

CYBERSECURITY READY SUITE™ SOLUTION BRIEF

Supplier Readiness for the Golden Dome Era

America's next generation of defense programs will rely on thousands of companies across the Defense Industrial Base protecting Controlled Unclassified Information (CUI) — wherever it is stored, processed, and shared.

• Protect CUI

• NIST SP 800-171

• U.S. Army NCODE

Through the U.S. Army's NCODE (Next-Gen Commercial Operations in Defended Enclaves) initiative, Exostar is proud to be an Army-approved provider — helping suppliers protect CUI inside secure, defended enclaves while implementing the security practices defined in NIST SP 800-171.

THE CHALLENGE

CUI doesn't stay in one place

CUI doesn't sit on one server or inside one application. It moves throughout your business every day — it is:

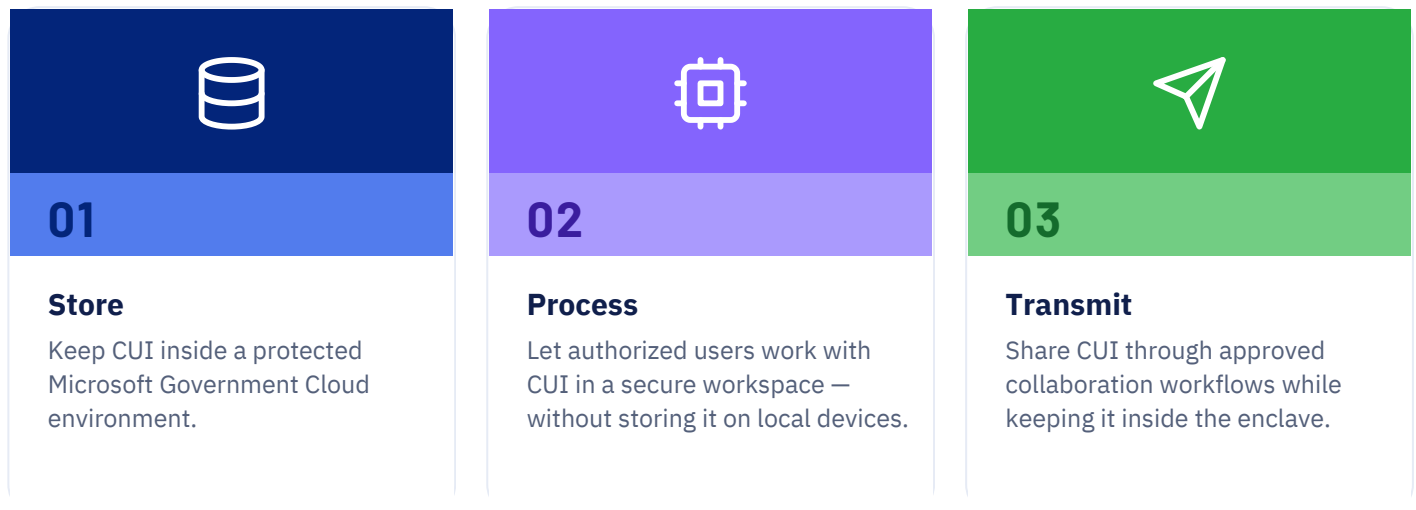
- Created by engineering teams
- Reviewed by manufacturing
- Sent to suppliers and subcontractors
- Shared with customers
- Accessed by quality teams
- Retained for contractual and regulatory purposes

Every time CUI moves outside a controlled environment, the opportunity for risk increases. Securing every laptop, shared drive, email attachment, and endpoint quickly becomes expensive, hard to manage, and difficult to scale. A better approach is to protect the one environment where CUI lives — an enclave.

ONE SECURE FOUNDATION

Store. Process. Transmit.

Every organization that handles CUI must answer three questions: where is CUI stored, where is it processed, and how is it transmitted? Exostar answers all three through a Microsoft-based defended enclave — one secure environment where CUI stays protected throughout its lifecycle.



THE CUI LIFECYCLE

Protecting the complete CUI lifecycle

Every piece of Controlled Unclassified Information follows a journey. Rather than protecting hundreds of individual locations where CUI could exist, organizations focus on the one environment where CUI is intentionally stored, processed, and transmitted.

- 1 Create or receive.** CUI enters your organization from a customer, partner, or internal team.
- 2 Access.** Authorized users securely access the environment.
- 3 Store.** CUI remains inside the protected enclave.
- 4 Process.** Users securely review, edit, and collaborate on sensitive information.
- 5 Transmit.** Information is shared through approved workflows while remaining protected.
- 6 Govern.** Policies, documentation, and operational practices support ongoing NIST SP 800-171 implementation.

THE CYBERSECURITY READY SUITE

Everything working together to protect CUI

Protecting CUI requires more than technology — it requires a cybersecurity foundation for secure collaboration, governance, and operational consistency. The Exostar Cybersecurity Ready Suite helps organizations:

- Protect CUI throughout its lifecycle
- Reduce cybersecurity complexity
- Build a stronger foundation for future requirements
- Implement NIST SP 800-171 security practices
- Support secure collaboration with customers, suppliers & partners

Built in Microsoft GCC High as a Teams-based defended enclave, the suite establishes one secure environment where sensitive information can be managed with confidence.

Meeting organizations where they are

Every supplier begins from a different place. Some already have cybersecurity controls; others are just beginning. Exostar provides a guided approach designed to meet organizations where they are.

- 1 Understand.** Review how CUI moves throughout your organization.
- 2 Protect.** Establish a secure environment for storing, processing, and transmitting CUI.
- 3 Operate.** Implement practical NIST SP 800-171 security practices while enabling secure collaboration across the Defense Industrial Base.
- 4 Grow.** Build a cybersecurity foundation that evolves alongside future Department of Defense requirements.

WHY EXOSTAR

A trusted partner to the Defense Industrial Base

For more than twenty years, Exostar has helped organizations securely collaborate across the Defense Industrial Base. Today, Exostar combines:



Army-approved NCODE provider — a recognized participant in the U.S. Army's NCODE initiative.



A Microsoft-based defended enclave designed specifically for protecting CUI.



Deep NIST SP 800-171 expertise and secure collaboration trusted across the DIB.



Decades of experience supporting suppliers, prime contractors, and government organizations.

CUSTOMER OUTCOMES

What a secure foundation delivers

Organizations that establish a secure foundation for protecting CUI are better positioned to:



Protect sensitive information

Keep CUI inside one secure environment throughout its lifecycle.



Reduce complexity

Simplify cybersecurity operations by limiting where CUI exists.



Improve security

Support NIST SP 800-171 practices through practical operational controls.



Collaborate securely

Work confidently with customers, suppliers, subcontractors, and government.



Prepare for the future

Build a cybersecurity program that supports future Department of Defense opportunities, including initiatives such as Golden Dome.

THE BOTTOM LINE

Protect the information that protects America's future



The future of defense depends on trusted suppliers — and trusted suppliers protect CUI. Whether you're just beginning your cybersecurity journey or strengthening existing capabilities, the Exostar Cybersecurity Ready Suite is a secure, scalable foundation for protecting CUI.

[Schedule a Consultation](#)

exostar.com/cybersecurity