Procurement & Supply Chain

How Top Government Security Agencies Conduct Supplier Due Diligence (& How You Should Too)

Share

Companies that contract with the U.S. government-in industries ranging from aerospace and defense to healthcare and technology-are under increased pressure to ensure their supply chains are compliant with new regulations and due diligence standards. This has traditionally been a high priority within the defense sector, as foreign affiliation, control and influence within the government's extended supply chain can pose a threat to national security.

But stricter due diligence is playing an increasingly large role in other industries as well. For example, any company contracting with the government must ensure they do not use certain

Chinese telecommunications equipment and services within their IT systems, according to a 2020 rule amending the Federal Acquisition Regulation (FAR). This is a sweeping regulation that requires comprehensive due diligence into company supply chains to ultimately secure the federal supply chain.

Having a thorough due diligence process in place not only bolsters your own company's risk mitigation strategies, but it keeps your government contracts out of hot water. This will be increasingly important in light of new laws, such as the UFLPA and Inflation Reduction Act, which prohibit goods and materials from being imported from certain regions.

We spoke with a Craft customer who is Head of Portfolio Management at a top agency within the Department of Defense to understand how they conduct due diligence.

Here are some of the key takeaways:

Key Risk & Opportunity Lenses to Track

In order to fulfill some of its core responsibilities, the agency needs to be able to access real-time intelligence on current or potential vendors and immediately surface any geostrategic or security risks they could present. Below are just a few risk and opportunity areas to track to build a comprehensive picture of your supply chain like a pro.

Risks

There are many types of risks to consider when assessing your supply chain. A robust supplier risk platform can help you identify, evaluate, and monitor these risks at scale:

Ownership

Foreign ownership and investment is a key concern for government security. As Michele Iversen, the Department of Defense's director of risk assessment and operational integration, explains:

"If the adversary is writing your code, he doesn't have to hack you to get in. We have to make sure that the adversary isn't in our supply chain."

Foreign Global Ultimate Ownership: When evaluating your supply chain, it's important to identify ownership for subsidiaries that have ultimate ownership in Nations of Concern. Ultimate beneficial ownership (UBO) means an entity owns or controls more than 25% of a company's shares or voting rights.

Nations of Concern are typically listed on one or more U.S. sanctions or international embargo lists. If one of your suppliers has a sanctioned UBO, your own operations will be in violation.

When evaluating risks, there are direct and indirect areas of concern.

Direct Nations of Concern include China, Russia, Iran, and North Korea (DPRK). Indirect Nations of Concern include nations whose economic measures are primarily dependent on Nations of Concern, such as some countries in Central America, South America, African nations, Eastern Europe, and the Baltics. While they may not be on sanctions or embargo lists, their connection to Nations of Concern ties their operations to foreign adversaries, which can put your supply chain at risk.

Foreign Investment: Foreign investment can pose similar risks to companies and national security. In a recent executive order, the Biden administration highlighted the need for a "robust foreign investment review process focused on identifying and addressing such risks."

Foreign investment from Nations of Concern is particularly important as these countries may have "a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure." Supplier intelligence can help you identify direct investment from firms or individuals that are headquartered in Nations of Concern.

Operations

Operational risks are the risks an organization faces in its day-to-day activities. There are multiple risk factors that can contribute here that are worth tracking, including:

Foreign associations: Identify different types of foreign associations within the company such as, foreign licensing, research, employment, board seats, and even talent programs. This is especially important with Nations of Direct Concern, even if they are not coming from Tier 1 suppliers.

Patents: Does the supplier have patents? Are the patents licensed outside the U.S.? How are they filing them? Where are they being held? This is a key issue since the government cannot own the IP and use filing with a research lab as mitigation.

Regulatory and Compliance Concerns: Suppliers that fail to comply with national and/or international regulations can put the business and its customers at risk. For example, if the supplier does not meet proper data security standards and experiences a breach, you may face fines and it could create risk to national security, depending on the nature of the data and the breach. Use supplier intelligence to identify current and past regulatory violations and/or governmental sanctions to surface potential red flags.

Operational Measures: Data that identifies challenges to company viability constitutes a risk to IP since long-term viability is dependent on successful operations and IP is lost when a business fails.

- **Personnel:** Personnel management and trends can be helpful indicators of a supplier's financial stability and long-term outlook. For instance, consider: Are employee numbers growing, falling, or consistent? Does the company of a robust employee infrastructure? Is employee sentiment positive or negative? High turnover rates (or strong negative sentiment), can spell danger for the long-term success of the supplier company.

- **Adverse Media**: Are there any media events that are likely to decrease the opportunities for the company or financially strain operations? Look for instances of bad press and overall reputation to understand the current and future potential for the supplier within that context.

Geography

Geography can tell you a lot about a supplier and potential risks tied to their business. Use a supplier intelligence solution to identify your vendor locations and any foreign supplier dependencies. Foreign manufacturing and revenue dependencies add risk to IP protection and offer opportunities for influence based on revenue incentives outside the U.S.

Finances

Financial risk indicators are a powerful way to get insight into a supplier's overall stability and trajectory, while further contextualizing other risk factors. This a multifaceted measure that varies between Public and Private entities:

Public: When monitoring public companies, pay attention to metrics like revenue and profitability decreases, significant leverage, loss of customers in reporting, and significant overseas revenue dependency.

Private: Monitoring private companies can be trickier since there is often less data available publicly. But pay attention to key financial metrics like the Dun & Bradstreet viability score, the D&B credit score, the D&B portfolio comparison, funding raised, and time since the last funding event.

Cybersecurity

As a leading indicator of future financial performance, cybersecurity is an increasingly important risk factor to track and measure across your supply chain. Not only does cybersecurity impact financial risk and opportunity, but as cyber attacks increase worldwide, organizations must consider their cyber risks beyond their own internal environments. This is further highlighted by the fact that 92% of U.S. organizations have experienced a breach that originated with a vendor. So even if your own cybersecurity measures are top notch, if your n-tier suppliers are less prepared, you are vulnerable.

You can use supplier intelligence that assesses the outward-facing cyber hygiene of a company to indicate the overall cyber posture of the organization as a whole.

Opportunities

Due diligence is often used to assess risk and surface potential causes for concern or disruption. But supplier intelligence can also help you determine opportunities for how your firm or division can grow with the vendor, and what type of relationship to expect.

Here a few key areas to monitor with your supplier intelligence:

Market Intelligence

Market intelligence identifies commercial market viability. How viable your suppliers' business is can inform whether you renew or expand your contracts with them. For instance, low viability constitutes a technical risk to IP as commercial revenue is often required for financial viability. Thus, IP is easily lost as a result of business failure. Use your supplier intelligence solution to better understand your suppliers' market viability and forecast opportunities.

Market Outlook & Characteristics

Total Addressable Market [TAM]: TAM helps you answer if there is a real market opportunity, and if so, what expected growth looks like. It's important to identify these long-term opportunities in the relationship, as they can inform your ability to expand into new verticals and markets with your supplier.

Market Constraints: Identify what factors are constraining the market and how they are impacting (or likely to impact) the company. The better you understand your suppliers' market constraints, the better you can work with your suppliers to innovate around these constraints and make calculated risks around those limitations.

Market Leaders: Is the company a market leader, or are they chasing the market? This helps determine how influential they are or have the potential to be in their domain of expertise.

Competitive landscape: Corporate viability is highly dependent on the ability to compete. Is the company in a highly segmented market with a number of niche players or a small fish in a pond of highly diversified, well-capitalized corporate giants?

It's crucial to use a supplier intelligence platform that can centralize all of this data for both Tier 1 suppliers and beyond. You need to be able to pull these insights on n-tier suppliers and provide customized alerts on all of these data points as needed.

Craft's supplier risk platform captures all of these data points and more to deliver clear, actionable insights on your supplier landscape. When you understand your supply chain beyond Tier 1, you can better identify and mitigate downstream risks you may have otherwise missed.