

Does your Transfer Guard Raise the Bar?

13 questions to ask your current provider

See how your vendor stacks up with the latest transfer guard capabilities and compliance requirements

While secure file sharing between federal, state, and local entities is required, doing so between varying classification levels can be inefficient, ineffective, and more importantly, insecure, creating unacceptable levels of risk.

In an effort to raise the security architecture bar for cross domain solutions beyond even the NIST Risk Management Framework (RMF) controls, the NSA and NCDSMO introduced their “Raise the Bar” initiative to continually improve the status quo within the cross domain community.

Time is running out to comply with Version 1 Raise the Bar requirements due 12/31/2020 so now, more than ever, is the time to ensure your vendor is not only compliant but also has industry-leading capabilities.

Find out how your vendor stacks up by asking them these 13 yes-or-no questions:

1. **Can your solution sustain a large file transfer rate for unstructured data (above 1.5 Gigabits in less than six minutes), or 9 GB/second with latencies as low as 1.3ms for structured data?**
2. **Does it support multi-directional (high-to-low and low-to-high) file transfer?**
3. **Is it NCDSMO listed?**
4. **Does it sanitize and remove malware and malicious viruses?**
5. **Does it include Reliable Human Review (RHR) for high-to-low “template-based submit” that makes transferring, replicating, and sharing files easy and a Directory Transfer Service Option (DTSO)?**
6. **Can it support 20+ domains and multiple data flows?**
7. **Does it have real-time support/access to developers?**
8. **Is it a single box solution?**
9. **Is it expandable to support other functions such as email box and printer consolidation?**
10. **Does it include multi-stage file sanitization and validation?**
11. **Does it support the latest versions of Microsoft documents, PDFs, and images?**
12. **Does it include 24x7 support?**
13. **Does it support the newer R.A.I.N. methodology by supporting two independent filters for each data type?**

If your vendor answered no to any of these questions, it's time to upgrade your solutions with Forcepoint **Trusted Gateway System**.

Designed to meet current NSA Raise The Bar guidelines, Forcepoint Trusted Gateway Solution integrates with cybersecurity-industry and adopted NSA-recommended data filtering technologies: **Glasswall, Purifile, Aware, McAfee, and Sophos**. (TSABI and SABI authorization in process.) Forcepoint Trusted Gateway System checks the box on every question above.

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.

forcepoint.com/contact