ChatGPT

Program Identification and Scope

It appears the **U.S. Army's Cross-Domain Cyber Modernization** effort is the program in question. This is a large-scale Army initiative (on the order of **$800 million** total value) focused on upgrading and engineering **Raise-The-Bar (RTB)–compliant Cross Domain Solutions (CDS)** across Army networks. The work is being executed through the Army's **Total Engineering & Integration Services IV (TEIS-IV)** contract – a 10-year, **$800M** multi-award IDIQ vehicle under Army ISEC [1]. Major defense contractors, including **GDIT** (a TEIS-IV prime) [2] and likely **Leidos** (as a teaming partner or subcontractor), are involved in this effort, which is based in Maryland and requires TS/SCI **with CI poly** cleared personnel due to the highly classified environments and NSA standards at play.

Program Objectives: The Army's cross-domain program is aimed at **modernizing and securing information-sharing across classification boundaries** in line with NSA's **RTB** guidelines. Engineering requirements explicitly call for **knowledge of RTB standards and NCDSMO processes**, meaning the team must design and upgrade CDS guard systems to meet the stringent security controls set by NSA's National Cross Domain Strategy Management Office [3]. In practical terms, this involves ensuring all Army-deployed cross-domain solutions (e.g. data guards, one-way diodes, etc.) pass NSA's lab-based security assessments and implement the **"Raise the Bar"** architecture improvements (such as hardware-enforced one-way transfers, robust content filtering, etc.) [3] [4]. The goal is to **"raise the bar" on cross-domain cybersecurity** so that classified data can be shared between networks (e.g. between different security enclaves or with coalition partners) rapidly **but without compromise** [5] [6]. This Army program was mentioned via an internal referral (by an Army VP), indicating it's actively in the **staffing and execution phase** now.

Contract Vehicle and Key Players

The **contract vehicle** for this initiative is **TEIS-IV** (Total Engineering & Integration Services IV). TEIS-IV is a contract awarded by Army Contracting Command (ACC) – Aberdeen Proving Ground (Huachuca Division) in late 2021, with a ceiling of roughly $800M over 10 years [1]. It's a **multiple-award IDIQ**, meaning several companies hold prime positions. Notably, **General Dynamics IT (GDIT)** is a prime contractor on TEIS-IV [2], and at least one **small-business prime (TekSynap)** highlighted that the **$800M IDIQ** supports Army ISEC's worldwide IT/cyber engineering mission [1]. Although Leidos is not listed as a prime on TEIS-IV, it likely participates as a subcontractor or on related task orders (Leidos has been hiring cyber engineers at Aberdeen Proving Ground with RTB/CDS expertise, suggesting involvement in this effort). In short, **GDIT, Leidos, and possibly others (e.g. CACI, TekSynap, etc.)** are collaborating under TEIS-IV to execute the program's task orders. The work is centered in **Maryland** (Aberdeen and Fort Meade areas), aligning with the presence of Army Cyber and NSA facilities there, hence the need for **CI polygraph-cleared** engineers.

Contract Scope: Under TEIS-IV, the Army can issue task orders for **full lifecycle support of C5ISR IT projects** – including design, implementation, cybersecurity compliance, testing, and sustainment [7] . The cross-domain modernization falls squarely within this scope. For example, task orders are likely funding:

- **Engineering assessments of existing Army CDS** (the "as-is" guards/transfer systems) and designing **RTB upgrades or replacements**.
- **Integration of NSA-evaluated CDS products** (such as new data guards that meet RTB v5 requirements) into Army networks.
- **Testing and lab certification support**, in coordination with NSA NCDSMO, to get Authority to Operate for each CDS under the new standards.
- **Operations & Maintenance (O&M)** of enterprise cross-domain services (sometimes referred to as **"Enterprise Cross Domain Service (ECDS)"** O&M). Job postings for an "ECDS Operations Manager" mentioned duties to "maintain a comprehensive ECDS O&M program" and ensure **RTB compliance** [8] , which aligns with this effort.

In summary, TEIS-IV is the contracting mechanism enabling the Army to rapidly task industry with these specialized cyber engineering services. The **prime contract** provides a **central vehicle** to fund multiple projects aimed at achieving an Army Unified Network with secure, RTB-compliant cross-domain data flow.

Relation to CDES, C5ISR Modernization, and Other DoD Initiatives

This Army program is **closely related to broader DoD cross-domain and cybersecurity initiatives**, but it is **not exactly the same as them – rather, it is complementary**:

- **DISA's Cross-Domain Enterprise Services (CDES):** The Defense Information Systems Agency runs the CDES program to provide enterprise cross-domain services for the DoD. Notably, in 2023–2025 DISA awarded Leidos a 5-year contract (~$35M) to support CDES engineering and integration [9] . The Army's $800M effort is **much larger in scope** – it likely covers Army-specific cross-domain needs (including tactical and coalition environments) beyond what DISA's smaller CDES service provides. However, they share goals: both aim to implement the NSA RTB guidelines across DoD systems. We can expect coordination between Army and DISA so that solutions are interoperable. In essence, the Army program **parallels CDES** (with the Army perhaps developing its own solutions or deploying CDS at Army sites), but it is **run separately under Army oversight**. There may be some overlap in technology and vendors (for example, a common RTB-compliant guard technology could be used in both DISA and Army environments), but organizationally CDES is a DISA initiative whereas the program at hand is an Army-funded effort [9] .

- **Army C5ISR Center / Cybersecurity Modernization:** The Army's Combat Capabilities Development Command C5ISR Center is heavily involved in cyber defense R&D and has its own projects to modernize crypto and network security. In fact, the Army **Unified Network Plan** explicitly calls for *"deploying…commercial solutions for classified and Raise-the-Bar compliant cross-domain solutions"* as a key objective of its cybersecurity modernization line of effort [10] . The program we've identified is essentially **how the Army is executing that objective**. It directly supports C5ISR modernization by upgrading the cross-domain infrastructure to be more secure and robust. For example, earlier this year CACI won a $198M task to help C5ISR Center with cyber defense engineering [11] [12] – that encompasses things like "cryptographic modernization and tactical network protection" which dovetails with ensuring cross-domain guards are up to snuff. Thus, the $800M Army CDS program is

one big piece of the Army's overall cyber modernization puzzle, ensuring that as the Army modernizes its network (Unified Network), the cross-domain aspects are handled in accordance with the latest NSA standards. It does **overlap in goals** with C5ISR Center's efforts, but it is likely **the funding/programmatic vehicle to achieve those goals** (with C5ISR Center and PEO EIS/IEW&S as stakeholders). In short, it's **part of the Army's C5ISR modernization push**, specifically addressing cross-domain info sharing which is critical for multi-domain operations [13] [10] .

- **DoD-Wide Initiatives (e.g. JADC2/MPE):** At the DoD level, initiatives like **Joint All-Domain Command and Control (JADC2)** and the **Mission Partner Environment (MPE)** emphasize seamless, secure data sharing among services and allies. Cross-domain solutions are a **key enabler** for those (since you must bridge networks of different classification and between nations). The Army's program certainly aligns with these efforts. For instance, the Army's **BICES** and MPE networks (used for intel sharing with coalition partners at Secret Releasable level) require RTB-compliant CDS as they evolve. In March 2024, a **$239M contract** was awarded to GD Mission Systems to sustain and enhance the *"Battlefield Information Collection and Exploitation System – Trusted Network Environment (TNE) cross-domain solution"* for coalition sharing [14] [15] . That is essentially the **coalition Secret REL cross-domain service (part of MPE)**. The Army's broader $800M effort likely interacts with such projects – ensuring that any cross-domain gateways for coalition use are RTB-compliant and that Army's own classified networks can plug into JADC2 data fabrics. However, **the $800M program is more encompassing** – covering internal Army needs (not just coalition), including cross-domain between different Army classification levels and between tactical and enterprise domains. Think of it as the Army equipping itself with a **unified, RTB-approved cross-domain capability** that will also support DoD-wide goals of info sharing. It does **not duplicate** JADC2 or MPE; rather it provides the secure plumbing needed for the Army to participate in those initiatives.

In summary, the program is **distinct but overlapping in intent** with CDES and other efforts. **It is the Army's dedicated investment to "Raise the Bar" for its cross-domain information systems**, in parallel with DISA and others doing the same in their realms. All these efforts are guided by the same NSA NCDSMO standards, so they are inherently connected. As such, an engineer on this program will be working on problems very similar to CDES (and may leverage some of the same solutions), and contributing to the Army's segment of the DoD's broader secure info-sharing architecture.

Sources:

- Army ISEC **TEIS-IV Contract (10-year, $800M IDIQ)** – prime contract overview (GDIT) [2] [1] .
- **DISA CDES program** award (Leidos, 5-year $35M) for cross-domain enterprise services [9] .
- Army **Unified Network Plan 2021** – calls for *"Raise the Bar compliant cross-domain solutions"* as part of cyber modernization [10] .
- Federal News commentary on RTB and cross-domain importance across DoD [5] [6] .
- GovCon news on Army coalition CDS (BICES TNE) and C5ISR cyber efforts for context [14] [12] .

---

[1] TekSynap Awarded the $800M, 10-year Multi-Award IDIQ Total Engineering & Integration Services (TEIS-IV) - TekSynap

https://www.teksynap.com/press-releases/teksynap-awarded-teis-iv/

2 7 TEIS IV | GDIT

https://www.gdit.com/about-gdit/contract-vehicles/agency-contracts/total-engineering-and-integration-services-teis-iv/

3 4 Raise the Bar sets high standards for Cross Domain Solutions - 5 key challenges for CDS vendors

https://www.glasswall.com/blog/raise-the-bar-sets-high-standards-for-cross-domain-solutions-5-key-challenges-for-cds-vendors

5 6 Defense, intel agencies look to "raise the bar" on cybersecurity

https://federalnewsnetwork.com/federal-insights/2023/08/defense-intel-agencies-look-to-raise-the-bar-on-cybersecurity/

8 Operations Manager - TS/SCI Poly Required - Built In

https://builtin.com/job/operations-manager-tssci-poly-required/3835760

9 Leidos Wins $35M DISA Contract to Modernize Cross-Domain Data …

https://washingtonexec.com/2025/06/leidos-wins-35m-disa-contract-to-modernize-cross-domain-data-sharing/

10 13 api.army.mil

https://api.army.mil/e2/c/downloads/2021/10/07/d43180cc/army-unified-network-plan-2021.pdf

11 12 CACI Wins $198M Army C5ISR Cyber Defense Support Contract; John Mengucci Quoted – GovCon Wire

https://www.govconwire.com/articles/caci-wins-198m-army-c5isr-cyber-defense-support-contract

14 15 > U.S. Department of Defense > Contract

https://www.defense.gov/News/Contracts/Contract/Article/3696684/