wiley

NEWSLETTER

Government Contract Trends as 2021 Winds Down

October 2021

It is hard to believe 2021 is in the back stretch. At the beginning of the year, we made predictions of what might come from the change in Administration in 2021. In this article, we take a look at what has happened in 2021 and what lies ahead in 2022.

Supply Chain Disruptions Take Center Stage

The massive worldwide shortages of semiconductor chips, manufacturing equipment, and a range of consumer goods is about to get worse, and will have a direct impact on government contractors. U.S. and global businesses are struggling—*and competing*—for access to finished goods as well as the raw materials and semi-finished components that are needed to manufacture those goods. Not only has overseas supplier output decreased due to temporary plant slowdowns or shutdowns (for a variety of reasons, including COVID-19 illnesses and inadequate power), but international shippers are further reducing (and in some cases eliminating) global supply as they cherry-pick the types of cargo to transport in order to maximize profit, disfavoring containers with heavier and hazardous product in favor of cheaper ones that cost less to carry. The United States' resulting inflation rate of 5.2% is the highest level since 2008 and double the century average of 2.2%. Inflation will likely carry over into next year and will likely be exacerbated by soaring energy costs. In light of these problems, nearly 70% of businesses now believe supply chains have become too global and need to become more regionalized.

Of course, the 2020 pandemic initially sounded worldwide alarms on supply chain vulnerabilities, and prompted a U.S. government initiative to resolve potential points of failure through a whole-of-

Authors

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Practice Areas

Bid Protests
Build America, Buy America
Buy American and Trade Agreements Acts
Civil Fraud, False Claims, *Qui Tam* and Whistleblower Actions
Cybersecurity
Environment & Product Regulation
Government Contracts
Internal Investigations and False Claims Act
Privacy, Cyber & Data Governance
Strategic Competition & Supply Chain

government strategy. This effort continued into the Biden Administration and led to President Biden's February 24, 2021 "Executive Order on America's Supply Chains," which aims to "strengthen the resilience of America's supply chains." The Order set forth two lines of effort. The first was for federal agencies to complete a targeted, 100-day review of supply chains in four key sectors: semiconductors, high-capacity batteries, active pharmaceutical ingredients, and critical minerals. The second directed agencies to conduct a one-year, comprehensive review of a broader range of sectors, including the defense industrial base; the public health and biological preparedness industrial base; the information and communications technology (ICT) industrial base; the energy sector industrial base; the transportation industrial base; and supply chains for agricultural commodities and food production.

The Administration completed its first 100-day review on June 4, 2021, and on June 8, 2021, President Biden announced the launch of a new Supply Chain Disruptions Task Force led by the Secretaries of Commerce, Transportation, and Agriculture. The purpose of the Task Force is to "focus on areas where a mismatch between supply and demand has been evident: homebuilding and construction, semiconductors, transportation, and agriculture and food." Along with the establishment of the Task Force, the Administration published a lengthy 250-page report that listed recommendations for government action to onshore critical supply chains. Its recommendations included the use of incentives to encourage the domestic growth of the semiconductor, battery, pharmaceutical, and mineral industries through U.S. government grants and loans, research and development (R&D) private-public partnerships, and improved supply chain integration with allies and partners.

In furtherance of this effort, the U.S. Department of Commerce issued last month a formal public request for information concerning specific risks that businesses encounter as a result of the highly globalized semiconductor supply chain, and additionally announced a virtual forum to discuss risks in the information and communications technology and services (ITCS) supply chain.[1] The U.S. Department of Defense (DoD) has similarly launched a supply chain working group to address vulnerabilities in the defense industrial base, and is now looking to augment the agency's and federal government's overall supply chain data and information gathering capabilities to promote better transparency and improve resiliency.

While these initiatives are in their nascent stages, and as federal agencies are still undertaking their one-year industry studies, American businesses continue to struggle with real and very difficult supply chain challenges. Current shortages continue to constrain operations and will continue in severity for the foreseeable future. For most industries, the focus right now is to maintain cash flow and output as best as possible, manage business relationships, and mitigate legal liability resulting from supply and purchase contracts.

To the extent that challenges persist in the near-term, federal government intervention may be necessary. In fact, it is important that companies avail themselves of opportunities to engage and share their perspectives with the U.S. government in order to drive the development of solutions that advance their individual business objectives while also promoting broader economic growth opportunities.

In the medium-term, these specific supply chain and inflationary problems will subside, but the reality is that the business community has changed forever. Businesses will depend much more heavily on regional supply chains, pursue greater diversity in their global supply chains, adopt longer-term inventory management systems, and develop more fortified business contracts to better manage risks in the event of future disruptions. Even though supply chain shocks can never be fully eliminated, resilient business strategies supported by sound government policies may better mitigate the impact of these shocks.

Congressional interest in supply chain issues within the defense industrial base also continues. The House-passed version of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022, H.R. 4350, includes several provisions aimed at shoring up the supply chain for critical defense items. It would require the Department of Defense to consolidate supply chain risk information gathered across the Department to enable Department-wide risk assessments and mitigation strategies, as well as to develop and implement a plan to work with private sector companies to reduce reliance on foreign adversaries for certain essential supplies and materials.

Finally, Congress and the Executive branch are turning to domestic content requirements for government contracts as another means of addressing supply chain issues. As we previously reported (here and here), the Administration is pursuing several Made in America initiatives that affect government contractors, including directing the Federal Acquisition Regulatory (FAR) Council to increase the domestic content requirements under the Buy American Act and establishing a Made in America Office (MIAO) that will review all requests for waivers of Made in America Laws. In October 2021, the Office launched its website madeinamerica.gov, which will eventually provide public access to those waivers. The Senate-passed infrastructure bill, H.R. 3684, also would codify in statute many of the provisions of President Biden's Made in America Executive Order, such as additional agency-wide guidance on waivers and the establishment of the MIAO and its public website. The House version of the FY22 NDAA would also increase the domestic content requirements for materials procured in support of major defense acquisition programs.

Cybersecurity Will Continue As A Priority

For the foreseeable future, increased cybersecurity requirements and, in particular, cyber incident disclosure requirements will remain a trend. What remains a huge open question is the status of the DoD Cybersecurity Maturity Model Certification (CMMC) program. The concept of CMMC was included in an interim Defense Federal Acquisition Regulation Supplement (DFARS) rule in September 2020, but DoD began a review of the program in March 2021. In May 2021, the Senate Armed Services Committee's Subcommittee on Cybersecurity held a hearing on cybersecurity in the Defense Industrial Base at which testimony suggested the CMMC review and the final DFARS rule would be delayed. That review and the increased delay was likely exacerbated by the Biden Administration's Executive Order on Improving the Nation's Cybersecurity, EO 14028. In September 2021, three industry organizations sent a letter to Deputy Secretary of Defense Kathleen Hicks expressing concern with the continuing uncertainty and lack of transparency into DoD's review. Furthermore, the small business community has expressed concerns with CMMC's impact on them and urged DoD to identify ways to provide more flexibility to alleviate that impact. A media report in September 2021 stated that DoD anticipated wrapping up its review by the end of this year. As of this newsletter, the DoD review is

ongoing, a final DFARS rule has not been issued, the Government Accountability Office's (GAO's) report on CMMC has not been issued, and EO 14028 awaits implementation. Although much remains unclear, it appears that if CMMC reemerges, it will likely be in a different form.

Cybersecurity also remains a focus in Congress. In response to recent hacking and ransomware incidents, Congress appears poised to implement a mandatory cyber incident reporting requirement for companies that own or operate critical infrastructure and possibly a broader cross-section of companies. The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection and Innovation and the Senate Homeland Security and Governmental Affairs Committee have held hearings on the issue in 2021, and multiple bills have been introduced to require entities to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS). Those bills differ in the breadth of entities that would be required to report cyber incidents to CISA and when they would have to make those reports. For example, the House version of the FY22 NDAA would require CISA to issue incident reporting regulations for entities that own or operate critical infrastructure, with reports required no ***sooner*** than 72 hours after confirmation that a covered cybersecurity incident has occurred. The Senate Homeland Security Committee approved the Cyber Incident Reporting Act of 2021, S. 2875, which similarly would require entities that own or operate critical infrastructure to report cyber incidents, but do so ***within*** 72 hours after an entity reasonably believes a cyber incident has occurred. Both bills also would establish a Cyber Incident Review Office within CISA to receive and evaluate such reports, among other responsibilities. Members of the Senate Intelligence Committee endorsed a broader, more expedited reporting requirement in S. 2407, the Cyber Incident Notification Act of 2021. That bill includes a ***24-hour reporting requirement*** that would apply to federal contractors, agencies, and cybersecurity service providers, in addition to the critical infrastructure providers that would be covered by the House NDAA and Senate Homeland Security bills. All sides appear to be working to include some sort of a reporting requirement in the final version of the NDAA that is expected to be passed by Congress and signed into law later this year.

The Senate Homeland Security Committee also approved the Federal Information Security Modernization Act of 2021, S. 2902, to update the Federal Information Security Modernization Act (FISMA) of 2014 and improve cybersecurity practices and requirements within federal government agencies. The bill includes provisions to improve cybersecurity coordination within the government and between the government and its contractors, require enhanced security protections for government information systems and the sensitive data they store and require agencies to notify individuals when their information is compromised.

Consistent with these efforts in Congress, the Federal Chief Information Security Officer has announced that the Office of Management and Budget and Department of Homeland Security have developed recommendations for new contract clauses to be included in government contracts to improve and enhance information sharing between the Government and contractors regarding cyber threats and incidents.

Bid Protests Trends and Numbers

Our group routinely conducts data analytics on protests filed at GAO, in particular, and at the Court of Federal Claims. On the GAO bid protest front, FY 2021 continued a five-year trend of a sustained reduction in the number of GAO bid protests, dropping by a fairly sizable margin. In the first year we began independently tracking protest data (FY2016), GAO received 2201 bid protests. (As we've explained before, our figures differ from those reported by GAO because we track only initial protests filed, rather than all docket entries, known as "B-numbers," issued, which would include supplemental protests and multiple protests under a common solicitation). The largest drop since FY16 came in FY19, when protests dropped 17.5% (from 2,023 in FY2018 to 1,668 in FY2019). After only a slight drop of less than 2% in FY2019 and FY2020, FY2021 experienced a 12.8% drop. The numbers alone do not identify the difference, of course. Although COVID-19 may have been a factor, we doubt that it played that significant of a role in these trends. After all, this is a continuing trend: protests have decreased in each of the last five years. During those five years, we have seen a number of changes at GAO. For example, GAO suspended Latvian Connections after the firm filed 150 protests in FY2016 alone. The threshold for protests of DoD task orders increased, and DoD implemented its enhanced debriefing process that is intended to reduce protests. And, with the implementation of GAO's Electronic Protest Docketing System (EPDS), GAO also implemented a filing fee for all protests.

We also keep a close eye on GAO's sustain rate. Because GAO has not yet decided all protests filed in FY2021, the numbers below are based on the fiscal year each protest was decided. Looking solely at the initial protests where GAO issued a decision on the merits (in other words, GAO sustained or denied the protest), GAO's sustain rate for protests that it decided in FY2021 was 12.7%. This is a decrease from both the previous year (13.8%), and GAO's average over the last six years (13.4%). One trend remains fairly constant, however: the difference in sustain rates depending on whether a protester files a supplemental protest. Where the protester filed only an initial protest, GAO's sustain rate for merits decisions in FY2021 was 7.8%. But where the protester filed one or more supplemental protests, that figure increased to 17.1%.

We also track protests filed at the Court of Federal Claims. The numbers are a bit rougher here because the court can consolidate cases. But, based on our analysis, we do not see the same pattern of year-over-year drops in protests at the court. The number of protests fluctuates each year, with a low of approximately 113 in FY2016 and a high of approximately 171 in FY2018. In FY2021, there appear to be more protests filed at the court than in FY2020 (140 in FY2021 vs. 120 in FY2020). One reason protesters might be turning to the court, including after protesting to GAO, is the opportunity for a more fulsome record. *See Oak Grove Techs., Inc. v. United States*, No. 21-775C, 2021 WL 3627111 at *11-13 & nn. 13-14 (Fed. Cl. Aug. 2, 2021) (citing K. Sacilotto & J. Frazee, *Is a Record by Any Other Name Still a Record?*, at *1 (American Bar Association 2021 Public Contract Law Virtual Federal Procurement Institute Mar. 12, 2021)).

Enforcement Trends

Perhaps not surprisingly, we anticipate a robust enforcement environment in the procurement space on the False Claims Act (FCA) front. Not including health care cases, in September and October alone, the U.S. Department of Justice (DoJ) has issued press releases on settlements in several FCA cases involving federal contractors and procurement contracts. *See, e.g.,* Press Releases involving a $4.5 million settlement to resolve FCA lawsuit for non-compliance with military specifications; a $1 million settlement to resolve overcharging

allegations; and a $6.15 million settlement of a FCA claim that energy company underpaid royalties for gas on federal lands. Further, DoJ has reversed some Trump-era policies that were perceived as more defendant-friendly, including two memoranda that restricted reliance on agency guidance documents for FCA enforcement actions. Senator Grassley (R-IA), the Ranking Member of the Senate Judiciary Committee, continues to advocate tightening the FCA, including to address the Supreme Court's decision in *Universal Health Servs. v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2016).

In a further FCA enforcement development, earlier in 2021, DoJ's Civil Division stated that cybersecurity was among its FCA enforcement priorities. Consistent with that announcement, on October 6, 2021, DoJ announced the launch of its Civil Cyber-Fraud Initiative. According to DoJ, "[t]he Civil Cyber-Fraud Initiative will utilize the [FCA] Act to pursue cybersecurity related fraud by government contractors and grant recipients." DoJ announced that its Initiative will focus on entities or individuals that put U.S. information or systems at risk by "knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches." Thus, the DoJ initiative mirrors efforts in Congress to increase and improve reporting of cybersecurity incidents. The benefits of this Initiative, according to the agency, include, among other things, "[h]olding contractors and grantees to their commitments to protect government information and infrastructure"; "[e]nsuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage"; and "[r]eimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations."

On October 13, 2021, DoJ discussed this Initiative further at a CISA cybersecurity summit. Notably, DoJ emphasized the importance of its reliance on whistleblowers, stating that "we expect whistleblowers to play a significant role in bringing to light knowing failures and misconduct in the cyber arena." DoJ also elaborated on "three common cybersecurity failures" that it characterized as "prime candidates" for potential FCA enforcement: (1) knowing failures to comply with cybersecurity standards, such as the cybersecurity terms in a procurement contract or grant, such as protection of government data, restriction on non-U.S. citizens accessing systems, or avoiding use of components manufactured by certain foreign companies; (2) knowing misrepresentation of security controls, such as misrepresentations regarding systems security plans or monitoring practices; and (3) knowing failure to timely report suspected breaches. And, DoJ has appointed a Chairperson within the Civil Division's Fraud Section to lead the Initiative, and it is partnering with agency Offices of Inspector General. DoJ reiterated that the Initiative will yield "an array of significant benefits," including improving cybersecurity practices overall and "raising the bar" for cybersecurity both within Government and for the public, "level[ing] the playing field" so that those companies that invest in meeting cybersecurity requirements will not be at a competitive disadvantage with companies that do not, assisting government experts with timely identifying and remediating vulnerabilities in government systems.

Finally, DoJ shows no signs of easing up on its Procurement Collusion Strike Force, aimed at detecting and enforcing antitrust violations in government procurement, grant, and program funding in the U.S. and in connection with U.S. government contracts abroad. At the end of 2020, the Strike Force's inaugural year, it added 11 new partners from U.S. Attorney Offices and federal agencies and established a permanent

director for the program. In November 2020, it had over two dozen grand jury investigations in progress. In June 2021, it announced the guilty plea of one Belgian security services company and the indictment of another and three former executives for price fixing, market allocation, and bid rigging in connection with DoD contracts.

Continued Emphasis on Climate Change and Environmental Issues

Climate change and environmental issues continue to be an area of emphasis for the Biden Administration. As we previously discussed, one of the first Executive Orders the President issued was a sweeping Executive Order to address climate change. That EO directed a government-wide approach to combatting climate change, including new regulations that would affect contractors. Despite this early emphasis, however, little regulatory activity has emerged. As of October 12, 2021, the FAR Council reports no open FAR cases directly related to the initial climate change EO. The FAR Council did issue an advanced notice of proposed rulemaking on October 15, 2021, related to a different EO, seeking public input regarding how greenhouse gas emissions can be considered in federal procurement decisions, how major procurements can better incorporate and mitigate climate-related financial risk and how best to standardize reporting on greenhouse gas emissions. Public comments are due by December 14, 2021 for consideration in the proposed rule.

Even though regulatory activity on climate change has been light, agencies have been developing climate change strategies and mitigation measures over the last few months. These activities culminated in the release of climate adaptation and resilience plans by 23 agencies on October 7, 2021. Those plans identified programs and missions that agencies deemed most at risk from climate change and identified senior leadership and accountability structures for addressing climate resiliency. Consistent with our other themes, several of the plans identified supply chain resilience as an area of focus and identification of alternative domestic suppliers for critical missions and programs as a key mitigation strategy. As agencies proceed with implementation of these plans, contractors can expect additional resiliency requirements to be incorporated into upcoming procurements.

---

1 https://www.bis.doc.gov/ictforum.