Forcepoint

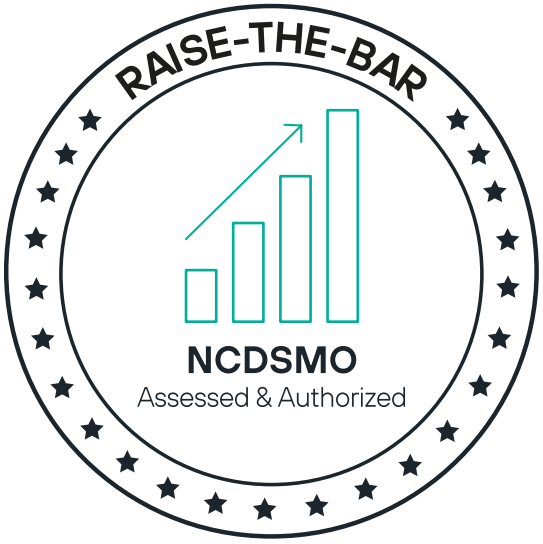
Solution Brief

Forcepoint Meets Current National Cross Domain Startegy Managment Office Raise-The-Bar Guidelines for Cross Domain

Forcepoint continues to be the only commercial vendor with both Access and Transfer solutions recognized by the National Cross Domain Strategy Management Office (NCDSMO).

Forcepoint continues to work and meet the NCDSMO Raise-The-Bar (RTB) requirements for their Cross Domain Solutions (CDS) – both transfer and access technologies and has received Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) authorizations.

- → **High Speed Guard (HSG)** – Transfer solution - designed to meet current RTB requirements and specifications. Has been included on the NCDSMO CDS Baseline List for TSABI and SABI since 2001. Continuously developing version releases and upgrades to meet compliance.
- → **Trusted Gateway System (TGS)** – Transfer solution - designed to meet current RTB requirements and specifications and integrates with cybersecurity industry and adopted NSA-recommended data filtering technologies: Glasswall, Purifile, and Aware. Continuously developing version releases and upgrades to meet compliance. The latest release is currently being evaluated against the latest RTB version.
- → **Trusted Thin Client (TTC)** – Access solution - completed lab-based security testing, meeting the RTB security guidelines and implementations. Continuously developing version releases and upgrades. Currently deployed in various classified, tactical and CSfC environments.
- → **SimShield** has completed lab-based security testing, meeting the RTB requirements



Additionally, Forcepoint enables customers to achieve streamlined Assessment & Authorization (A&A), resulting in deployable technologies that meet mission requirements while maintaining the highest level of security.

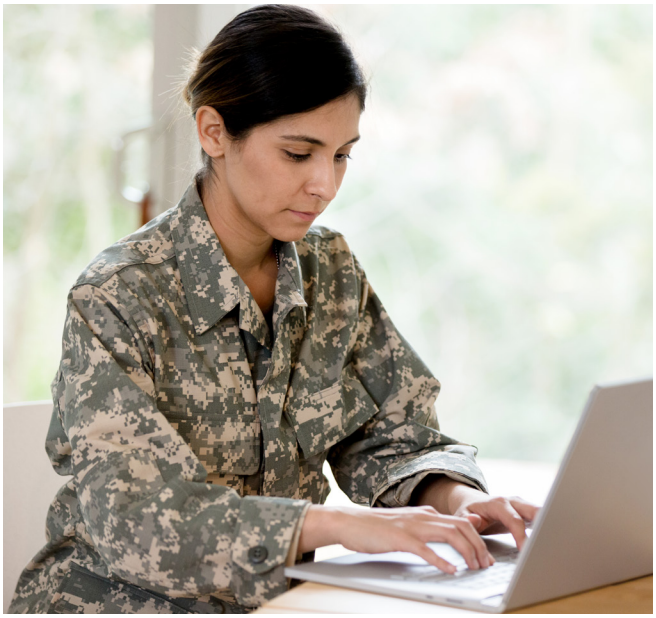
Raise-The-Bar strengthens the security posture of Cross Domain Solutions

RTB requirements and specifications increase the security design, development, engineering, architecture and implementation bar for all CDS's beyond just the NIST Risk Management Framework (RMF) controls. The RTB requirements are also intended to:

- → Reduce adversarial attacks against or through a CDS
- → Reduce developer mistakes in the design, engineering and development processes

Secure technology development and engineering

Forcepoint works directly with NCDSMO to ensure we are designing and building secure and creditable solutions before going into testing. This rigorous vetting process and its positive results are demonstrated by each Forcepoint technology that has successfully met the RTB guidelines and received favorable deployable risk ratings.



The following Forcepoint CDS technologies that have recently gone through Lab Based Security Assessments (LBSA) and evaluated against the RTB requirements include:

- → **Forcepoint High Speed Guard and High Speed Guard SP (v5.x)** – specializing in rapid, machine-to-machine data transfer with the industry's fastest transfer rates of more than 9Gb/s and latencies as low as 1.3ms– is redesigned with two built-in redundant filtering capabilities, the Rule Engine and the Filtering Engine, to provide consistent policy enforcement across all transfer mechanisms
- → **Forcepoint Trusted Gateway System (v5.x)** – specializing in file transfer with two-person review workflow–is redesigned so that the functionality and responsibility is distributed among several distinct Linux processes running at each of the guard-supported security labels. This ensures that compromise of any single process will not pose a significant threat to the overall security of the system. This version also includes more robust filtering and transformation capabilities, leveraging third-party solutions such as Glasswall, Purifle, and Aware. Trusted Gateway System is also a R.A.I.N. (Redundant, Always Invoked, Independent Implementations, and Non-Bypassable) compliant solution.
- → **Forcepoint Trusted Thin Client (TTC) & Trusted Thin Client-Remote (TTC-R) v2** – provides seamless, simultaneous access to multiple networks from a single device– completed numerous security improvements such as additional hardening and security restrictions on the Thin Client, including FIPS 140-2 compliance, improved dual-authentication controls, and in-depth network traffic validation with use of robust IPsec to secure communications. Initial SABI testing under the RTB guidelines was completed July 2017 and has additionally completed delta testing with a favorable rating. The delta test included functionality required for Trusted Thin Client Remote deployments utilizing Commercial Solutions for Classified (CSfC) components.
- → **Forcepoint SimShield (v3)** – specializing in data transfer for multi-level training and testing environments utilizing HLA, DIS, and/or TENA protocols–was the first Forcepoint product to meet RTB guidelines through enhanced role and process separation. With the completion of SABI testing, SimShield continues to provide enhancements in support of our customers' training and testing missions.

forcepoint.com/contact