wiley

ALERT

Defense Contractors Likely Target of Increased Scrutiny Under New Administration

January 21, 2025

Secretary of Defense nominee Pete Hegseth testified during his confirmation hearing on January 14, 2025, that if confirmed*, he intends to use audits to identify potential waste and abuse in defense spending, explaining that he sees audits as a "strategic prerogative" of the Defense Secretary. Hegseth's testimony aligns closely with other messaging coming from the incoming Administration, which has signaled an intention to focus on perceived government bloat and wasteful spending.

Given that defense spending accounts for approximately 60% of all government-wide contract spending, defense contracts could be a target for significant oversight under the new Administration. Accordingly, defense contractors should prepare for a potential increase in the intensity and volume of oversight, which may come from multiple directions, including federal agencies, agency-contracted third parties, agency offices of inspectors general (OIGs), and Congress.

A likely focus of that oversight will be defense contract management – i.e., whether the U.S. Department of Defense (DOD) is properly managing its contract and grant awards to ensure financial accountability and mitigate the risks of fraud or misuse. While much of this oversight will, at least nominally, be focused on the Department's activities, oversight work like this can have a significant downstream impact on defense contractors and their subcontractors and suppliers, whose performance is often evaluated as part of the audit process and who may find themselves featured (at times, unfavorably) in public reporting.

Authors

Diana R. Shaw
Partner
202.719.3379
dshaw@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Government Contractors & Grantees

Government Contracts

Oversight, Investigations & White Collar Enforcement

White Collar Defense & Government Investigations

Another likely focus of oversight will be contractor and supplier compliance with government cybersecurity requirements, particularly for those within or supporting the defense industrial base. The federal government has become increasingly concerned about possible risks and vulnerabilities in contractor and vendor cybersecurity, including the potential for data breaches, nation state intrusions into sensitive networks, and other cyber risks. There are a variety of obligations that impose varied burdens on contractors, and the government has increasingly worked to shift the burden to contractors to mitigate risk through a series of cybersecurity requirements and related enforcement mechanisms, including in recent Executive Orders and use of the False Claims Act.

Government-directed oversight in the coming year will target this issue. In fact, DOD OIG has identified addressing the continued cyber threats targeted at contractors within the U.S. defense industrial base as critical to protecting defense critical infrastructure and has already announced multiple audits in 2025 focused on cybersecurity issues.

There are several steps that government contractors can take now to begin to prepare for a potential uptick in government audits and other oversight over the next year. If, for instance, your organization has been audited before, review past audit findings to identify trends, themes, and recurring risk areas; similarly, evaluate progress made on any prior audit recommendations and, to the extent possible, wrap up corrective actions that are close to crossing the finish line.

Consider undertaking a proactive self-assessment or internal pre-audit to evaluate your programs, operations, and performance against the likely criteria you would be evaluated under in a government audit, using a risk-based approach to identify which programs or operational units to target first. A self-assessment can be tailored to risk and budget needs, and ideally would be performed under attorney-client privilege.

And, of course, get your documents in order. Good recordkeeping is often half the battle in a government audit – government auditors can get sidetracked by the lack of documentation of performance even in instances when actual performance was stellar. Records need to be thorough, complete, clear, well-organized, and accessible. Use this time to complete and organize your files.

Finally, not all oversight is the same or has the same implications. An OIG audit, for example, is entirely different, and should be handled differently, than a congressional investigation. If you receive a notice or inquiry suggesting that your company is going to be involved in some form of oversight, it is imperative that you seek additional information to understand, among other things, what entity is directing the oversight, what type of oversight is being conducted and under what evaluative standards, and what your entity's role or posture is in the proceedings.

For more information about the topics discussed in this alert, please contact the authors.

**Hegseth's nomination was voted out of the Senate Armed Services Committee on January 20, 2025, and will now proceed to the Senate floor for a vote.*