OWL Cyber Defense™

Strengthening Decision Advantage with Raise the Bar

Keep missions ahead of emerging threats with high-assurance CDS.

Raise the Bar for real mission value across the cross-domain ecosystem.

- → RTB provides rigorous standards to reduce exploitable weaknesses and mission risk in CDS.
- → RTB provides clear guidance to streamline accreditation, improve interoperability, and build trust in CDS performance.
- → Owl collaborates with NCDSMO and ensures V2CDS, XD Vision, XD Bridge ST and XD Guardian XML CDSs are validated for achieving RTB guidance.
- → Keeping pace with RTB updates preserves accreditation, hardens security posture and maintains defenses against evolving threats.

Outpace Adversaries with RTB-Ready CDS

As the threat landscape accelerates and adversaries remain relentless in their hunt for exploitable gaps, continuously strengthening cross-domain security posture becomes a decisive factor in whether a mission gains or loses decision advantage.

For over a decade, the U.S. Government's Raise the Bar (RTB) strategy, led by the National Cross Domain Strategy & Management Office (NCDSMO), has set the standard for cross-domain security through prescriptive guidance on Cross Domain Solution (CDS) product assessment, authorization, and integration of critical upgrades, ensuring that missions can trust the data they rely on. This critical strategy ensures that every CDS approved for use by U.S. defense and intelligence agencies delivers the highest level of security to protect national interests, enable faster, more confident action, and prevent any system from becoming the mission's weak link.

By following the Raise the Bar's design principles, agencies gain practical direction for how CDS should be engineered, assessed, integrated and maintained, converting cross-domain discipline into a persistent edge in decision advantage.

5 core principles in the NCDSMO's Raise the Bar strategy include:

1. **"RAIN" principle:** Short for redundant, always invoked, independent, non-bypassable, RAIN is an application of Policy Enforcement Failure Analysis (PEFA) and ensures security mechanisms remain effective and cannot be easily bypassed.
2. **Robust Filtering:** Filter cleanliness, correctness and integrity ensure a 'known good state' for the right data to get to the right domain according to policy and regardless of the number of simultaneous transfers.
3. **Least Privilege, Knowledge & Functionality:** Ongoing verification that only the necessary permissions & functions are used to diminish unnecessary risk and implemented in part via stringent Mandatory & Discretionary Access Controls.
4. **Fortified Dev Environment:** Physical isolation from risky networks and data movement in and out via advanced hardware-enforced one- and two-way security mechanisms protects the environment from additional threat.
5. **Supply Chain Integrity:** Developers responsible for the integrity of the supply chain adhere to several safeguards regarding acceptable sourcing (including anti-tamper guidance) and configuration of the CDS as well as risk identification, assessment, prioritization and mitigation.

203-894-9342 | owlcyberdefense.com

While the Raise the Bar strategy in its current state is considered functionally complete, like any mission-critical capability, it should not be treated as finished. Rather, Raise the Bar and the CDS that have been validated against the program must be regularly revisited and updated to remain ahead of evolving threats and maintain mission-ready assurance.

For over 25 years, Owl Cyber Defense has remained committed to continuously innovating, securing, maintaining, updating, and hardening our CDSs—and offers a validated suite of solutions designed to keep pace with evolving threats while enabling secure, reliable cross-domain operations:

Scan to learn more

CDS V2CDS

Voice and video CDS enabling secure, RTB-compliant, real-time collaboration across classified domains; first NCDSMO Baseline-listed VoIP CDS for U.S. DoD and IC.

Scan to learn more

CDS XD Vision

NCDSMO-validated collaboration CDS delivering secure, voice, video, and data across domains, with scalable multi-domain architecture and fine-grained policy controls for complex mission environments.

Scan to learn more

CDS XD Bridge ST

Hardware-enforced, NCDSMO-validated CDS providing high-speed, high-assurance, RTB-aligned data transfer and hardware-enforced domain separation to improve decision advantage in contested cyber environments.

Scan to learn more

CDS XD Guardian XML

NCDSMO-validated XML guard providing content inspection, validation, and transformation between domains, enforcing fine-grained data policies to block malformed or malicious XML while enabling mission-essential information sharing.

Ready to align your CDS with RTB and protect decision advantage at every layer? Connect with the OWL team to discuss requirements, answer RTB questions, and navigate assessment and authorization with confidence.

Scan the QR code to contact us

OWL Cyber Defense™

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

For more information on Owl, or to schedule a demo, visit **www.owlcyberdefense.com.**

203-894-9342 | owlcyberdefense.com