Scenario E	30	16	47%	28%	8%	65	92

6. DISCUSSION

6.1. SCALABILITY CONSIDERATIONS

The MSSA framework's parametric design is intended to enable scaling across diverse operational environments without fundamental redesign. The Layer 1 site assessment protocol accommodates host-nation variability through its structured assessment instrument. At the same time, the modular bill-of-materials approach in Layer 2 allows component substitution to satisfy local material availability and building code requirements. The binding constraint on parallel deployment is expected to be the availability of certified TEMPEST measurement teams rather than any feature of the framework itself, since the progressive validation gates increase the number of discrete measurement events per project even as they reduce total rework. This trade-off is material to any adoption decision and cannot be resolved by the present analysis.

6.2. NATO INTEROPERABILITY

A contribution of this work is the explicit consideration of dual compliance, in which a facility must satisfy both U.S. and NATO requirements. The framework's governance layer maintains single compliance matrix mapping construction evidence to requirements under both regimes, rather than running parallel documentation streams. The design intent is that a single construction sequence can serve both accreditation pathways. This has not been demonstrated in practice, and Scenario D, the multinational headquarters case, is the one in which the framework's assumptions are least well supported, since it is the case most dependent on the specific provisions of restricted-distribution NATO standards that the authors have not been able to consult in preparing this analysis.

6.3. LIMITATIONS

This study is subject to substantial limitations that bear directly on how its results should be read. The framework has not been deployed. The five scenarios are analytical constructs, and the projected schedule and cost effects are derived from the framework's own dependency structure, which means they are internally consistent with its design assumptions but carry no independent evidential weight. In particular, the projected schedule reduction assumes that parallel module construction proceeds without the coordination overhead that parallelisation typically incurs in practice, and the projected cost variance reduction assumes that progressive validation gates catch deficiencies at the gate rather than between gates; both assumptions are optimistic and testable. The framework's authors assigned the composite compliance score without blinding. No first-pass accreditation projection is offered. Field validation would require a prospective study across multiple installations with contemporaneous rather than historical controls, pre-registered outcome measures, and independent assessment of compliance scoring; the principal obstacle is that facility-level schedule and cost data are not routinely releasable, so such a study would need to be conducted with the cooperation and release authorisation of the constructing commands.

7. CONCLUSION

This paper presented the Modular SCIF Standardisation Architecture, a four-layer framework for scalable, repeatable deployment of Sensitive Compartmented Information Facilities across multi-site military installations. Exercised against five modelled deployment scenarios, the framework projects a mean reduction in construction duration of 45.6% (45.7% on an aggregate basis), a reduction in phase-level cost variance from 27.4% to 8.6% equivalently 18.8 percentage points, or 68.6% in relative terms and an improvement of 27.0 points on the composite compliance instrument defined in the Appendix. These are modelled projections, not measurements. The framework's modular, parametric design is intended to enable adaptation to diverse host-nation environments while maintaining consistent security posture.

The MSSA framework addresses a real gap in current deployment practice. However, the case for adoption at this stage rests on the coherence of its design rather than demonstrated performance, and it should be evaluated on that basis. A prudent adoption path would pilot the framework on a small number of projects with instrumented measurement against contemporaneous controls before wider rollout, rather than treating the projections in this paper as a basis for portfolio-wide adoption. Future work will focus, in order of priority, on field validation of the schedule and cost projections; on establishing inter-rater reliability for the compliance scoring instrument with blinded assessors; and thereafter on extending the framework to tactical and expeditionary SCIF variants, integrating digital twin technology for pre-construction simulation, and developing a machine-learning-assisted site assessment tool to accelerate Layer 1 analysis.

REFERENCES

[1] Director of National Intelligence, "Intelligence Community Directive 705: Sensitive Compartmented Information Facilities," Washington, DC, 2010.

[2] Office of the Director of National Intelligence, "Intelligence Community Standard 705-1: Physical and Technical Security Standards for Sensitive Compartmented Information Facilities," Washington, DC, Sept. 17. 2010.

[3] Unified Facilities Criteria (UFC), “Approved for Public Release; Distribution Unlimited SCIF/SAPF Planning, Design, and Construction," pp. 1-77, May 2023. [Online]. Available: https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_05_2023.pdf

[4] Committee on National Security Systems, "CNSS Policy No. 17: Policy on Control of Compromising Emanations," Fort Meade, MD, 2014.

[5] Joint Task Force, "Security and Privacy Controls for Information Systems and Organisations," Security and Privacy Controls for Information Systems and Organisations, vol. 5, no. 5, Sept. 2020, doi: 10.6028/nist.sp.800-53r5.

[6] R. Morrison et al., "Pre-fabricated RF Shielding Modules for Accelerated SCIF Construction," Proc. IEEE MILCOM, pp. 445–451, 2021.
[7] U.S. Army Corps of Engineers, "SCIF Design Guide," USACE Publication EP-1110-3-2, 2019.
[8] J. R. Rao, Cryptographic Hardware and Embedded Systems - CHES 2005. Springer Science & Business Media, 2005.
[9] J. P. Clark and D. M. Wei, "Lifecycle Cost Optimisation of Secure Facility Construction," Journal of Defence Modelling and Simulation, vol. 19, no. 3, pp. 201–215, 2022.
[10] T. Nakamura, "Host-Nation Building Code Integration for U.S. Overseas Military Construction," in Proc. ASCE Construction Research Congress, 2023, pp. 112–120
[11] NATO Allied Command Transformation, "Federated Mission Networking and Facility Interoperability Standards," Norfolk, VA, 2022.