Bloomberg Law

Defense Contractors Will Face Higher Risks as Spending Increases

By Elizabeth D'Aunno and Erik Swabb

Jan. 25, 2023, 4:00 AM

WilmerHale attorneys Elizabeth D'Aunno and Erik Swabb warn that with increased spending on US defense, government contractors must elevate compliance as a top priority to avoid enforcement actions.

Bloomberg Law News 2023-01-25T14:16:02183890682-05:00

Defense Contractors Will Face Higher Risks as Spending Increases

2023-01-25T04:00:24000-05:00

Ongoing geopolitical developments such as Russia's war in Ukraine and tensions between China and Taiwan have continued to fuel higher US military spending.

The demand for military weapons is the strongest it has been in years, with historic investments by US allies and partners, and record US national defense funding that jumped by $76 billion to $858 billion for fiscal year 2023. This includes $816.7 billion specifically for the Pentagon.

President Joe Biden signed the National Defense Authorization Act into law in late December, targeting defense readiness across the board, including shipbuilding and aircraft, as well as munitions and military exercises around the world.

For government defense contractors, accelerated spending, strict regulatory requirements, and motivated regulators bring elevated enforcement risk.

Increasing Procurement Speed

Government customers are spending at record levels, and they are also looking to procure at lightning speed.

US officials are pressing the defense industry to boost production rates and are also using various tools to accelerate acquisition timelines. This includes the use of undefinitized contract actions, where terms, specifications, or price are not agreed upon before the contractor's performance begins. IDIQs, known as indefinite delivery/indefinite quantity contracts, are also being used.

Last fall, Under Secretary of Defense for Acquisition and Sustainment William LaPlante said the US is "committed to getting things on contract as quickly as possible, ultimately to send that clear and persistent demand signal to our partners in industry."

Walking a Regulatory Tightrope

Rapid expansion of supply chains to accommodate increased demand for defense items comes with serious compliance risks.

Defense contractors stepping up to meet this accelerated procurement face the challenge of delivering faster, while the government scrutinizes their adherence to regulatory requirements intended to enhance supply chain security and cybersecurity.

Navigating new regulatory requirements in these spaces will be burdensome. For example, suppliers whose contracts are subject to the Buy American Act must now meet elevated domestic content thresholds for domestic end products. And recent acquisition rules now require disclosing work performed in China on certain Department of Defense contracts.

Contractors will also have to comply with the safeguards set forth in the new Cybersecurity Maturity Model Certification 2.0 program, expected to go into effect this year.

The federal government has also signaled greater consequences for noncompliance. For example, the Department of Justice has opened numerous investigations and announced recoveries under its Civil Cyber-Fraud Initiative, seeking to hold contractors liable under the False Claims Act for certain cybersecurity failures.

Motivated Regulators

The Covid-19 pandemic reminded US regulators that rapid increased government spending usually attracts more fraud. Likewise, the Pentagon learned the hard way from the wars in Afghanistan and Iraq that big government spending quickly draws fraud.

Officials are determined to apply those lessons to Russia's war in Ukraine, for which Washington has already committed more than $26 billion in security assistance since Russia's invasion.

The DOD has said its focus on oversight runs the gamut of government contracting fraud, including procurement collusion, involvement of suspended or debarred contractors, submission of defectively priced proposals, and inadequate records management.

The inspectors general for the DOD, the Department of State, and the US Agency for International Development are particularly motivated to combat fraud in US assistance to Ukraine. This could assuage concerns on Capitol Hill, where Republicans have pushed for more oversight of that effort.

Some in Congress have proposed creating a special inspector general, similar to the special inspectors general established for the Iraq and Afghanistan wars. That would intrude upon the missions of the OIGs for the DOD, DOS, and USAID and potentially divert resources from them.

As a result, these OIGs are highly incentivized to investigate fraud and pursue enforcement actions.

Taking Preventive Action

Fortunately, government contractors can take preventive action to help mitigate this heightened enforcement risk.

First, they can conduct a health check of compliance programs. A targeted review can look at components such as corporate culture, roles of key personnel, policies and procedures, employee training, internal reporting channels, and recordkeeping practices.

Also, a contractor can review a specific program or function, such as supply chain or cybersecurity, that may be at greater risk of noncompliance and/or external scrutiny.

An ounce of prevention is worth a pound of cure.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners. Write for Us: Author Guidelines

Author Information

Elizabeth D'Aunno is a counsel in WilmerHale's defense, national security, and government contracts practice. She advises clients in complex investigations and enforcement actions related to government contracts.

Erik Swabb is a partner at WilmerHale. He represents defense companies and other government contractors in high-stakes investigations, regulatory matters, and other challenges. He previously served as general counsel of the Senate Armed Services Committee.