

Securing the Distributed Classified Mission

Commercial Solutions for Classified (CSfC)

- CSfC and Type 1 Encryption ·
- CSfC Mobile ·
- CSfC Tactical
- Adding Cross Domain Solution(s)

Prepared for
The U.S. Department of Energy (DOE)
Robert Link – CSfC Chief Technologist

October 2026

OSC EdgeTechSolutions, LLC Unclassified // Proprietary // Use or disclosure
of data contained on this sheet is subject to restrictions.

For Additional Information, Please contact:



Lisa Dials

Senior Director, Business Development

lisa.dials@osc-global.com

(240) 444-4679



© 2026 OSC EdgeTechSolutions – A CIRI Company. All Rights Reserved

Using CSfC to Solve Complex Problems

01

Extend the Mission Beyond Fixed Infrastructure

Use CSfC to securely extend classified connectivity to mobile users, remote locations, tactical environments, and new facilities without replicating traditional classified infrastructure everywhere the mission operates.

02

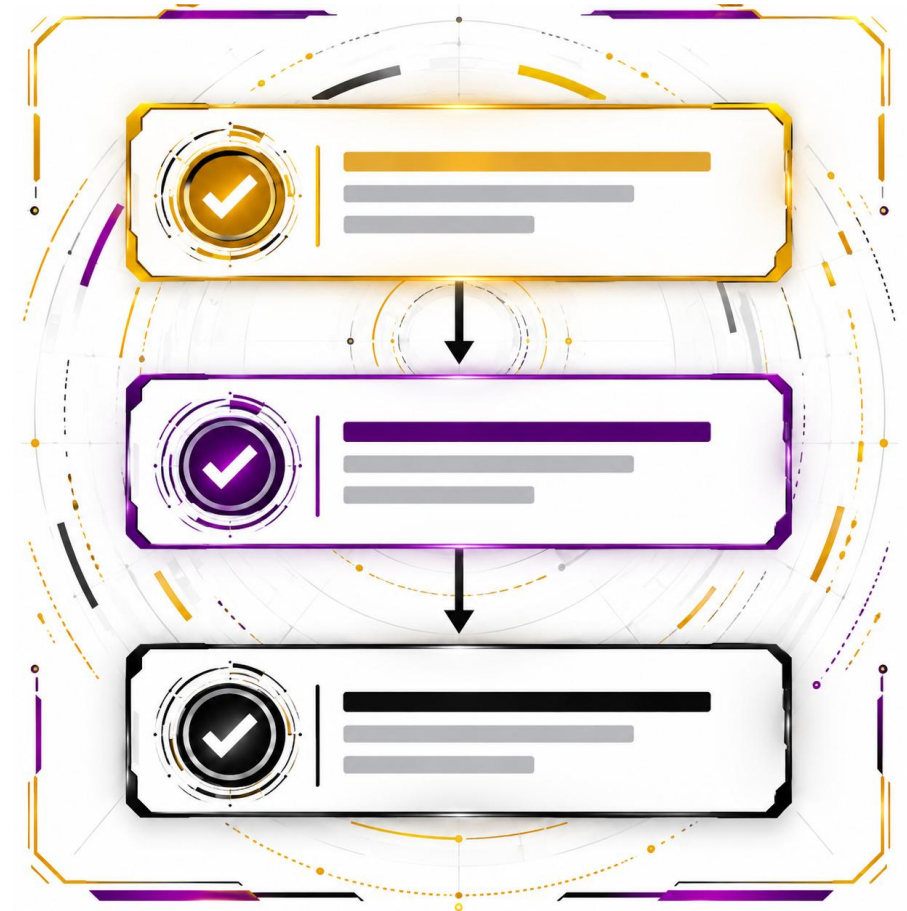
Integrate Existing and Emerging Technologies

Combine CSfC with existing Type 1 transport, VDI, cloud, tactical compute, wireless, and Cross Domain capabilities to create a unified architecture rather than solving each requirement with a separate system.

03

Simplify Without Sacrificing Security

Reduce dedicated devices, circuits, Data-at-Rest exposure, and infrastructure while introducing layered encryption, centralized management, continuous monitoring, and policy-enforced access across the environment.



Where DOE classified work actually happens

National laboratories, production sites, and field offices distributed across the country

Mission personnel increasingly need secure access to classified information and applications across geographically dispersed facilities, rather than relying solely on centralized classified environments.

- **Emergency and radiological response teams deploying wherever the mission requires** Response personnel may be sent with little notice to locations where dedicated classified infrastructure does not exist, creating an immediate requirement for secure, rapidly deployable access and reach-back capabilities.
- **Secure transport operations that are classified and mobile by definition.** These missions operate continuously between fixed locations, requiring classified connectivity that can move with personnel and operations instead of depending on access to a traditional secure facility.
- **Incident command posts established in hours, not months.** During emergencies and contingency operations, temporary command environments must become operational quickly. Classified communications and access need to deploy at the same operational tempo without waiting for permanent infrastructure.
- **Inter-site programs with teams and collaborators located across multiple states** Programs increasingly depend on personnel, laboratories, and mission partners working together from geographically separated locations, creating a need for secure access that enables collaboration without requiring everyone to operate from the same classified facility.



Today's mission is distributed and mobile, yet classified access remains concentrated within traditional secure environments.

Three gaps — everything after this maps back here

1 Access is tethered

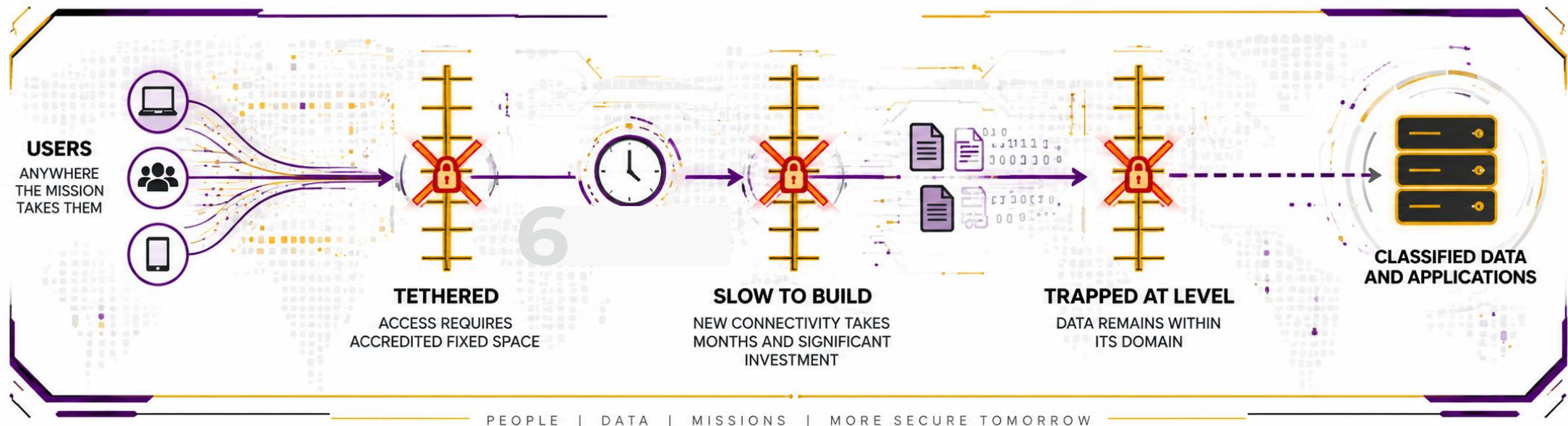
Classified work requires accredited fixed space. When the mission leaves the building, the classified capability does not go with it.

2 Build is slow and capital intensive

Standing up new classified connectivity is measured in quarters and infrastructure can be costly, which pushes programs toward workarounds.

3 Data is trapped at level

Once information is in a domain it stays there. This is the constraint mission owners actually complain about.

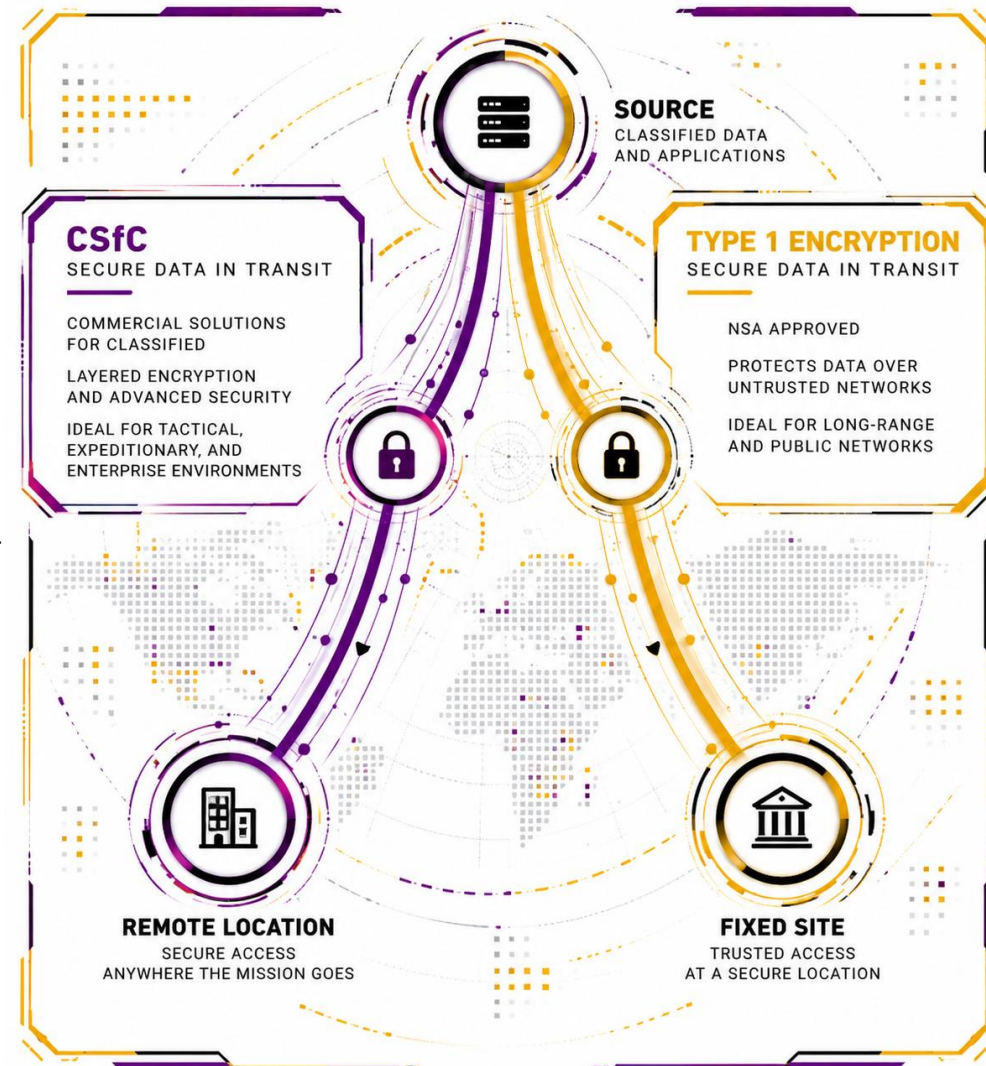


Gaps 1 and 2 are primarily connectivity challenges that can be addressed through the appropriate encryption architecture. Gap 3 presents a fundamentally different challenge—securely accessing or moving information across security domains—which requires a dedicated Cross Domain Solution (CDS)

Different Architectures. Same Mission: Secure Classified Data in Transit

- **Type 1 Encryption:** Uses government-certified, high-assurance cryptographic equipment to protect classified information, relying on controlled keying material and a tightly managed NSA-defined lifecycle.
- **Commercial Solutions for Classified (CSfC):** Uses two independent layers of NIAP-validated commercial security products, integrated in accordance with an NSA-published Capability Package and operated as an NSA-registered solution.
- **Two Approved Approaches:** Both Type 1 and CSfC provide sanctioned methods for protecting classified information across National Security Systems, but they achieve that protection through fundamentally different architectures.
- **Different Operational Models:** Each approach carries a different security and risk model, acquisition and sustainment cost structure, deployment model, and allocation of responsibility for managing and accepting residual risk.

There is no one-size-fits-all answer—the mission, environment, and risk determine the right approach.



Type 1 / HAIPE — what TACLANE gives you today

- **High-Assurance Protection:** Provides a single, government-certified encryption layer designed to protect classified information at **Top Secret/SCI and below**, delivering a well-established approach for securing data in transit.
- **Broad TACLANE Portfolio:** Current options include the **TACLANE-FLEX (KG-175F)**, **TACLANE-10G (KG-175X)**, **TACLANE-Micro (KG-175D)**, **TACLANE-1G (KG-175G)**, and **TACLANE-Nano (KG-175N)**, providing platforms sized for different performance, deployment, and mission requirements.
- **Modernized Key Management:** The **TACLANE-FLEX** and **TACLANE-10G** support Advanced Cryptographic Capabilities and **KMI over-the-network keying**, helping streamline key distribution and reduce the operational effort associated with traditional keying workflows.
- **Operational Strengths:** Type 1 solutions provide **high throughput, mature technology, established operating procedures, and a familiar accreditation model**, making them a proven option for organizations already operating within traditional classified environments.
- **Operational Burden:** Type 1 encryption also introduces requirements for **classified keying material, COMSEC accountability, secure storage and handling, specialized support processes, and externally driven technology refresh cycles** that must be incorporated into the program's lifecycle and sustainment planning.



One high-assurance layer, end to end

CSfC — Commercial Technology. Layered Protection. Mission Ready.

Layered Commercial Encryption: CSfC uses **two independent encryption layers**, built from products on the NSA CSfC Components List and validated against applicable NIAP Protection Profiles, to provide defense-in-depth for classified information.

- **Capability Package Architecture:** Components are integrated in accordance with an applicable **NSA-published Capability Package (CP)**, with the completed solution registered with NSA before entering operational use.
- **Defined Security Boundaries:** The architecture maintains distinct **Red, Gray, and Black security boundaries**, with Gray infrastructure supporting critical security and management functions such as administration, firewalls, SIEM, and IDS/IPS between the inner and outer encryption layers.
- **Continuous Compliance:** CSfC solutions must remain aligned with the applicable Capability Package and are **revalidated against the most recently published CP requirements**, helping ensure the architecture continues to meet current NSA security expectations.

CURRENT CAPABILITY PACKAGES

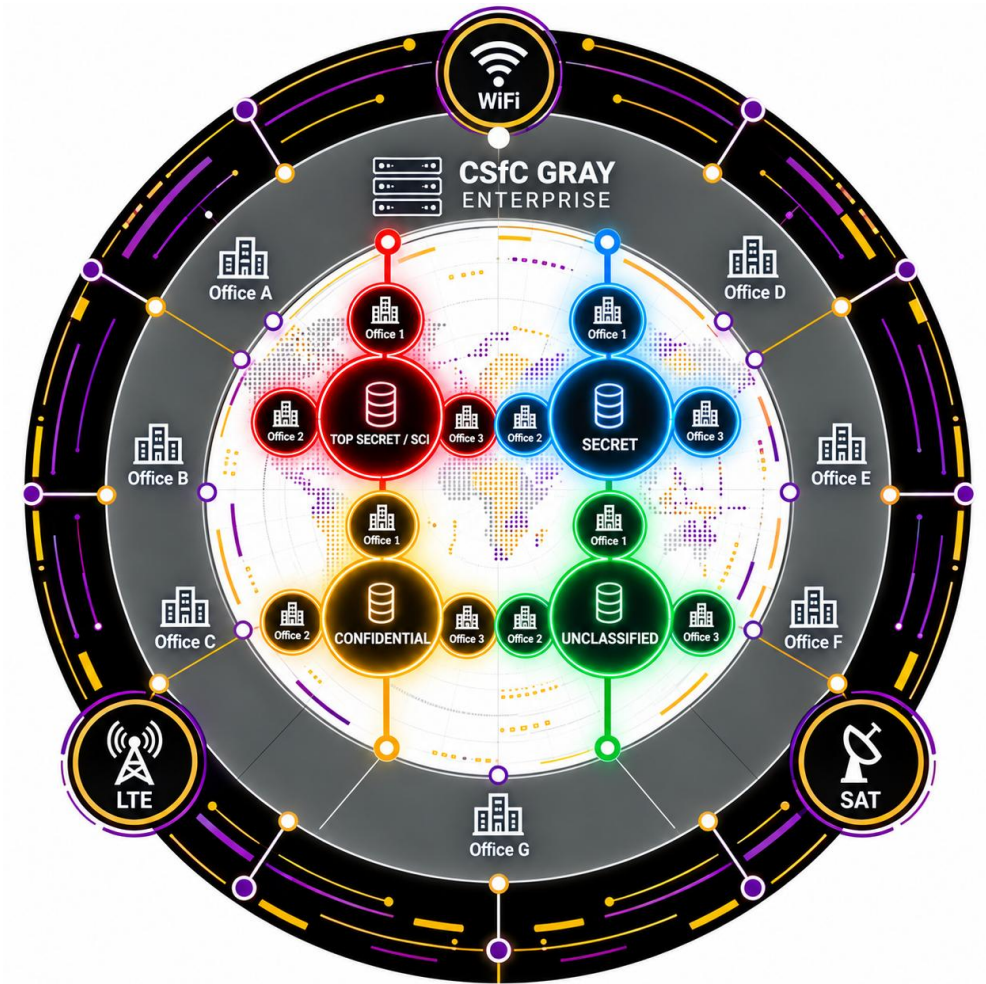
Mobile Access — v2.8.0

Multi-Site Connectivity — v1.3.0

Tactical — v1.0.0

Campus WLAN — v3.2.0

Data-at-Rest — v5.1.0



Outer ring: Black Transport · Middle: GRAY Transport · Inner:
Various Classifications as needed

The Capability Packages are pieces, not products



The greatest design challenges occur where the pieces come together—overlapping boundaries, duplicated Gray services, and inconsistent key management can introduce complexity and risk across the entire solution.

1 One problem, several packages

CSfC is an integrated architecture, not a single Capability Package. Most operational deployments combine multiple CPs to meet the full mission requirement.

2 Annexes bind the pieces

The annexes provide the common security framework that connects individual Capability Packages—standardizing key management, Enterprise Gray services, and continuous monitoring across the architecture.

3 The registered solution is the assembly

The individual components are the building blocks, but the assembled architecture is the registered CSfC solution. Every layer must work together as one cohesive security design.

Head-to-head — the dimensions that decide it

	Type 1 (TACLANE)	CSfC (layered COTS)
Assurance basis	One government-certified hardware layer	Two independent commercial layers
Approval path	NSA certification and COMSEC accreditation	CP compliance plus NSA solution registration
Keying	Classified keying material; KMI over-the-network keying	Commercial PKI per the CP; no classified key to hold
Lifecycle burden	COMSEC custodian, controlled storage, accountability	Trusted integrator, two stacks to patch, annual revalidation
Deployment speed	Paced by procurement and certification cycles	Paced by commercial refresh; far shorter
Throughput ceiling	Up to 10 Gb/s on the KG-175X	Bounded by commercial gateway and device capacity
Mobile and edge fit	Limited; the Nano narrows but does not close the gap	Purpose-built through the Mobile Access CP
Who owns the risk	Certification underwrites the device itself	Your Authorizing Official owns the solution

No column is colour-coded as the winner. A matrix with a green column reads as a sales pitch — and this room will treat the whole brief accordingly.

Where each approach wins

1 Fixed, High-Throughput Backbone — Type 1

For established site-to-site connections with predictable requirements, dedicated infrastructure, and sustained high-throughput transport, **Type 1 encryption remains a strong fit**. It provides a mature, purpose-built approach for protecting the WAN backbone while allowing CSfC to be layered above that transport where additional flexibility is required.

2 Rapid Site Expansion — CSfC

When standing up a new location or extending classified connectivity to additional facilities, **CSfC provides greater architectural flexibility** through commercial components and the Multi-Site Connectivity Capability Package. This can reduce dependence on deploying dedicated Type 1 infrastructure to every new network edge. NSA notes that MSC can support multiple sites and security levels depending on mission requirements.

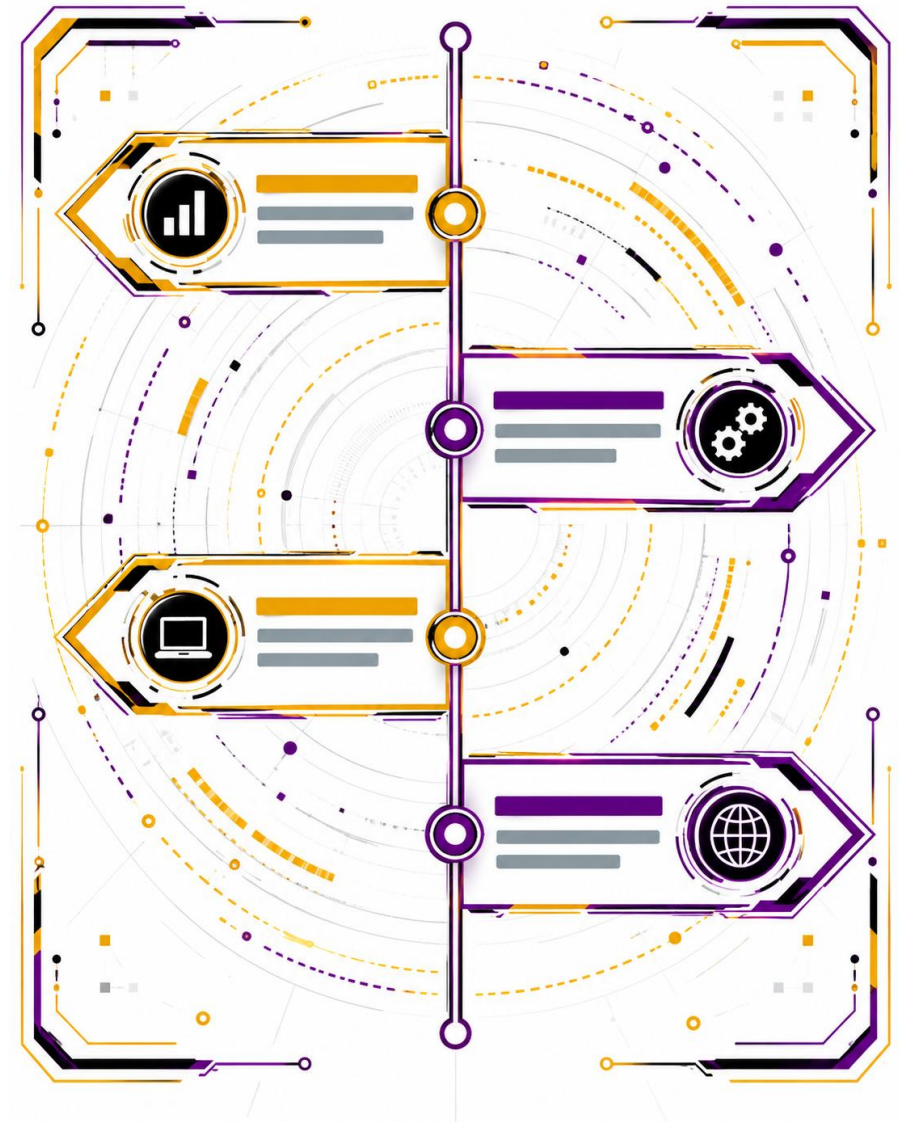
3 Mobile, Temporary & Expeditionary Operations — CSfC

For users and missions that move, **CSfC is specifically designed to extend classified connectivity beyond traditional fixed infrastructure**. NSA's Mobile Access architecture supports classified data over wired, domestic cellular, and trusted wireless networks, and CSfC also includes provisions for tactical environments.

4 Controlled, Austere & Contested Environments — Mission Dependent

Outside traditional U.S.-controlled infrastructure—or where RF, physical security, connectivity, and operational conditions introduce additional risk—the answer becomes **mission and threat dependent**. Type 1 may remain appropriate for high-assurance transport, while CSfC can provide layered commercial encryption and tactical/mobile flexibility. The AO, mission requirements, applicable Capability Package, threat environment, and residual risk should drive the architecture rather than forcing either technology into every scenario.

NOTE: For #1 Currently if you need more than 100Gb/sec then CSfC is the winner

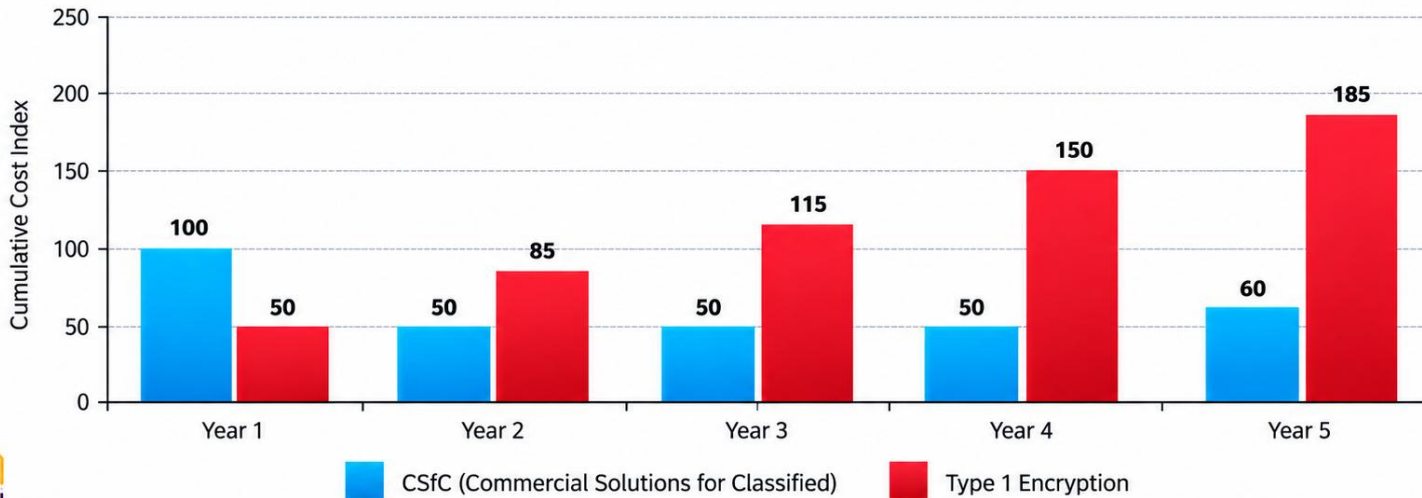


Lifecycle cost — CSfC moves the money

Lifecycle Cost Comparison

CSfC vs. Type 1 Encryption

(Illustrative cumulative costs – index, not an estimate)



Lower initial cost. Comparable long-term investment. Both deliver mission-ready security.

1 Type 1 Encryption Hardware & Sustainment:

Higher upfront costs are driven by specialized encryption hardware, COMSEC infrastructure, keying requirements, and deployment support, with recurring lifecycle costs for maintenance, hardware refresh, licensing, and COMSEC operations.

2 CSfC Integration & Flexibility:

Upfront costs are primarily driven by engineering, integration, documentation, validation, and registration, while long-term costs can benefit from commercial hardware, software-based upgrades, centralized management, and more flexible technology refresh cycles.

Type 1 / HAIPE — what TACLANE gives you today

- **Classified Access Anywhere:** Enables secure **classified voice, video, and data** from commercial end-user devices across commercial cellular, Wi-Fi, and other supported transport networks.
- **Mobile Access Architecture:** Built in accordance with the **NSA CSfC Mobile Access Capability Package**, providing a standardized architecture for extending classified connectivity beyond traditional fixed facilities.
- **Layered Security:** Maintains clearly defined **Red, Gray, and Black security boundaries**, with Gray infrastructure providing management and security services between the outer VPN gateway and inner encryption layer.
- **Protection Beyond Transit:** Pair CSfC Mobile with **Data-at-Rest (DAR)** protections to secure classified information stored on the endpoint if a device is lost, stolen, or compromised—or integrate a **Cross Domain Solution (CDS) access architecture** that keeps classified data within the protected enterprise environment, with **no classified data stored on the endpoint or transmitted outside the authorized secure session**.
- **Registered & Maintained:** The complete solution is **registered with NSA** and maintained through ongoing compliance, monitoring, and revalidation against applicable CSfC requirements as they evolve.

Extending classified access to where the mission happens—without compromising policy or security.



Four DOE missions that change on day one



Emergency & Radiological Response

Rapidly establish classified reachback from incident command posts and response locations, giving deployed teams secure access within hours instead of requiring a return to fixed accredited facilities.



Secure Transport Operations

Extend classified connectivity directly to mobile operations, supporting missions that are, by their nature, never at a fixed site.



Protective Force & Continuity Operations

Maintain classified mission access when a facility is unavailable, degraded, or evacuated, providing an alternate means for critical personnel to continue operations.



Inter-Site Program Collaboration

Enable laboratories and mission partners to securely collaborate across locations without requiring new fixed classified infrastructure each time teams, programs, or mission requirements change.

PEOPLE | INFORMATION | MISSION | ANYWHERE

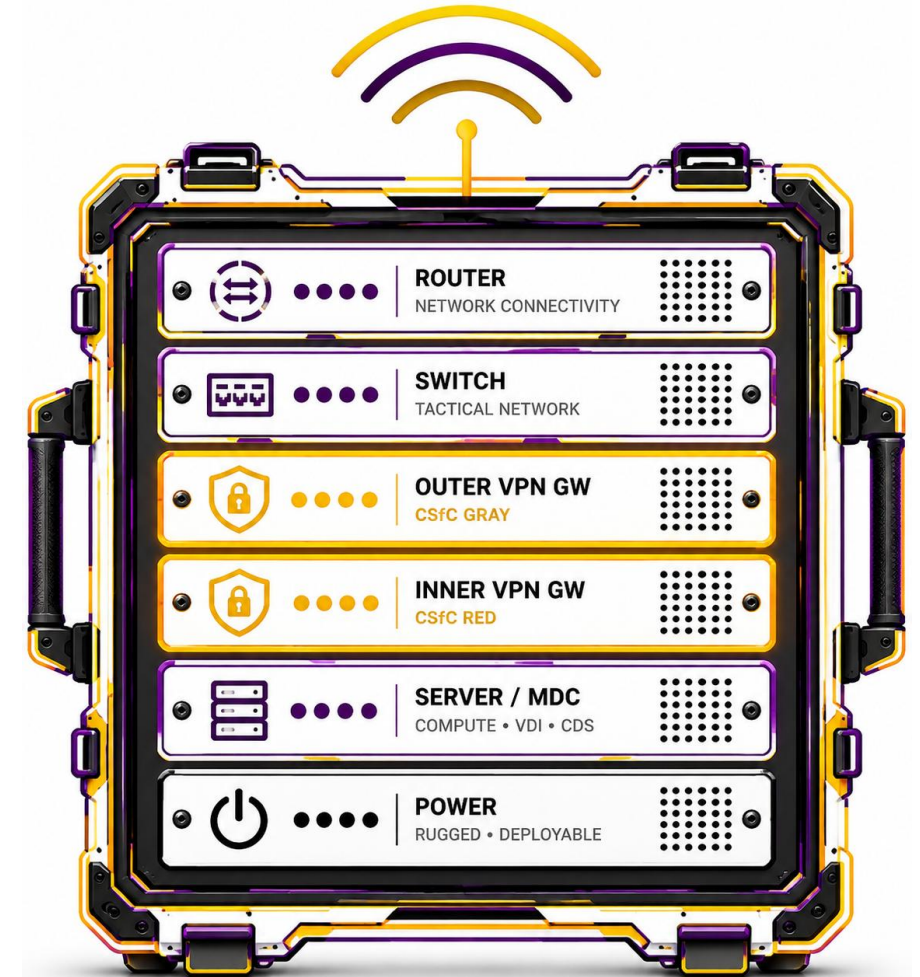
Wherever the Mission Goes, Secure Access Goes With It.

The Classified Enterprise at the Tactical Edge

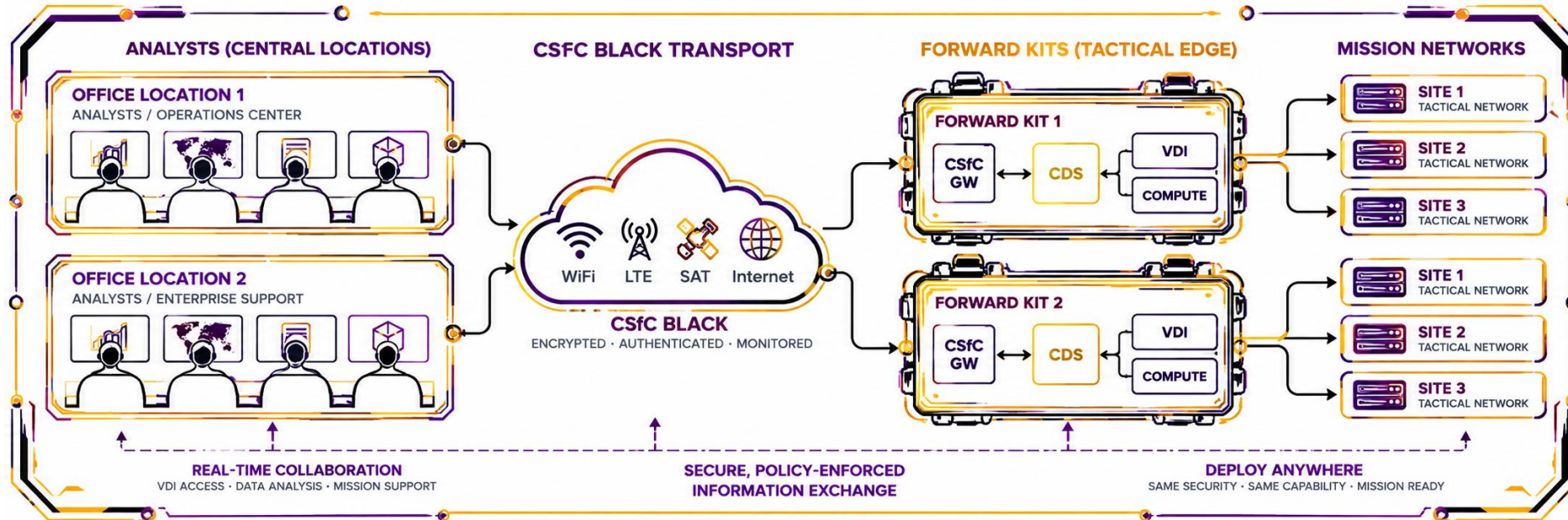
- **Ruggedized Tactical Infrastructure:** Modular, COTS-based compute, networking, and security platforms allow a complete CSfC infrastructure stack to be packaged into compact, transportable form factors, bringing enterprise-class capabilities to tactical and expeditionary environments.
- **Edge Compute & Resilience:** Integrated compute and storage can support virtual machines, containers, and mission applications at the tactical edge, providing local services designed to continue operating in disconnected, intermittent, and limited-bandwidth (DIL) environments.
- **Tactical Wireless Connectivity:** Deployable wireless architectures can extend CSfC-protected Wi-Fi, cellular/LTE, and mesh connectivity to command posts, field teams, vehicles, and other distributed users while aligning with applicable CSfC Capability Packages.
- **Integrated Security & Management:** Small-form-factor infrastructure can consolidate PKI, certificate lifecycle management, VPN management, network security, monitoring, and administration, reducing the equipment footprint while simplifying deployment and sustainment in the field.

What this means for DOE

Bring the classified enterprise to the mission: CSfC, VDI, compute, and Cross Domain capabilities deployed in hours, not months, while maintaining the same security and compliance framework as the fixed environment.



Capability at the Edge; Expertise Remains at the Enterprise



1 Deploy the capability, not the team

A CSfC-enabled tactical kit at the incident site collects and hosts data locally and keeps collecting when the link drops.

2 Expertise at NOC, Mission Support at the Edge

Cleared analysts reach the kit over a CSfC Mobile or Multi-Site path from their home facility instead of travelling to the site.

3 CDS Enables Secure, Policy-Enforced Information Retention

Evidence up, taskings and reference data down — one audited transfer path in place of hand-carried media.

CDS controls and documents how information crosses security domains—but policy still determines what is authorized to cross. Chain-of-custody and RD/FRD review requirements remain part of the process.

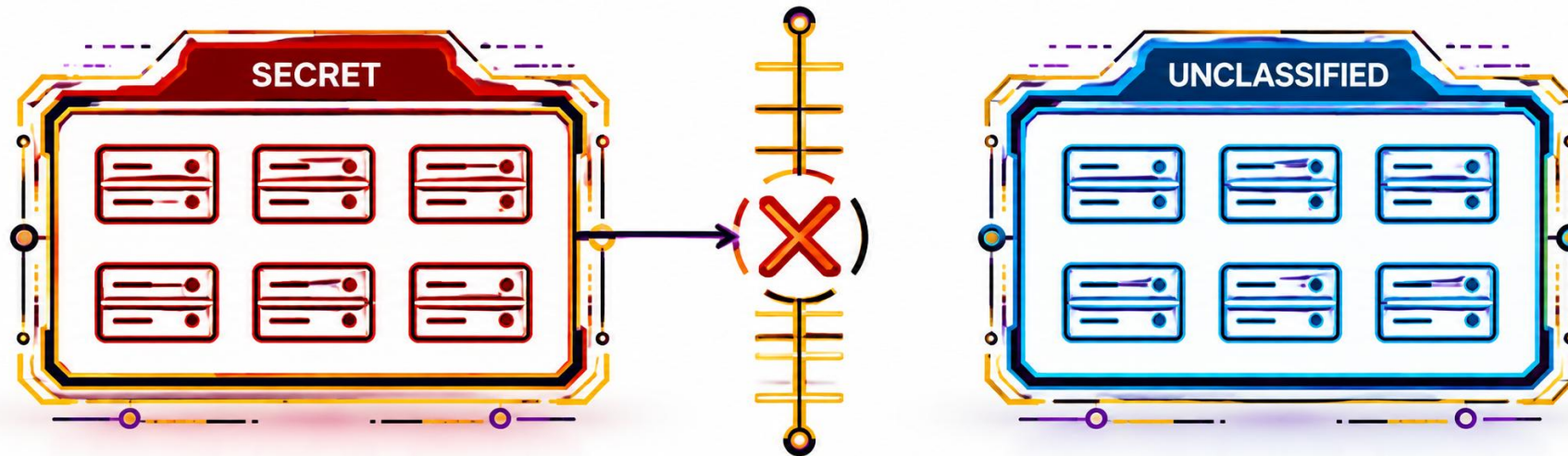
The honest risk picture

- **Mobile Connectivity Carries Inherent Risk:** Commercial cellular and Wi-Fi introduce risks that cannot be completely eliminated. CSfC addresses those risks through layered security controls, defined architectures, and documented operating requirements.
- **Risk Acceptance Remains with the Government:** The Government Authorizing Official (AO) ultimately accepts the residual risk associated with implementing and operating the solution in accordance with the applicable Capability Package.
- **Protect the Endpoint:** Loss, theft, or compromise of a mobile device must be treated as a core design scenario. Data-at-Rest protection—or an architecture that prevents classified data from being stored on the endpoint—must be addressed from the beginning.
- **Physical Security Still Matters:** Secure technology does not eliminate physical risk. Standoff requirements, device handling procedures, and clear end-user operating guidance are integral parts of the deployed security architecture.
- **Continuous Monitoring Requires Resources:** ConMon is not simply a technical feature—it requires people, processes, tooling, and sustained operational ownership. The organization must be prepared to monitor and respond throughout the solution lifecycle.
- **Understand the Residual Risk:** The applicable Capability Package documents the architecture's known threats, assumptions, and residual risks. Those risks should be understood by engineering, cybersecurity, and the AO before the solution is authorized and fielded.



If there is one risk takeaway from this brief, make it this: understand the residual risk, plan for it, and manage it deliberately.

Encryption Secures Data in Transit; Crossing Security Domains Requires a Cross Domain Solution.



1 What encryption does

Type 1 and CSfC secure the path information travels, they protect the data in transit without changing its classification or security domain.

2 What it cannot do

Encryption protects information in transit—it does not authorize it to cross security domains. Cross-domain transfer requires a separately authorized CDS.

3 What it costs today

Manual transfers, duplicated work, and delayed information flow create operational friction—often when timely access to information matters most.

Cross Domain Solutions; Bridging Security Domains for the Mission

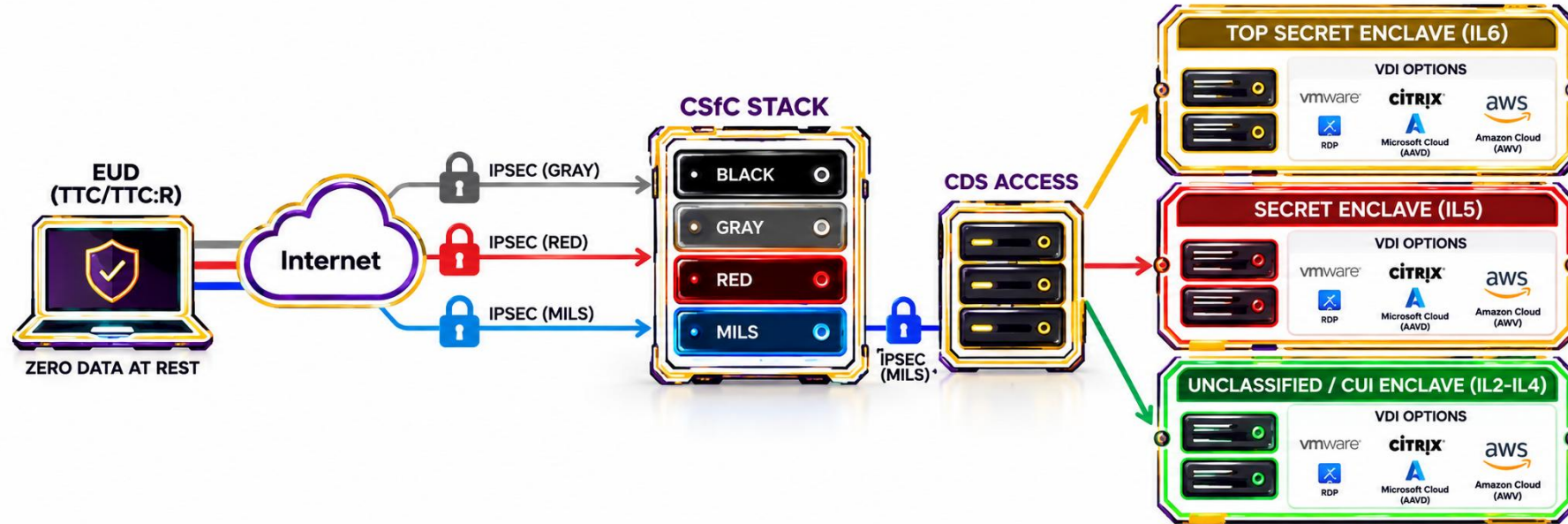


- **Access — Work Across Domains Without Moving the Data:** Provides users secure access to applications, desktops, or information residing in a different security domain from a single endpoint, while the source data remains within its authorized domain.
- **Transfer — Move Information Between Security Domains:** Enables controlled, policy-enforced movement of information between systems operating at different classification levels or security domains, with inspection and filtering applied to the transfer.
- **Multilevel — Multiple Classifications, One Environment:** Supports information at multiple classification levels within a multilevel environment, allowing authorized users to access data based on their identity, permissions, and approved level of access.

The recommendation:

Deploy an Access CDS to provide secure multi-domain desktop access, paired with a Transfer CDS to enable controlled, policy-enforced movement of evidence and mission data between security domains. Select both from the NCDSMO Baseline—leveraging approved, proven capabilities without introducing bespoke development.

One device, one transport, several classified networks



1 Several networks, one path

Each classified environment is delivered as a secure virtual desktop, allowing users to access multiple security domains from a single endpoint. A common CSfC transport provides the secure connectivity, reducing the need for separate physical devices and dedicated network connections for each classification level.

2 Zero data on the device

The user session and classified data remain within the protected data center environment, with no classified information stored on the endpoint. If a device is lost, stolen, or compromised, the mission impact is limited without creating a classified data-at-rest exposure on the device.

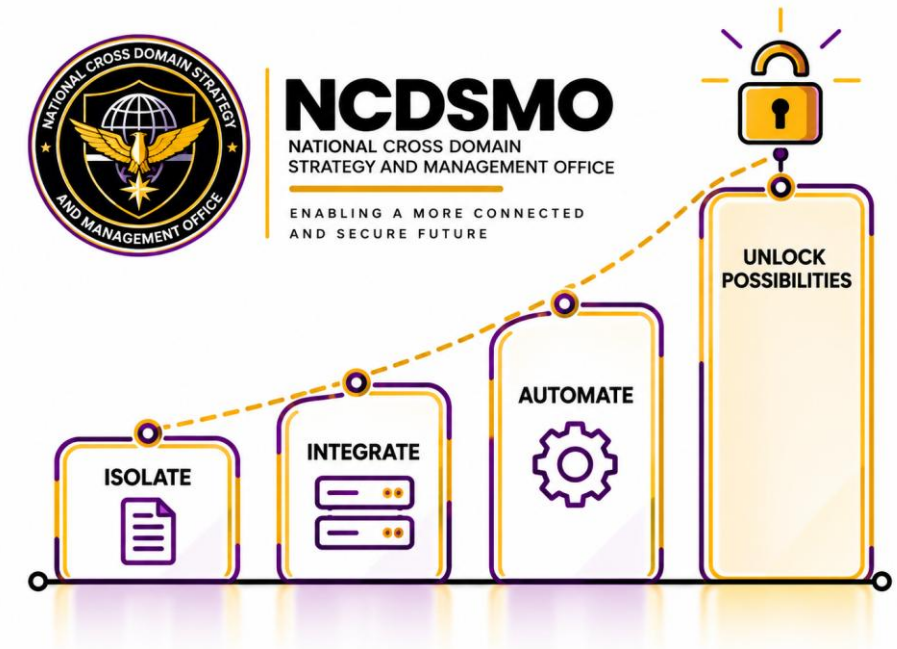
3 Fewer things to protect

Fewer devices per user, fewer dedicated network connections, and less dependence on fixed accredited spaces simplify the overall architecture—while significantly reducing the Data-at-Rest footprint that must be secured, managed, and continuously monitored.

A CDS Access solution enables users to securely reach applications and data across multiple security domains from a single endpoint while keeping the information within its authorized environment. Because the data is accessed rather than transferred or stored locally, the potential spill surface is significantly reduced rather than simply relocated.

Raise the Bar sets the entry price

- **Raise the Bar (RTB)** establishes the cybersecurity standards and security expectations for Cross Domain Solutions (CDS), published by the NSA's National Cross Domain Strategy and Management Office (NCDSMO) and first introduced in 2018.
- **National Security Memorandum 8 (NSM-8), issued in January 2022**, increased federal focus on CDS cybersecurity by requiring agencies operating Cross Domain Solutions connected to National Security Systems (NSS) to report their progress toward meeting Raise the Bar requirements.
- **CDS products undergo rigorous security evaluation.** Vendors must successfully complete a Lab-Based Security Assessment (LBSA) before an evaluated CDS can be included on the NCDSMO Baseline, providing government organizations with a vetted foundation for selecting cross-domain capabilities.
- **The operational takeaway is straightforward:** start with solutions on the NCDSMO Baseline, engage NCDSMO and the appropriate security stakeholders early, and build sufficient time into the program schedule for engineering, assessment, authorization, integration, and deployment.



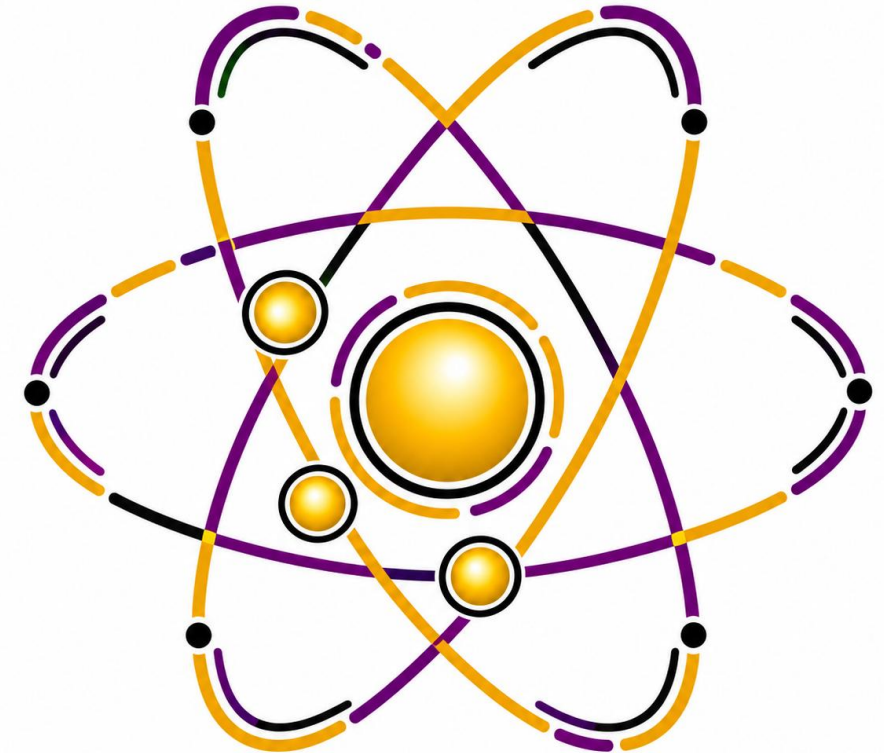
For National Security Systems, Cross Domain security is not a competitive differentiator—it is a compliance requirement. CDS capabilities must meet the security requirements established by the National Manager and applicable CNSS/NCDSMO policy.

What this rules out

Bespoke CDS development and compressed acquisition strategies that underestimate the time required for product selection, security assessment, integration, authorization, and operational fielding.

Restricted Data changes the Cross-Domain problem

- **RD and FRD Bring a Different Policy Framework:** Restricted Data (RD) and Formerly Restricted Data (FRD) are governed by the Atomic Energy Act and associated DOE requirements, adding controls beyond the traditional national security classification framework.
- **Filtering Must Understand DOE Data:** Nuclear weapons information and other controlled nuclear information can introduce specialized review, release, and filtering requirements that cannot be addressed by a generic DoD-oriented cross-domain policy alone.
- **Classification Must Be Part of the Architecture:** DOE classification and information-security stakeholders should be involved during requirements development and CDS design—not brought in only after the technical solution has been selected.
- **Automation Does Not Replace the Release Decision:** Where automated inspection and filtering cannot make an authoritative determination, the transfer workflow should incorporate human review and approval before information is released across the security boundary.



RD / FRD

RD and FRD introduce requirements unique to the Department of Energy's nuclear security mission. A generic cross-domain architecture that does not account for these requirements from the outset can create significant challenges during security assessment, authorization, and operational deployment.

Three authorities, one solution

NSA CSfC: Protect the Transport

Build and maintain the encryption architecture in accordance with the applicable NSA CSfC Capability Packages and annexes. The solution must use appropriate CSfC components, implement the required layered security architecture, complete required testing and documentation, and be registered with NSA before protecting National Security Systems.

DoD: Harden and Approve the Platform

The underlying infrastructure must meet applicable DoD cybersecurity and interoperability requirements before it becomes part of the operational solution. Systems should be hardened in accordance with applicable DISA Security Technical Implementation Guides (STIGs), maintained within approved security configurations, and—where required—use products listed on the DoD Approved Products List (APL). These controls establish the hardened platform on which the CSfC and Cross Domain capabilities operate.

NSA NCDSMO: Control the Cross-Domain Boundary

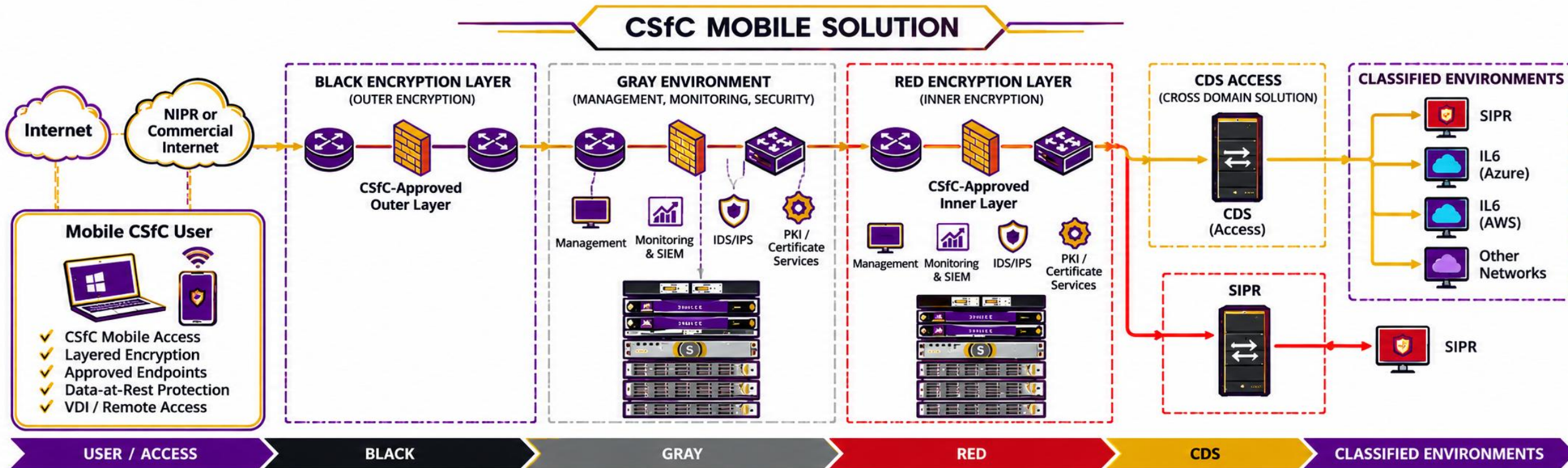
The Cross Domain Solution must satisfy NCDSMO security requirements for accessing or transferring information between security domains. NCDSMO establishes CDS security requirements, oversees cross-domain testing, and maintains the Raise the Bar strategy for improving CDS security throughout design, assessment, implementation, operation, and sustainment.

Where these three authorities converge, the requirements are not always identical—and at times may compete. The challenge is engineering them into a single, cohesive architecture that satisfies each requirement without compromising the mission. That is not simply a documentation exercise; it requires experienced systems engineering, security integration, and accreditation expertise—and it is exactly the work we do.



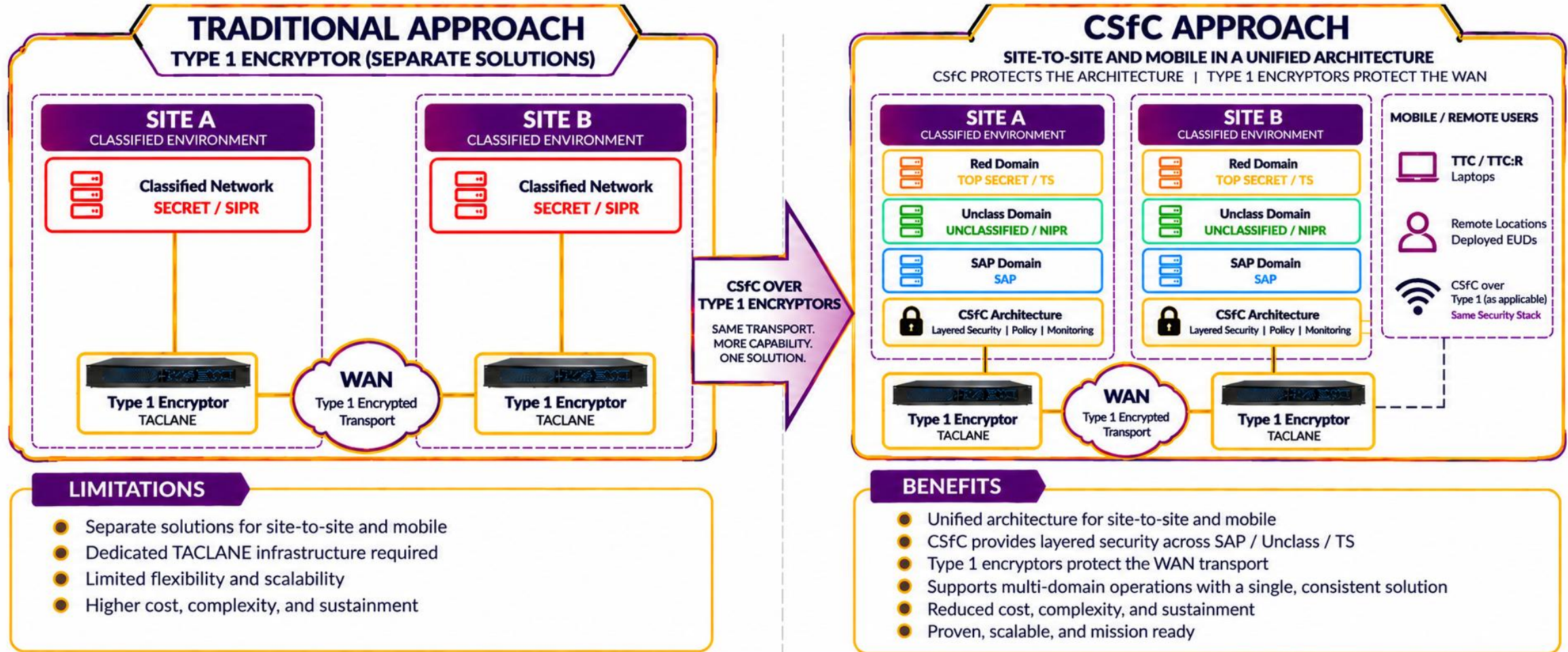
This is not a conceptual architecture—it is a proven operational solution. We have successfully deployed this architecture across 10 DoD environments, supporting more than 25,000 EUDs across all branches of the U.S. Armed Forces. These deployments demonstrate that CSfC, Cross Domain, VDI, and DoD security requirements can be engineered into a single, scalable solution that works in real-world mission environments.

When a solution comes together...



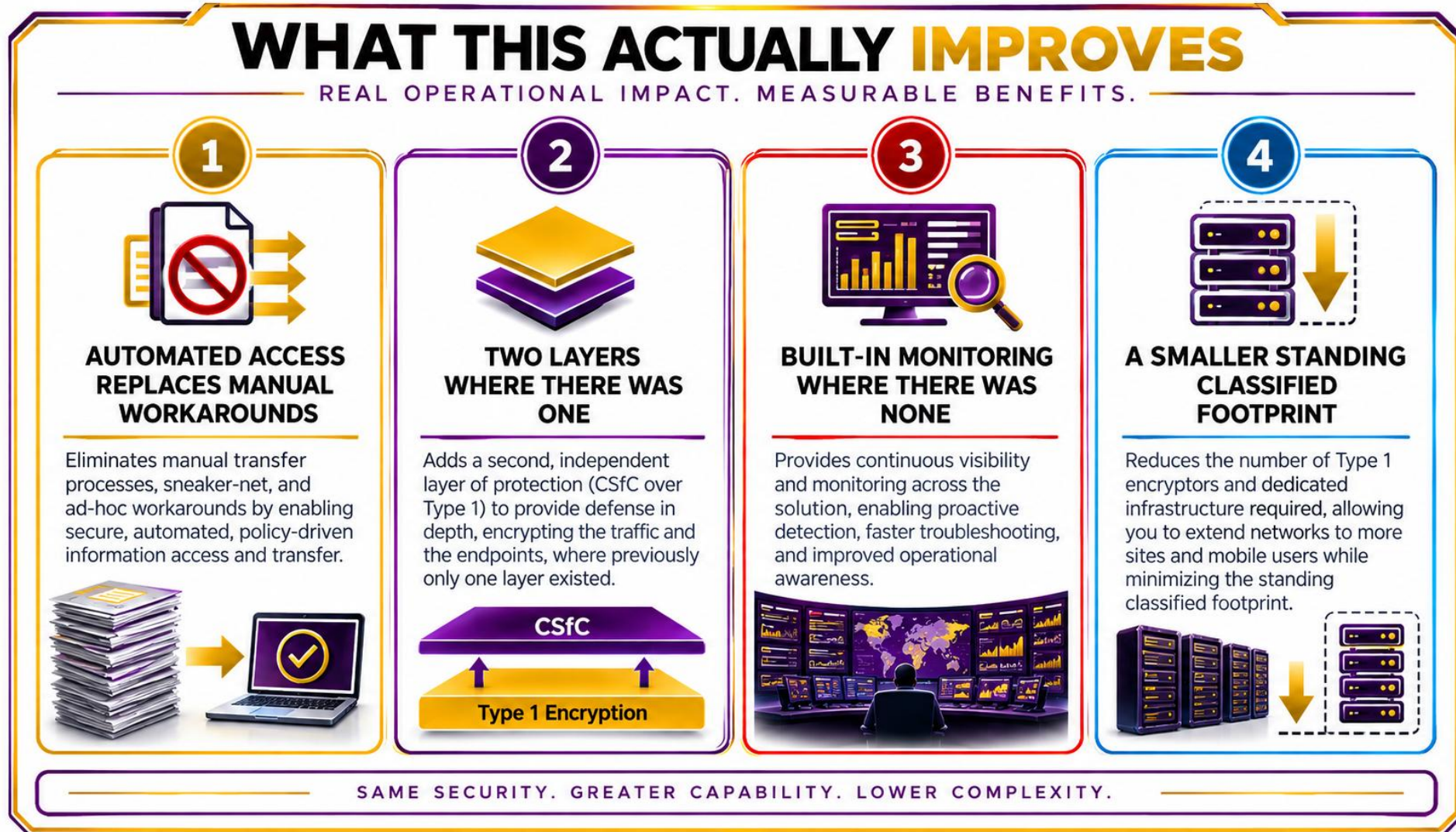
SECURE ACCESS. ANYWHERE THE MISSION GOES.

Target architecture — three capabilities, one design



Existing Type 1 encrypted networks can continue to serve as the secure WAN transport for CSfC, allowing organizations to extend classified connectivity to additional sites and mobile users while reducing the number of dedicated Type 1 encryptors required at the network edge.

What this actually improves



Governance and the authorization path



1 Authorizing Official (AO)

Accepts operational risk and grants the Authority to Operate (ATO) for the complete solution, ensuring the architecture supports the mission while operating within an acceptable level of residual risk.

2 ISSM / ISSO

Develops and maintains the security documentation, validates applicable cybersecurity controls and DoD requirements—including STIGs and APL requirements where applicable—and coordinates the authorization package throughout the assessment and approval process.

3 Trusted integrator

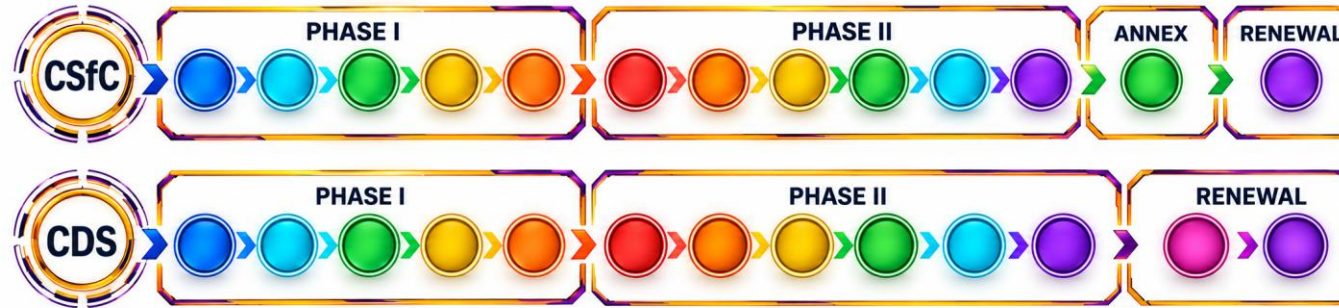
Designs, integrates, tests, and validates the complete solution across CSfC, CDS, network, compute, and DoD security requirements—providing the engineering expertise and technical documentation necessary to move the architecture from concept through authorization and operational deployment.

4 Classification office

Provides classification guidance and ensures information flows, access methods, and transfer policies comply with applicable handling and release requirements. For DOE environments, this becomes especially important when RD, FRD, or other nuclear-related information is involved.

Engage your NSA Client Advocate and NCDSMO early—before the pilot begins, not when the solution is ready for registration. Demonstrating that these stakeholders are already engaged shows the architecture is being developed with the appropriate security authorities involved from the outset and significantly strengthens the credibility of the proposed approach.

A phased roadmap with real decision gates



CSfC

Phase I — Requirements, Design & Acquisition

Months 1–4 | Define It. Design It. Fund It.

1. Gather Mission & Security Requirements
2. Design the CSfC Solution
3. Establish Funding & Acquisition Strategy
4. Procure the Solution
5. Initiate CSfC Registration

CSfC Phase II — Build, Validate & Authorize

Months 4–10 | Build It. Secure It. Prove It

1. Install & Integrate the Solution
2. Configure to the Capability Package
3. Harden & Document the Environment
4. Engineering Validation & Limited Testing
5. Complete CSfC Registration Review
6. CSfC eVote / AO Approval & Authorization

Month 11 — Test Annex / Operational Validation

1. Prove the Deployed Solution

Month 12 — Registration Renewal Validation

1. Sustain Compliance

CSfC/CDS is not simply an installation project—it is a lifecycle: define, design, register, build, validate, authorize, test, and continuously maintain compliance.

CDS

Phase I — Requirements, Design & Acquisition

Months 1–3 | Define It. Design It. Fund It.

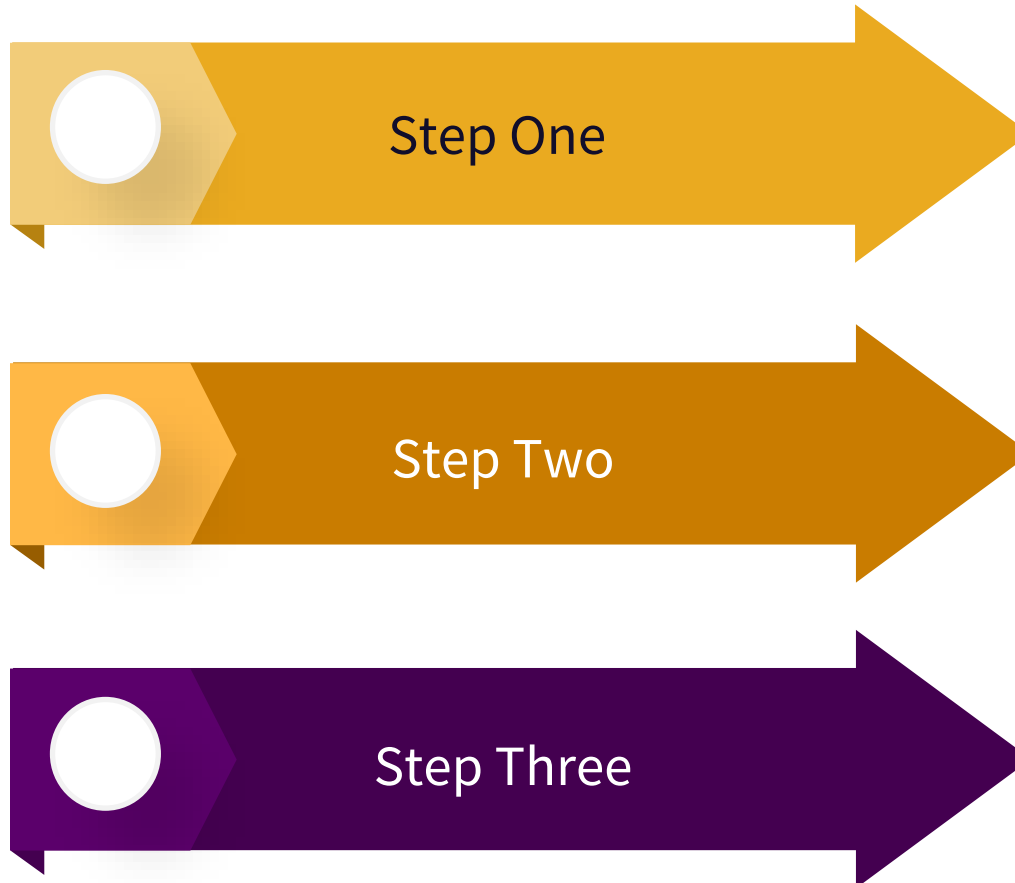
1. Gather Mission & Cross Domain Requirements
2. Design the CDS Architecture
3. Establish Funding & Acquisition Strategy
4. Procure the Solution
5. Initiate the CDS Registration / Approval Process

Phase II — Build, Validate & Authorize

Months 4–8 | Build It. Validate It. Assess It.

1. Install & Integrate the CDS
2. Engineering Validation
3. NCDSMO / Government Coordination
4. Conduct the SBSA Event (Major)
5. Remediation & Limited Operational Testing
6. NSA eVote / Approval

Three Decisions



Define the CSfC Mission Opportunities

Where can secure classified access extend beyond today's fixed infrastructure?.

Define the Cross Domain Mission Needs

Where are mission users constrained by separate security domains or manual information-transfer processes?

Engage Early – Architect Together

Bring the mission, cyber, classification, acquisition, and engineering stakeholders together to define the path forward.

Now's a good time to talk about a “Pilot”.

Prepared, not presented

- **CSfC Reference Architecture:**
Component-level architecture identifying Black, Gray, and Red boundaries, candidate products, and major supporting services.
- **Detailed Cost Model:**
Lifecycle cost model covering acquisition, integration, licensing, accreditation, sustainment, and technology refresh assumptions.
- **CSfC Registration & Renewal:**
End-to-end process covering registration, implementation, validation, Test Annex activities, authorization, and annual renewal.
- **Cross Domain Data Flow:**
Defined CDS Access and Transfer workflows, including information flows, filtering requirements, auditing, and release controls.
- **TACLANE / Type 1 Baseline:**
Technical specifications, throughput, interfaces, key-management requirements, redundancy, and lifecycle considerations for applicable platforms.
- **Capability Package Baseline:**
Current CSfC Capability Package and annex versions, including significant changes and potential architecture impacts.
- **RD/FRD Considerations:**
DOE-specific handling, access, transfer, filtering, release, and classification requirements for RD and FRD information.
- **Monitoring & SIEM Architecture:**
Centralized logging, monitoring, IDS/IPS, SIEM integration, alerting, retention, and continuous-monitoring requirements.
- **Tactical Kit Engineering Package:**
Detailed BOM, transit-case layout, power, connectivity, cabling, spares, and deployment requirements for the tactical solution.
- **Risk Register:**
Documented technical, security, operational, accreditation, and sustainment risks with associated mitigations, ownership, and residual risk.

NSA CSfC — Current Program & Capability References

● CSfC Program Home PROGRAM

NSA's primary CSfC landing page for program overview, Components List, Trusted Integrators, registration, announcements, FAQs, and current program resources.

[OPEN SOURCE →](#)

● Current Capability Packages CURRENT

Authoritative page for current CSfC Capability Packages and annexes. As of September 2026 it lists MA 2.8.0, Campus WLAN 3.2.0, MSC 1.3.0, DAR 5.1.0, Enterprise Gray 1.2.0, WIDS/WIPS 2.0.0, and Tactical CP resources.

[OPEN SOURCE →](#)

● Archived Capability Packages ARCHIVE

NSA archive of superseded CP versions. Useful for configuration history and gap analysis, but NSA states new registrations must use the latest approved Capability Package.

[OPEN SOURCE →](#)

● CSfC Customer Handbook GUIDE

NSA quick-reference guide explaining CSfC roles, Capability Packages, layered COTS architecture, product selection, implementation, testing, registration, and lifecycle responsibilities.

[OPEN SOURCE →](#)

● Mobile Access CP — Current MA 2.8

Use the current Capability Packages page for the approved Mobile Access CP. Version 2.8.0 superseded the older 2.7.x material and adds current CNSA 2.0 objective requirements.

[OPEN SOURCE →](#)

● Solution Registration PROCESS

Official registration guidance. NSA requires CSfC solutions protecting NSS to be registered and validates required forms, network diagrams, and compliance with the associated Capability Package(s).

[OPEN SOURCE →](#)

Cross Domain, DoD Hardening & Integration References

● NCDSMO — NSA

CDS

Official National Cross Domain Strategy & Management Office page. Defines NCDSMO responsibilities for CDS security requirements, testing oversight, threat intelligence, standards, guidance, and Raise the Bar.

[OPEN SOURCE](#) →

● Raise the Bar & NCDSMO Guidance^{RTB}

The NCDSMO page is the public authoritative starting point for Raise the Bar. It also provides links to the NCDSMO standards and guidance libraries hosted on Intelink for government users.

[OPEN SOURCE](#) →

● NCDSMO Documentation — Intelink-U

INTELINK

Government-accessible NCDSMO standards and guidance library for CDS architecture, engineering, implementation, management, monitoring, filtering, and current RTB requirements. Access may require an authorized account.

[OPEN SOURCE](#) →

● DoDI 8540.01 — Cross Domain Policy

POLICY

Department of Defense instruction establishing DoD policy and responsibilities for cross-domain capabilities. Use with current component guidance and NCDSMO requirements when engineering or authorizing CDS.

[OPEN SOURCE](#) →

● DoDI 8510.01 — DoD RMF

RMF

Current DoD Risk Management Framework instruction (July 19, 2022). Defines the RMF process used to manage cybersecurity risk and authorize DoD systems throughout their lifecycle.

[OPEN SOURCE](#) →

● DISA STIGs — DoD Cyber Exchange

HARDEN

Authoritative public repository for Security Technical Implementation Guides and Security Requirements Guides used to harden DoD technologies and support RMF control implementation.

[OPEN SOURCE](#) →

● TACLANE Network Encryption

TYPE 1

General Dynamics Mission Systems' current TACLANE portfolio page covering certified high-assurance network encryptors from tactical/mobile HAIPE devices through high-speed enterprise Ethernet encryption platforms.

[OPEN SOURCE](#) →

● OSC Edge — CSfC Engineering

INTEGRATE

OSC Edge's CSfC capability page describing NSA Trusted Integrator services, classified remote access, CSfC engineering, accreditation support, VDI integration, deployment, O&M, and sustainment.

[OPEN SOURCE](#) →

● OSC EdgeTech — ANC 8(a)

8(a)

OSC EdgeTechSolution's current site for its CIRI-owned, SBA 8(a) federal IT and cybersecurity capabilities, including CSfC, engineering, enterprise IT, and streamlined ANC acquisition pathways.

[OPEN SOURCE](#) →

Thank You

For Additional Information, Please contact:



Lisa Dials

Senior Director, Business Development

lisa.dials@osc-global.com

(240) 444-4679

