Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Top 4 Gov't Contracting Policies Of 2024: Midyear Report

By **Daniel Wilson**

Law360 (August 9, 2024, 9:52 PM EDT) -- Federal agencies have made several prominent policy moves affecting contractors this year, headlined by programs incentivizing whistleblowers to come forward with information about contracting fraud, tweaks to a wide-ranging cybersecurity standard, and guidance for how agencies should purchase generative software.

Here, Law360 examines four significant policy changes from the first half of 2024 that will affect government contractors.

Generative Tools Guidance Recognizes Technology's Growth

Released in April and stemming from an October executive order acknowledging significant growth in the use of so-called artificial intelligence over the past few years, the General Services Administration issued guidance for "responsibly and effectively" buying generative software and related hardware.

Generative tools, also known as large language models, use algorithms to produce content such as text or video, and the guidance suggests considerations for federal acquisition staff to take into account, such as the specific problem an agency is trying to solve and whether a different solution is more appropriate.

It also directs agencies to ensure existing acquisition requirements, such as domestic sourcing and cybersecurity rules, are followed and suggests potential existing acquisition vehicles to use, but isn't completely comprehensive or prescriptive in accounting for issues such as potential risks or inappropriate use cases.

Offering that flexibility was a reasonable approach for the GSA to take, particularly because "AI governance is incredibly specific to the end use," said Eric Ransom, a Crowell & Moring LLP partner and former in-house counsel at Scale AI.

"I love that GSA is not being prescriptive at this point, it's just offering some really approachable resources that, I think, recognize a lot of the important points," he said. "First, AI is about solving problems. It's about that end use. It's not about just buying some capability in a vacuum."

Sustainability Rule Closes Loophole

The Federal Acquisition Regulatory Council finalized a rule in April that puts teeth into a long-standing requirement for federal agencies to make environmentally friendly purchases.

Under the rule, agencies must make sure their purchases use sustainable products and services, such as water- and energy-efficient products or products made with recovered materials, "to the maximum extent practicable," with limited exceptions, such as when purchasing weapons or when sustainable products are significantly more expensive than alternatives.

Before the sustainability rule, the Federal Acquisition Regulation had already directed agencies to use sustainable products and services in 95% of its new contract actions.

However, that 95% standard lacked a reporting mechanism and was vague enough for agencies to easily skirt the requirement, attorneys told Law360 when the rule was released.

The new rule instead requires agencies to formally justify a decision not to buy sustainable items, creating a clearer standard for agencies to comply with and contractors to try to enforce through bid protests.

DOJ Immunizes Self-Disclosure of Corporate Wrongdoing

A U.S. Department of Justice pilot program giving people credit for disclosing information on corporate criminal misconduct they are involved in, although not limited to contractors' employees, specifically calls out contract fraud as an area where the DOJ wants whistleblowers to come forward.

The pilot, introduced in April, offers nonprosecution agreements to individuals involved in certain types of criminal corporate wrongdoing who voluntarily and completely disclose related nonpublic information to the DOJ, as long they aren't the company's CEO or chief financial officer or the leader of the criminal scheme, and agree to fully cooperate with prosecutors and forfeit any related profits.

One of the types of offenses called out by the DOJ is "fraud against, or the deception of, the United States in connection with federally funded contracting." The program joins a similar DOJ program announced in March and officially launched earlier this month, offering financial incentives for company whistleblowers who report corporate wrongdoing they aren't involved in.

With the huge amounts of federal funding made available through infrastructure, COVID-19 relief and other similar legislation in recent years, it is not only traditional government contractors who need to be aware of the self-disclosure and whistleblower programs, said Amy Hoang, co-chair of Seyfarth Shaw LLP's government contracts practice group.

"With the influx of infrastructure dollars to state and local construction projects ... you're seeing a whole new class of players that are accepting federal dollars, and therefore opening themselves up to these enforcement mechanisms," she said.

NIST Tweaks Cybersecurity Standard

After a raft of new cybersecurity policies in 2023 amid a series of high-profile data breaches, federal agencies have continued to introduce new cybersecurity requirements this year, most prominently an update to the National Institute of Standards and Technology's guidelines for protecting sensitive federal information.

NIST's Special Publication 800-171 provides guidelines for protecting the confidentiality of federally controlled unclassified information, or CUI, stored or processed outside the government. The new version is the third revision of the guidance, intended to give organizations doing business with the government "clearer, more straightforward guidance for protecting the sensitive data they handle," NIST said.

The agency reduced the number of CUI security controls to 97, down from 110 in the previous version, and allowed for the use of "organization-defined parameters," letting agencies tweak certain requirements to meet their needs, such as whether contractors can allow remote access to systems containing agency CUI.

The guidance underpins several federal cybersecurity requirements, highlighting that cybersecurity compliance is a complicated process where contractors have to be aware of all related policies across multiple agencies, said Crowell & Moring LLP counsel Michael Gruden, a cybersecurity specialist.

"There really is no operating in a vacuum when it comes to cybersecurity safeguarding or regulation," he said. "Even if agencies are thinking that they're operating independently, it's unavoidable that these various regimes are going to intersect, and there's going to be a reckoning with how to harmonize them and how to integrate the various compliance regimes together."

--Editing by Brian Baresch and Drashti Mehta.
