EXOSTAR
Together We Thrive

THOUGHT LEADERSHIP

EXECUTIVE WHITE PAPER

From supply chain to trusted community

How connected business networks are reshaping the Defense Industrial Base

An Exostar executive perspective

The Defense Industrial Base is becoming a trusted community

The Defense Industrial Base is entering a new operating era. Programs such as Golden Dome will depend on diverse ecosystems — government, primes, OEMs, commercial innovators, manufacturers, technology providers, and thousands of small and midsized suppliers.

That expansion creates opportunity, but it multiplies the identities, relationships, applications, and sensitive exchanges organizations must govern. Establishing trust one relationship at a time creates growing administrative, operational, and security burdens.

> **The DIB is evolving from a traditional supply chain into a trusted business community.**

A trusted community does not create business relationships or contracts. It provides the identity, governance, and secure collaboration foundation that lets organizations manage those relationships confidently once they exist: identity establishes who an organization or user is, governance controls access, and the community lets established trust support many approved relationships.

Trusted collaboration will become strategic infrastructure for the next generation of defense programs. Communities establish the foundation; capabilities such as AI-powered supplier discovery build upon it.

Organizations that establish trust quickly and collaborate securely will be better positioned to support mission requirements, attract partners, and respond to future opportunities.

Six conclusions for defense leaders

01.
Cybersecurity inside a single organization is no longer enough.

02.
Trust must extend across organizational boundaries.

03.
Recreating identity, onboarding, and governance for every relationship simply does not scale.

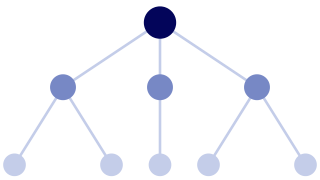
04.
Trusted communities make trust more reusable across approved relationships.

05.
The value of a trusted community increases as participation and relationships grow.

06.
Trusted collaboration will become a strategic capability for government, buyers, and suppliers alike.

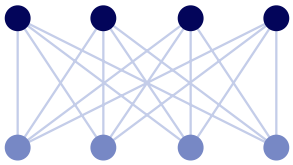
The progression

The traditional model
LINEAR & TIERED



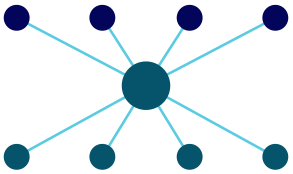
- One direction
- Tier by tier
- Limited visibility

The connected model
EVERY RELATIONSHIP FROM ZERO



- Duplicate onboarding
- Separate accounts
- Repeat questionnaires

With Exostar
TRUST ESTABLISHED ONCE



- One identity
- Governed access
- Reusable trust

From a tiered chain, to a web of relationships each rebuilt from zero, to a community where trust is established once and shared by every participant.

The Defense Industrial Base is entering a new operating era

Defense programs have always depended on supplier relationships, but the scale and nature of those relationships are changing. Future programs will draw upon established defense contractors, commercial technology companies, specialized manufacturers, engineering firms, software developers, and emerging suppliers — many with limited experience in defense cybersecurity or regulated collaboration.

Golden Dome illustrates the scale and diversity of that transformation, requiring rapid supplier participation and secure information exchange across organizational boundaries. The DIB can no longer be viewed as a linear chain supporting a prime contractor; it is becoming a connected ecosystem in which organizations serve multiple customer relationships at once.

Larger, more distributed
Defense programs span more organizations than ever.

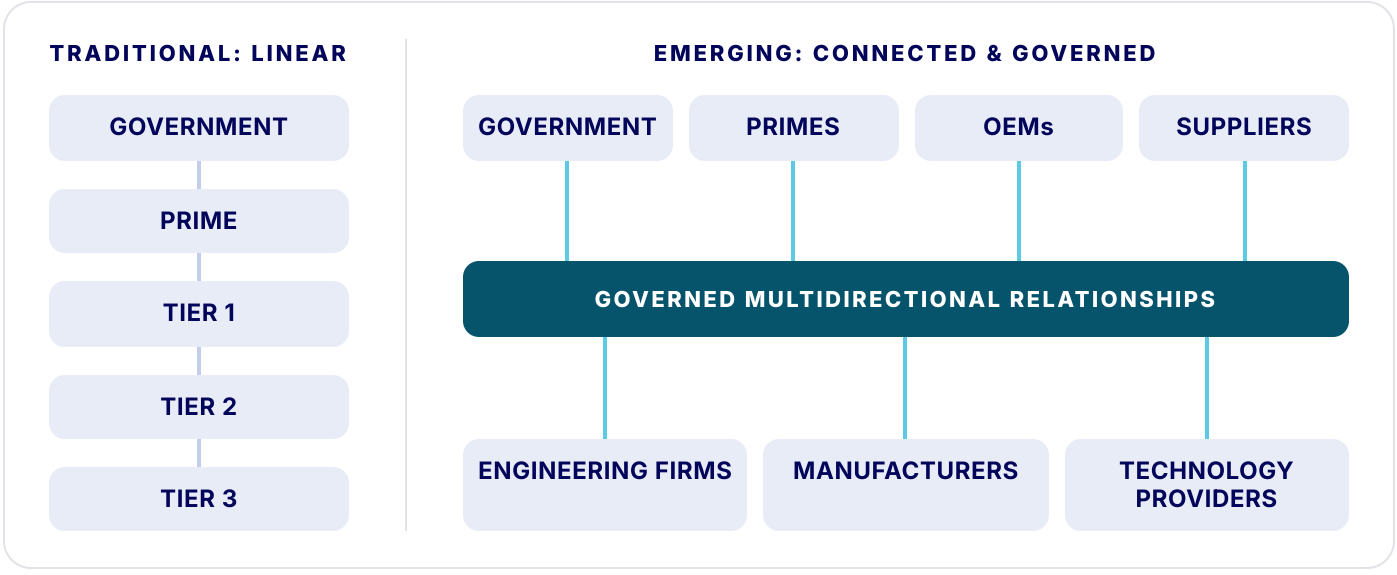
Many-to-many
Suppliers support multiple buyers and programs at once.

New entrants
Commercial innovation brings new participants into the DIB.

Ecosystem dependence
Mission success relies on collaboration across boundaries.

Digital collaboration
Digital engineering and cloud work raise cross-company interaction.

Golden Dome
A timely example of the evolving model.



Trust has become the new operating challenge

Trust is not established through individual technologies alone. It is created through the combination of verified organizations, trusted users, governed access, and consistent collaboration practices that allow organizations to confidently work together over time.

Cybersecurity discussions traditionally focus on protecting the individual enterprise — networks, endpoints, applications, users, and data. Those responsibilities remain critical, but defense programs are not executed within a single company.

Engineering teams share information with suppliers. Procurement onboards new organizations. Manufacturers exchange production and quality data. Program leaders coordinate across companies — and Controlled Unclassified Information is stored, processed, and transmitted throughout those relationships.

Six trust decisions every organization must answer

01.
Company validation
Is this company legitimate?

02.
User identity
Is this user who they claim to be?

03.
Credentials
What level of authentication is required?

04.
Authorization
What business relationship supports the request?

05.
Information access
Can sensitive information be exchanged without unmanaged risk?

06.
Ongoing governance
How will access be approved, monitored, and removed?

The challenge is no longer only securing the enterprise. It is securing and enabling the relationships between enterprises.

The hidden cost of recreating trust

Most external business relationships still begin from zero. When organizations start working together, they repeat many of the same activities: verifying companies, establishing identities, onboarding users, exchanging cybersecurity documentation, provisioning application access, and defining collaboration workflows. Each step is necessary — but repeating it for every new relationship creates growing administrative and operational complexity.

> **The Trust Tax is the administrative, operational, and security cost of re-establishing identity, onboarding, and governance for every new relationship instead of building on an existing trusted foundation.**

	VERIFY Verification & onboarding	IDENTIFY Identity & access management	ATTEST Cybersecurity questionnaires	APPROVE Manual approvals & provisioning	COLLABORATE Portals, records & environments
BUYER A	×1	×1	×1	×1	×1
BUYER B	×2	×2	×2	×2	×2
BUYER C	×3	×3	×3	×3	×3

THE TAX — Fifteen repeated efforts for one supplier and three customers — and the count grows with every added relationship.

TRADITIONAL MODEL

- Duplicate onboarding
- Separate accounts
- Repeat questionnaires
- Multiple portals

WITHIN A COMMUNITY

- One identity
- Reusable trust
- Governed access
- One environment

ON TRUST AS INFRASTRUCTURE

Trust is not a soft business concept. It is operational infrastructure that enables secure participation across the Defense Industrial Base.

Trust is becoming infrastructure

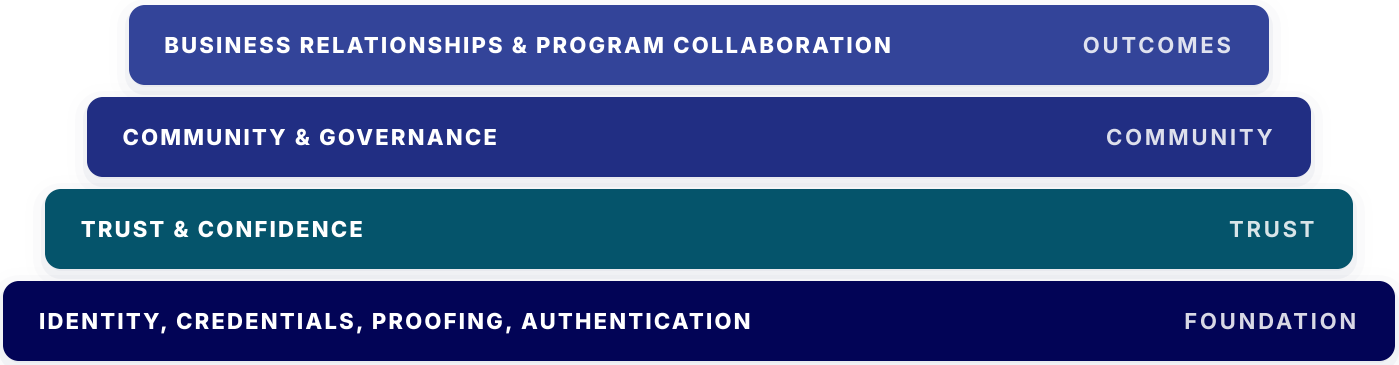
Infrastructure has traditionally meant networks, servers, cloud platforms, applications, and identity systems. As defense programs become more interconnected, trust itself must be treated as part of the operating infrastructure — the capabilities and governance needed to establish confidence in organizations and users, authorize access, support secure collaboration, and maintain those relationships over time.

Identity is foundational, but identity alone does not create a trusted business relationship. Authentication can confirm that a credential is valid; it does not establish whether the company is legitimate, whether the user represents that company, or whether a valid business relationship supports access.

The progression of trust

Identity	Confidence	Trust	Community	Business value
Who the organization and user are	Credentials, affiliation, assurance validated	Access approved on identity and business context	Trust extended across approved relationships	Faster collaboration and broader opportunity

Trust as a structural layer



EACH LAYER RESTS ON THE ONE BELOW IT

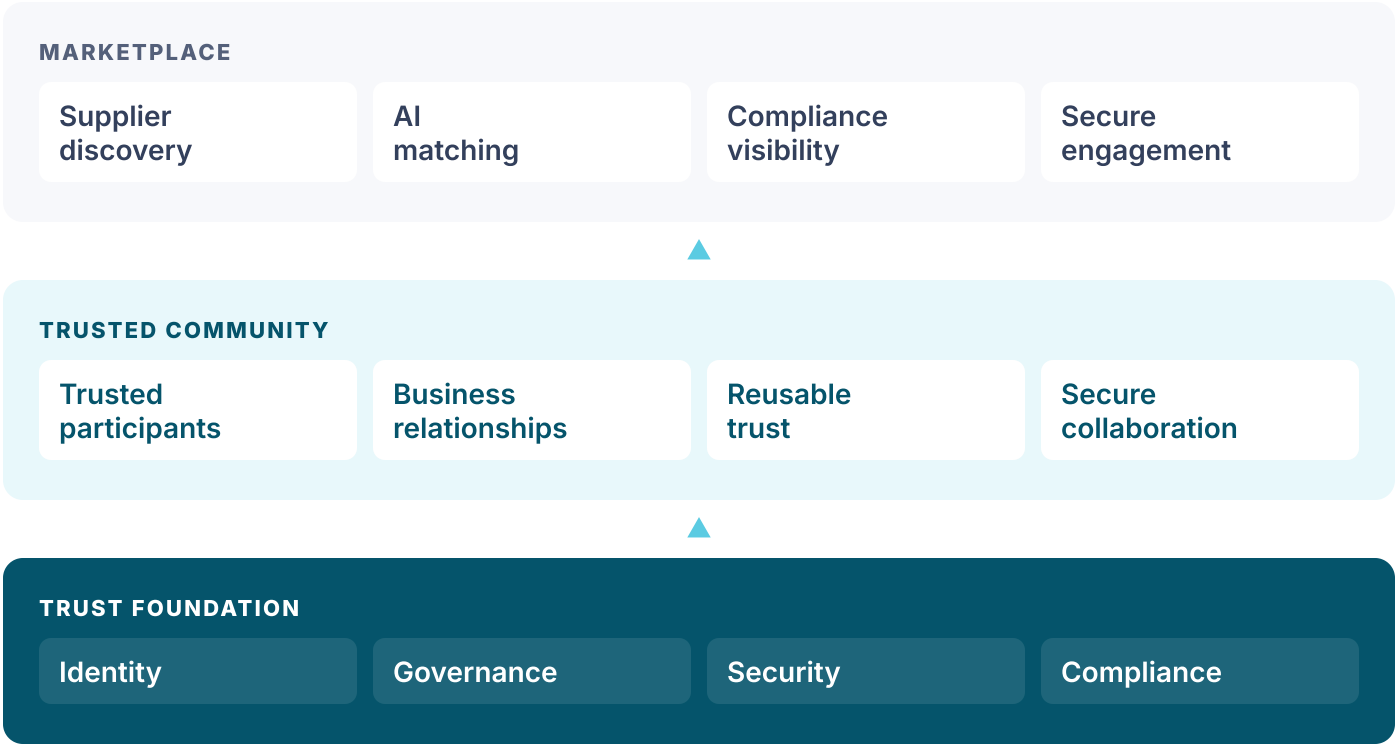
Communities do not replace individual business relationships. They create a trusted operating environment that makes future collaboration more efficient without replacing customer-specific governance or approvals.

The rise of trusted communities

Traditional point-to-point models assume every organization must establish trust independently with every customer, supplier, or partner. As defense ecosystems grow, that approach becomes difficult to sustain. Rather than recreating trust for every new relationship, organizations participate in a shared environment built on trusted identity, governance, and secure collaboration.

Each business relationship remains customer-specific and appropriately governed — but organizations begin from a stronger foundation of trust rather than starting from zero.

A layered architecture — discovery rests on trust



A trusted community is not a marketplace: the community establishes the trusted operating environment; a marketplace builds on it. Participation does not eliminate customer-specific onboarding or access decisions — it gives them a consistent starting point.

What trusted communities enable

As participation grows, so does the value of the community. Buyers benefit from a broader ecosystem of trusted organizations; suppliers participate through familiar identity, governance, and collaboration models. Instead of repeatedly recreating trust, organizations build upon an established foundation.

FOR BUYERS

Less repetitive administration, greater confidence in external participants, and simpler collaboration across increasingly complex supplier ecosystems.

FOR SUPPLIERS

Less friction, stronger credibility, and a more consistent way to participate in customer programs while maintaining governance for each relationship.

OVER TIME

Because trust is already established, the foundation extends to AI-powered supplier discovery, compliance visibility, secure messaging, and future marketplace experiences.

Characteristics of a trusted community

- Verified organizations and identity-proofed users
- Shared identity and governance framework
- Relationship-specific access and approvals
- Secure collaboration across organizational boundaries
- Connected business processes
- Ongoing lifecycle management and reusable trust

> **Organizations do not simply gain access to applications. They become trusted participants in the Defense Industrial Base.**

Twenty-five years of trusted collaboration

For more than twenty-five years, Exostar has helped government organizations, prime contractors, OEMs, suppliers, and partners establish trusted identities and securely collaborate across the Defense Industrial Base.

Organizations typically join because a customer, supplier, or partner invites them into a shared business process. Exostar enables those relationships — it does not broker them.

> **The Exostar Community is a trusted business network that enables organizations to establish, manage, and grow trusted business relationships through shared identity, governance, and secure collaboration.**

The Exostar Community ecosystem

The community is the trusted operating foundation beneath existing business relationships — not an open marketplace where every participant automatically connects with every other. Approved relationships remain governed and intentional.

Why organizations join trusted communities

Organizations participate because they need a trusted way to collaborate with customers, suppliers, partners, and government organizations that already have — or are establishing — a business relationship. The community provides the trusted foundation that allows those relationships to begin more efficiently and operate more securely.

Prime & OEM value

Primes and OEMs must coordinate large supplier ecosystems while maintaining governance and accountability. A trusted community helps them engage external organizations more confidently, reduce repetitive onboarding, govern access, and connect supplier information with collaboration and execution.

Supplier value

Suppliers must establish credibility, complete onboarding requirements, access shared applications, protect sensitive information, and support program execution. Becoming a trusted participant reduces friction, strengthens customer confidence, and provides a more consistent foundation for future relationships.

Shared community value

All participants benefit when collaboration is built upon verified organizations, governed access, familiar processes, and a shared foundation of trust. Organizations do not simply gain access to applications — they become trusted participants in the Defense Industrial Base.

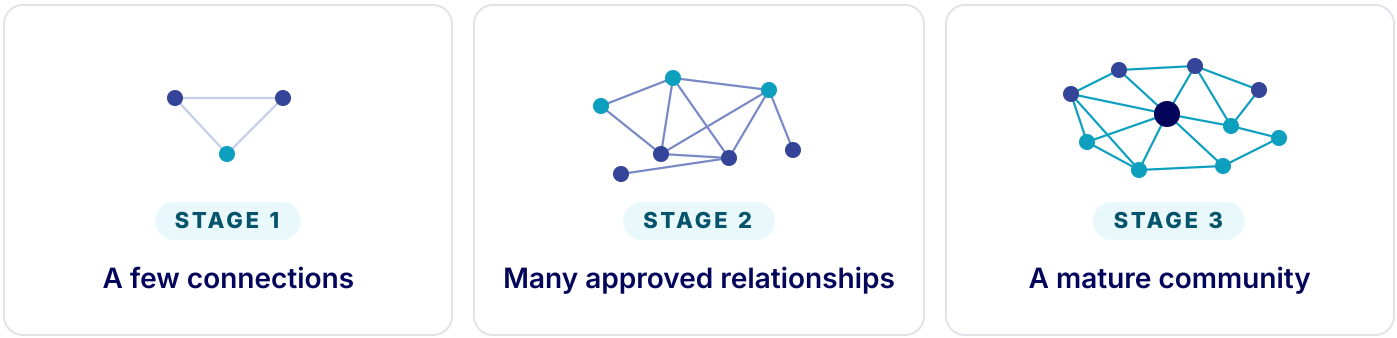
The network effect of trust

Traditional software creates value primarily through functionality. Trusted communities create value through participation. Every new trusted participant expands the number of organizations that can collaborate through familiar identity, governance, and secure business processes — so organizations spend less time establishing foundational trust and more time collaborating.

Trust remains relationship-specific and governed. Every customer continues to control its own supplier relationships, approvals, and access decisions. The network effect comes from reducing the effort required to establish trusted collaboration — not from removing governance.

The trusted collaboration flywheel

Every participant strengthens the community



As communities mature, the same foundation supports AI-powered supplier discovery, compliance visibility, secure messaging, and intelligent matching. These capabilities build upon the trusted community — they do not replace it.

Trusted collaboration across the business lifecycle

Trusted collaboration does not end once access is granted. Trust must support the full lifecycle of a business relationship — from initial identity through supplier onboarding, secure collaboration, execution, and ongoing governance — as one continuous lifecycle rather than disconnected products or processes.

01 ESTABLISH IDENTITY	Verify organizations and users, authenticate securely, and govern application access.	MAG · proofing · credential management · MFA
02 ONBOARD & ASSESS	Collect supplier information, manage cybersecurity questionnaires, and track onboarding and recertification.	Supplier Management · assessments · approvals · recertification
03 PROTECT INFORMATION	Store, process, and transmit CUI within controlled environments shared with suppliers and customers.	Managed on Microsoft 365 · Cybersecurity Ready Suite · CMMC Ready Suite
04 COORDINATE EXECUTION	Connect demand, commitments, shipments, quality, and supplier performance across boundaries.	DemandLine · SupplyLine
05 MAINTAIN TRUST	Update access, supplier records, cybersecurity information, and relationships as needs change.	Supplier discovery · compliance visibility · secure engagement

THE EXOSTAR COMMUNITY — A CONTINUOUS FOUNDATION BENEATH EVERY STAGE

Trust established at the beginning of a relationship carries through its entire lifecycle, so collaboration does not restart each time the relationship moves forward.

Government is already moving toward standardized participation

The U.S. Army's NCODE initiative illustrates a broader shift across the Defense Industrial Base. As cybersecurity expectations increase and supplier ecosystems expand, government organizations recognize that many businesses need more standardized, repeatable pathways for secure participation.

NCODE connects eligible organizations with government-contracted External Service Providers that deliver standardized cybersecurity environments and shared-responsibility models — reducing complexity while helping organizations protect Controlled Unclassified Information and support applicable DFARS and NIST SP 800-171 requirements.

A standardized path to secure participation

01 SUPPLIER IDENTIFIED
An eligible organization enters the program.

▶

02 VETTED PROVIDER
A contracted provider delivers a standardized offering.

▶

03 IMPLEMENTATION
A preconfigured environment is deployed under shared responsibility.

▶

04 SECURE PARTICIPATION
CUI is protected and the organization can participate.

Beyond cybersecurity, NCODE reflects a larger industry trend: government and industry increasingly recognize that scalable participation depends on common operating models and reusable approaches to secure collaboration. The same principles extend further. Trusted communities reduce barriers to participation, simplify collaboration, and create more consistent ways to establish trusted business relationships.

NCODE demonstrates that

- Standardized participation reduces complexity.
- Ecosystem approaches strengthen the DIB.
- Preconfigured environments accelerate readiness.
- Trusted providers improve confidence.
- Shared responsibility increases accessibility.

Strategic implications for defense leaders

The shift from isolated enterprises to trusted communities requires leaders to rethink transformation, supplier engagement, cybersecurity, and collaboration.

Government leaders	Support standardized participation models that strengthen the DIB, reduce unnecessary barriers for small businesses, and improve supplier-ecosystem resilience.
Primes & OEMs	Treat external collaboration as strategic infrastructure. Connect identity, onboarding, cybersecurity, collaboration, and execution into one consistent operating model.
Suppliers	View trust and readiness as competitive business assets. Organizations that establish trust quickly and demonstrate readiness are better positioned for future programs.
CIOs & CISOs	Expand cybersecurity thinking beyond enterprise protection. Evaluate technologies on their ability to securely support collaboration across organizational boundaries.
Supply chain & procurement	Move beyond disconnected onboarding and compliance processes. Build supplier ecosystems capable of supporting the full relationship lifecycle.

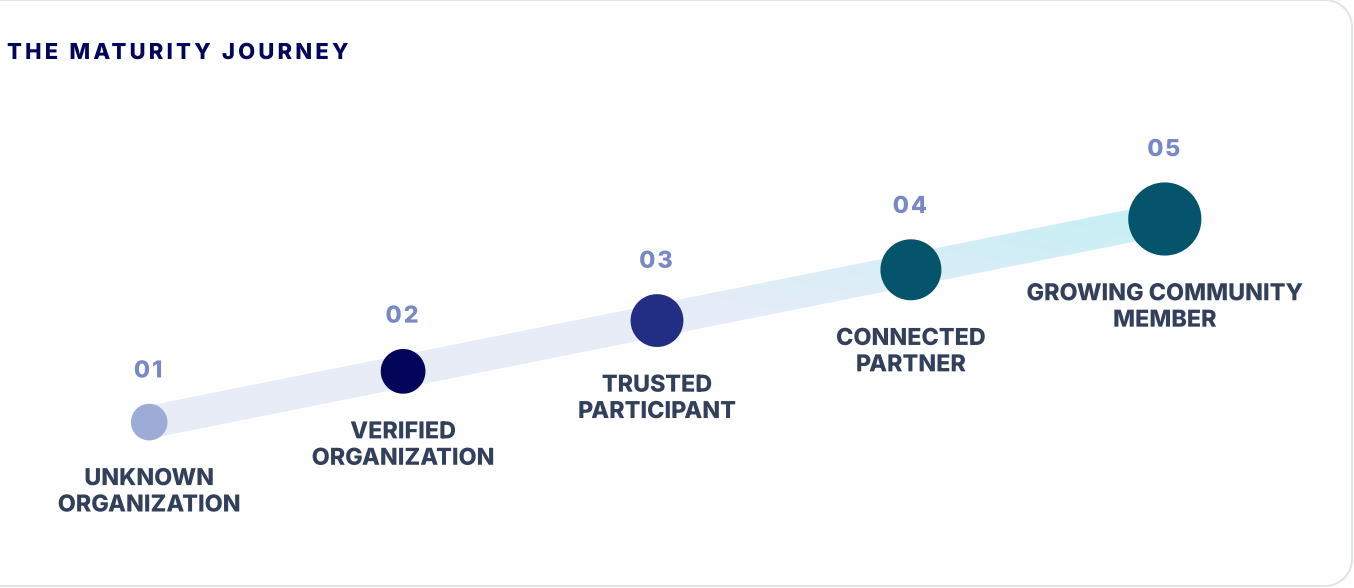
Executive questions

- How much effort is spent recreating trust for every supplier relationship?
- Are we building isolated systems or participating in a trusted ecosystem?
- Are identity, onboarding, collaboration, and execution connected — or managed independently?
- Does our operating model support the scale required for future defense programs?
- Can new suppliers become productive quickly without compromising governance?

Becoming a trusted participant

The future of defense will not be defined solely by the technologies organizations deploy. It will be defined by how effectively organizations establish trust, collaborate across company boundaries, and participate within a connected industrial ecosystem. Increasingly, competitive advantage will come from the ability to participate confidently in trusted business relationships.

Becoming a trusted participant does not replace procurement, supplier qualification, or contracting. It provides the trusted foundation that allows organizations to establish and manage those relationships more efficiently while maintaining appropriate governance.



As trusted communities grow, they enable entirely new capabilities. Supplier discovery, AI-powered matching, compliance intelligence, secure engagement, and future marketplace experiences become possible because they build upon an established foundation of trusted participants rather than isolated organizations. The community establishes the trusted operating environment; marketplace capabilities extend it.

> **The future of defense will be built on trusted relationships operating at ecosystem scale. Trusted communities provide the foundation that makes that future possible.**

THE NEXT STEP

Let’s talk about what trusted participation looks like for your organization.

An executive conversation on identity, onboarding, and secure collaboration across your supplier ecosystem.

Schedule an executive conversation

exostar.com | info@exostar.com