

Forcepoint Meets Current NSA & NCDSMO 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).

Most recently Forcepoint has achieved Top Secret/SCI And Below Interoperability (TSABI) and Secret And Below Interoperability (SABI) authorizations across the product line. Forcepoint product solutions meet the National Security Agency (NSA) Raise-The-Bar guidelines.

- ▶ Newest versions of **SimShield**, and **Trusted Thin Client** have completed government lab-based security testing, meeting the government's Raise-The-Bar security guidelines and concepts.
- ▶ **High Speed Guard**, designed to meet current NSA Raise-The-Bar guidelines, has been included on the NCDSMO Baseline for TSABI and SABI since 2001 with the newest version in process.
- ▶ **Trusted Gateway System** is designed to meet current NSA Raise-The-Bar guidelines, and integrates with cybersecurity industry and adopted NSA recommended data filtering technologies: **Glasswall, Purifile, Aware and Sophos**. (TSABI and SABI authorization is in process)
- ▶ Enabling customers to achieve streamlined Assessment & Authorization (A&A) resulting in **faster speed to mission while maintaining the highest level of security**.



RAISE-THE-BAR STRENGTHENS THE SECURITY POSTURE OF CROSS DOMAIN SOLUTIONS

Raise-The-Bar (RTB) guidelines—led by the NSA and NCDSMO—raise the security architecture bar for Cross Domain Solutions (CDS) beyond even the NIST Risk Management Framework (RMF) controls with a particular emphasis on Guard solutions that move (Transfer) data and files between segmented networks.

As cyber threats continue to escalate in scale and frequency, it is imperative that our solutions continue to stay ahead of the adversary—particularly CDS that protect the worlds' most sensitive data and support the most critical missions. The RTB best practices address two threats:

- ▶ Adversarial attacks against or through a CDS
- ▶ Developer mistakes in the cross domain implementation and development

MORE ARCHITECTURALLY ROBUST AND SECURE

Forcepoint works directly with the cross domain security community to ensure we are designing and building accreditable solutions before they even reach the test labs. This rigorous process and its positive results are demonstrated with Forcepoint SimShield, our first solution to successfully meet the guidelines and receive one of the best ratings ever given for a transfer solution.

- ▶ **Forcepoint High Speed Guard** and **High Speed Guard SP** version 5 – 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. High Speed Guard has successfully completed SABI government lab-based testing with a favorable rating (for a specific customer use case). The round of testing currently in process is to authorize all supported data types and flows. This product generation has also favorably completed TSABI testing.
- ▶ **Forcepoint Trusted Gateway System** version 5 – 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. Also includes more robust filtering and transformation capabilities, leveraging 3rd party solutions such as Glasswall, Purifle, Aware and Sophos. Trusted Gateway System is a R.A.I.N. (Redundant, Always Invoked, Independent, and Non-bypassable) compliant solution.
- ▶ **Forcepoint Trusted Thin Client (Trusted Thin Client Remote)** version 2 – providing 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 FIPS140-2 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 recently 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** version 3 – specializing in data transfer in multilevel 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.