

Government Agency

Case Study

Predictive Protection for Electric Cars and Nuclear Weapons

How a government agency built assurance into its supply chain

Industry

Government

Employees & Contractors

106,000

Location

Washington, D.C.

Product

Interos

Key Benefits

- Visual representation of risk
- Continual assurance
- Integration with other SC systems
- Shareable intelligence
- Visibility into multiple vendors and vulnerabilities

“We were able to pull up their past performance and ask other customers if they were satisfied. The response was yes, and we decided to move ahead.”

—CIO

Summary

When failure is not an option

In 2012, the US Government Accountability Office (GAO) examined IT supply chain risk at the federal level, and a government agency was tasked with finding better ways to handle supply chain risk. The agency was concerned with IT components relating to national security systems, as well as the components that were actually inside nuclear weapons and other national security systems.

“We had requirements for supply chain assurance, but we didn’t have a way to evaluate if they were effective,” said the then Chief Information Officer (CIO), “We had policies, but we didn’t have a program.”

The Challenge

Specialized experience was in short supply

Supply chain risk management is a unique challenge for every organization. For the agency, it was particularly complicated due to the critical nature of its systems and the inclusion of classified, national security systems under its charge. The department required a vendor skilled in delivering against its distinctive requirements but found the necessary abilities hard to find.

First, the agency turned to the leading consulting firms. “They said they could do it, but we saw that supply chain wasn’t their real expertise,” according to the CIO. “We didn’t want to someone with no real track record to ‘figure it out’ on our critical systems.”

The agency also preferred to work with a smaller vendor who was available if a problem arose. “We needed to be able to pick up the phone and get help immediately if there was a problem, the kinds of things that could wrong for us aren’t the kinds of things that can wait till Monday.”

Then the agency found Interos, which had both previous experience and current engagements with other federal agencies. “We liked that supply chain risk management was Interos’ specialty. That’s all they think about all the time.”

The Solution

No more strangers in the supply chain

Interos applied a framework built around twelve risk factors that assessed criteria including leadership stability, foreign ownership or control issues, and supplier geography. Interos reviewed vendors, researched IT systems on request, examined who built those systems, and identified the components to expose any potential vulnerabilities.

“The framework was a big highlight for us,” said the CIO. “Interos gave us assessments across those factors, and we were able to make reasoned decisions on whether to include a certain provider in our supply chain.”

Interos was first brought into the Office of the CIO but soon became a shared service available to other programs. Vendors already doing business across the agency were also analyzed, reducing risk throughout the agency.

Today, Interos is able to visualize and model the potential impact of risk on multiple or specific vendors, products, and services. Intelligence can be integrated into other systems, so assurance is built into the entire supply chain.

“We were using the usual process: do due diligence, hope for the best, and then do more due diligence. The process was rudimentary and spotty. Once we had Interos, we had continual assurance.”

—Agency CIO

Results

“Better than anything else on the market”

Through its work with Interos, the agency was able to define security measures and improve its understanding of risk in its systems. “We got what we paid for, and it was worth it for the added assurance that it was unlikely an adversary was putting back doors in our equipment,” said the CIO.

Before engaging Interos, the agency only conducted assurance measures according to the traditional due diligence cycle—at the beginning of a supplier relationship, during a contract renewal, or when a significant event occurred.

Interos was able to deliver what the agency needed at the time and has continued to improve since. “What Interos offers today is orders of magnitude better than anything else on the market. Back then, if someone had shown me what Interos offers today, I would have called my CISO immediately and said go get this.”

About Interos

Interos Inc., (Interos.ai) located in the Washington, D.C. area, delivers transparency, knowledge, and modeled outcomes so organizations can make smarter decisions about their global connections. Interos, with AI technology, visualizes relationships, computes supply chain health, and monitors ecosystem interactions to reveal opportunities and risks. Interos serves customers in finance, aerospace, CPG, food, manufacturing, retail, technology and the government.