QUANTIFIND
THE RISK INTELLIGENCE COMPANY

Exposing Vendor Risk at Scale: Balancing Speed, Automation and Human Oversight in Procurement Security

Executive Summary

Every vendor in the defense supply chain is a potential point of infiltration for U.S. adversaries. During a briefing session hosted by Quantifind Co-Founder John Stockton, he discussed the operational hurdles of evaluating Foreign Ownership, Control and Influence (FOCI) in an increasingly complex vendor landscape.

The traditional manual processes used to vet thousands of incoming entities annually create severe bottlenecks for resource-constrained analyst teams. To counter this challenge, Quantifind has partnered with the Defense Innovation Unit (DIU) to build an AI-Enhanced Diligence Evaluation (AIDE) platform. The AIDE program introduces a scalable framework that not only compresses investigation timelines from weeks to minutes but also extends each review across an entity's wider network of associated people and companies. This whitepaper explores how the use of responsible, transparent AI and automation through platforms like Quantifind's Graphyte empowers federal agencies to conduct comprehensive, continuous vendor threat mitigation with expanded data sources and without overextending human analysts.

The Scale and Complexity of the Vendor Threat Landscape

The volume of new entrants into the defense industrial base has reached unprecedented levels. DIU alone handles hundreds of applications per project through its Commercial Solution Opening (CSO) process, examining more than 5,000 companies annually. Other Federal entities, such as the Defense Counterintelligence and Security Agency (DCSA), face even larger volumes ranging from 50,000 to 100,000 entities at its high-water mark.

Evaluating these vendors involves significant complexity because risk exists on a broad spectrum. While explicit foreign ownership thresholds are heavily regulated and relatively easy to spot, subtler vectors of control and influence are far more difficult to detect. Security leaders emphasize that adversaries systematically exploit these gray areas, injecting capital and leveraging hidden connections to obscure their involvement. Against this kind of concealment, manual verification falls short, forcing small analyst teams to assume unquantified risks during procurement cycles.

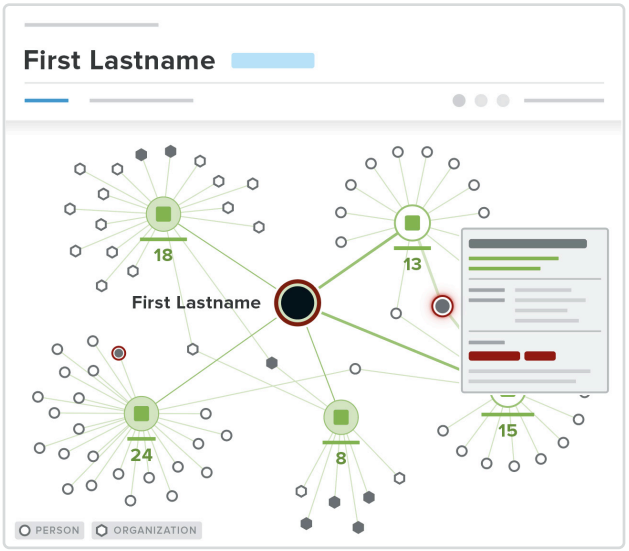
5,000+
companies screened anually by DIU

50,000+
entities screened anually by DCSA

Technical Framework for Automated Risk Detection

Effectively exposing hidden corporate risk requires shifting away from isolated data silos toward integrated, multi-source ingestion. Quantifind's Graphyte platform establishes an advanced technical baseline by combining structured and unstructured data drawn from both open-source and commercial sources:

- **Structured Data:** Ingesting global corporate registration records, international trade data, regulatory watchlists and comprehensive sanctions lists.
- **Unstructured Data:** Processing high-volume foreign language news archives, press releases and media reports to extract latent relationships that traditional databases miss.



Above: Quantifind's Relationship Network gives investigators a visual means to navigate multi-degree connections.

Using best-in-class machine learning models, Quantifind performs entity resolution and relationship extraction to synthesize these messy, disparate datasets into a coherent network. Within the Graphyte platform, analysts can visualize and explore multi-tiered corporate structures and webs of influence, identifying instances where a seemingly independent vendor is funded by foreign investment firms or state-owned enterprises.

By illuminating these layered connections rather than relying on an opaque risk score, the technology provides the objective features necessary for Government personnel to make informed risk determinations.

Operationalizing Continuous Evaluation and Mitigation

This risk landscape also means that vetting a vendor at the initial point of entry is no longer sufficient to guarantee long-term procurement security. Ongoing corporate changes, such as mergers, acquisitions and private equity adjustments, necessitate a transition to continuous evaluation models.

Implementing this at scale requires an efficient, multi-tiered screening funnel, including these capabilities being built by Quantifind for the DIU AIDE program:

High-Volume Batch Processing
Large vendor registries, such as SAM.gov, can be continuously run through automated pipelines to identify baseline anomalies and flag new risk signatures cheaply and efficiently.

Targeted Deep Search
When a new risk is identified, the system transitions to a goal-centric deep search, deploying advanced processing resources to perform first-level verification of entity data.

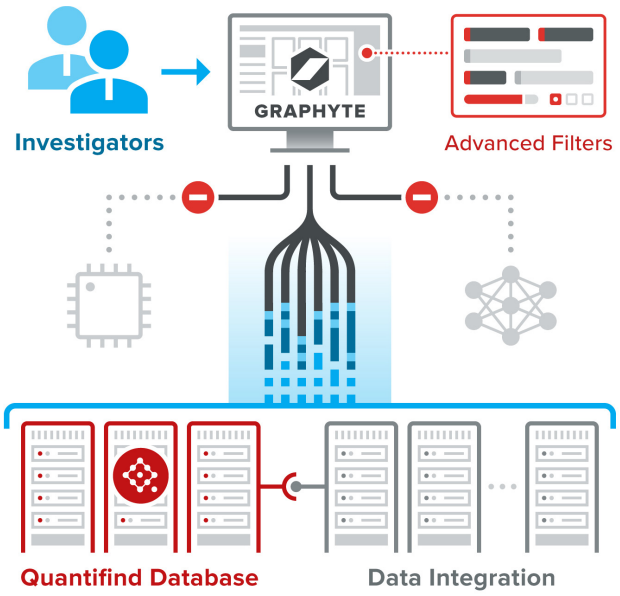
Human-in-the-Loop Triage
Human analysts review, verify, and approve concise, auditable reports generated by Large Language Models (LLMs), which summarize metadata and cluster complex findings—catching errors while maximizing overall workflow efficiency.

This structured approach changes the procurement dynamic from a strict “yes or no” bottleneck into an active mitigation process. Armed with clear, unclassified evidence drawn from Publicly Available Information (PAI) and Commercially Available Information (CAI), contracting officers can confidently negotiate security terms, restructure milestone agreements, or require the removal of adversarial capital while still successfully onboarding critical technologies.

Data Governance, Privacy and Customization

Deploying artificial intelligence within Public Sector workflows demands rigid compliance with security and privacy standards. To satisfy Federal data governance requirements, Quantifind’s underlying technology operates on a memoryless transactional architecture. Queries submitted by Government users are processed securely and are not retained or utilized to train external foundational models, preserving strict operational privacy.

Furthermore, because different Federal Agencies maintain distinct risk appetites and operational mandates, the architecture supports deep customization. Security teams can filter risk factors, adjust confidence thresholds, and select specific data integrations to match their internal policies and priorities.



Conclusion

Protecting the integrity of the defense industrial base requires an immediate shift away from slow, manual vendor vetting processes toward automated, intelligence-driven screening. The AIDE program demonstrates that combining multi-source data integration with advanced machine learning provides the speed and scale necessary to uncover complex foreign influence vectors without overwhelming human teams. By incorporating unclassified, verifiable, open-source intelligence through platforms like Quantifind, Public Sector leaders can establish a proactive, continuous risk monitoring posture that ensures secure, resilient and rapid technology acquisition.

The challenge facing acquisition organizations is no longer whether sufficient data exists to assess vendor risk—it does. The challenge is transforming that data into timely, actionable insight before a vulnerability becomes an exposure. The agencies that move now from episodic screening to continuous risk awareness will be the ones that acquire critical technology at speed without ceding ground to adversaries. The data is available and the technology is proven; what remains is the decision to implement it.