CONVERGENCE

QUANTIFIND

Vendor Vetting Recommendations: Intelligence Sharing to Expose Adversarial Capital

Edited by Quantifind and the Convergence Working Group
June 2024

On June 13, 2024, Quantifind and Deloitte hosted a second Convergence event in Arlington, VA on the topic of Adversarial Capital. Attendees included individuals from the government, financial institutions, and tech companies, all part of a larger ecosystem aimed at exposing the influence of adversarial capital in the US Defense Industrial Base and beyond.

The preceding Convergence event in March produced a whitepaper, "**A Collective Defense Against Adversarial Capital**", with recommendations centered on standards and definitions of FOCI (Foreign Ownership, Control, and Influence). This paper builds on that work and summarizes the recent event, focusing on the specific problem of intelligence sharing in the vendor vetting ecosystem. After describing the problem, we present several additional recommendations from the discussion.

Vendor Vetting Ecosystem

There are many disparate agencies and groups within the US Government concerned with vendor vetting, from innovation (SBIR, AFWERX, DIU) to acquisitions. These small, resource-limited teams are concerned with a wide variety of risks that vendors present, including financial viability, fraud, and national security threats. The threat of adversarial capital is of particular interest, including the underlying threats of over-dependence, espionage, and embedded exploits that foreign-controlled vendors may present.

While there is a strong community of individual public servants that compose this network, information sharing between them remains limited. Without sufficient sharing, the ecosystem suffers from redundant efforts and costs, missed risk signals, conflicting assessments, and situations where agencies work at cross-purposes.

A system with too many silos adds unnecessary risk, and sharing information can help mitigate the calculated risk that is eventually accepted and managed by government organizations in working with any set of non-ideal, but necessary vendor partners.

Recommendations for Effective Sharing

Here we present recommendations for an effective sharing framework, starting with an emphasis on what to avoid. Instead of an over-consolidated and over-centralized approach, we recommend a form of "loose-coupling" that effectively shares information and resources, but does not dictate a one-size-fits-all solution.

Note: These recommendations are not endorsed by any organizations who participated in the Convergence event. They are suggestions from complex conversations with multiple viewpoints. Any mistakes or misrepresentations are the authors' responsibility.

*Disclaimer: This document does not represent the formal opinions of any attending organization.

Tags: Adversarial Capital, Industrial Base Resilience, Economic Security, Insider Threats, Foreign Malign Influence

Recommendation:
Avoid a Single Risk Score

Centralizing vendor risk assessments, giving every vendor a single risk score from a single framework, is tempting but inappropriate. People who argue for this approach will use the analogy to individual or organizational credit rating systems, or even go as far as recommending methods closer to the social credit score assigned in China. There are benefits to centralization and consolidated approaches like sanctions lists are often the most effective solution to restrict access and impose policy. However, applying this approach to vendor vetting at scale (over millions of entities) fails across government agencies for the same reason that it would fail across banks or individuals: risk-based decision-making is context-dependent.

Risk appetites and postures vary widely from organization to organization. All risk frameworks will share common objective elements and considerations, but the fact remains that risk decisions are highly situation-dependent and a heavy-handed approach would severely limit the flexibility and decision-making power of individual agencies with individual missions.

Agencies need to make their own calculated risk assessments based on their constraints and guidance. In the parallel world of banking, some banks look at customers in “risky industries’’ (e.g., marijuana or cryptocurrency) as a threat, while others look at them as an opportunity. Similarly, some agencies look at a vendor’s involvement in the Russian economy as a risk, while others would look at it as a necessary precondition for their mission. Sometimes the bug (from one agency’s perspective), is the feature (to another).

Consolidation would also introduce new risks. A single shared framework invites exploitation, as companies could find loopholes to evade risk definitions the moment that they are codified. Expanding blanket bans over large vendor lists would also lead to endless lawsuits from black-listed vendors, who may not be appropriate for one mission, but perfectly suitable for another which they have the right to pursue.

Recommendation:
Share Contacts and Facts

Instead of a single risk assessment, the government should enable a framework for vendor vetting groups to share:

Contacts: Allow investigators to see if another investigator has previously investigated the same vendor. This networking would support knowledge sharing, comparison of notes, and resiliency of the overall intelligence network. The visibility could take the form of match-making, where connections between teams are only made when there is an overlap in their vendor lists, though this would require adequate entity resolution. In addition to sharing key information, the detailed knowledge of other relationships would potentially short-cut labor-intensive processes. If one agency has already taken a calculated risk on a vendor, other agencies can save time and resources by considering that decision.

Facts: Share the features, or objective attributes of vendors, that can power assessment models. Each group should have the freedom to use shared features (vendor addresses, owners, activities, etc.) in their own context-dependent models. Some groups would ignore features that other groups consider red flags. Some groups would be grateful when another group uncovered a particular data record that they had missed, providing a missing link to a foreign state owned enterprise (SOE) or another key red flag. Some degree of standardization of this “vendor feature matrix” is warranted, but individual groups should be given almost full autonomy on what to do with it. Of course, all objective statements must contain provenance on where the raw data came from so the final user can assess validity transparently and for themselves.

Reports: In some cases, it may be more pragmatic to share one agency’s final risk assessment report with another agency, either in addition to or in replacement of raw, objective data. The access to these reports should be managed by the source organization, and the responsibility of how to interpret the report and independently source the raw information should lie with the consuming agency. In essence, one agency can be used to “tip” another agency, but that does not absolve the latter from verifying all necessary information in their own assessment.

This type of scaled up sharing network would have utility even if it only facilitated gov-to-gov interactions. However, built properly, it would be relatively easy to extend the network, where appropriate, to other partners including: US allies, private sector institutions, and non-governmental organizations (NGOs) interested in fighting particular threats.

Recommendation: **Incentivize Vendor Transparency**

Vendor vetting screening should be limited to those entities who want to work with the USG. Vendors who are "open books" and disclose more information to the USG should be rewarded for their transparency with increased access to government contracts and opportunities. Companies that register for government contracts of any kind already agree to blanket terms and conditions, and any new requirements should have the same USG-wide blanket character. In other words, vendor vetting requirements should be "opt-in", and require a degree of disclosure somewhere between what it takes to be registered in the SAM.gov database and what it takes to receive a facility clearance (FCL) from DCSA.

In contrast, vendors who hide information or use obfuscation methods and shell companies to misrepresent themselves unnecessarily should be excluded from certain opportunities. In the context of FOCI and adversarial capital risk, it is difficult to measure "intent" of a particular vendor (e.g., to steal national security secrets) but it is easier to objectively show a vendor's efforts to hide certain facts or misrepresent itself ("it's not the crime but the cover-up".) The same methods that reveal false claims and fraud can be used to expose identity laundering and other efforts to hide foreign influence.

Recommendation: **Empower Vendor Cooperation**

The vendor vetting process should not be adversarial. Sometimes the government will expose risks or exposure points associated with a vendor that the vendor did not even know about. An open line of communication will help a vendor mitigate risk and, eventually, give the government more safe options for acquiring technology and services.

The government can enable the company to more effectively share information about its own partners (investors, customers, data providers). Currently, a company's partners are reluctant to reveal information (e.g., their limited partners and general partners). Clear directives and secure sharing mechanisms need to be set up that allow the USG to independently compel these partners to cooperate and share information on a need-to-know basis. These partners are likely to be compelled more by carrot (more contracts available to a portfolio company), than stick (punishments for not complying).

Recommendation: **Prioritize Open Source Data and Interoperable Workflows**

To enable the most sharing possible, priority should be placed on open source data including publicly and commercially available information (PAI, CAI). The fact that a particular vendor is being investigated is not always the highest level of sensitivity and this freedom should be leveraged to allow the most sharing as possible. In some cases, there will be sensitive high-side investigations as well and the standardized approaches recommended here should be compatible and interoperable with high-side integration, albeit in a one-way fashion.

Summary: **A Collective Effort, Individually Led**

A shared vendor vetting ecosystem should be a collective effort and no single organization should dictate or control a risk management approach for all USG entities. At the same time, leadership by individual organizations will be necessary for this collective vision to reach its potential.

Leadership will be necessary to fund a basic sharing system. Leadership will be necessary to set sharing standards. And leadership by example will be necessary to show how such a system can be used to impact existing vendor vetting workflows.

This vision represents the expansion and scaling of efforts that are already happening in pockets of excellence, albeit in overly manual ways at inconsistent levels. By following the recommendations here, the government can scale these efforts, maintain necessary flexibility, and drastically reduce the risk exposure from working with complex networks of partners.