Government Contractors Beware: Implications of the DOJ’s New Procurement Collusion Strike Force

Vic Domen, Gerald Stein, and Amanda Wait

The Antitrust Division of the U.S. Department of Justice enforces U.S. antitrust laws to protect consumers. This includes some of the nation’s largest consumers—federal, state, and local government agencies and instrumentalities. The Antitrust Division recently signaled a renewed interest in prioritizing the enforcement of antitrust violations in public contract procurement by launching the Procurement Collusion Strike Force in November 2019.1 This initiative likely means an increase in the number and scope of procurement fraud audits, investigations, and prosecutions for current and aspiring government contractors.

The Strike Force is particularly relevant and timely in light of procurement activities of federal, state, and local governments responding to the COVID-19 pandemic.2 On March 9, 2020, for example, Attorney General William Barr announced the DOJ’s intention “to hold accountable anyone who violates the antitrust laws of the United States in connection with the manufacturing, distribution, or sale of public health products such as face masks, respirators, and diagnostics.”3

The Procurement Collusion Strike Force

Historically, the public procurement space has been uniquely vulnerable to collusion for several reasons. To begin with, it can be a lucrative target for anticompetitive conduct.4 In 2018, the federal government spent over $550 billion on contracts for goods and services. Of this $550 billion, state and local governments received over $79 billion in grants to fund major public infrastructure projects. Public procurement is particularly vulnerable because regulatory requirements or processes governing public procurement can be repetitive and predictable, making them more readily subject to manipulation through collusion than other types of procurement. And because government agencies often require highly specialized goods and services, the pool of qualified firms that repeatedly bid for the contracts may be limited. This small market facilitates the ability of qualified bidders to collude, particularly during emergency procurement, such as disaster relief projects. Lastly, the enormous volume of goods and services that the government buys makes monitoring contracts and orders difficult.5

5 Id.
To combat this problem, in November 2019, the Antitrust Division launched the Procurement Collusion Strike Force (PCSF), an interagency partnership with a broad mandate to deter, detect, and aggressively prosecute companies and individuals violating antitrust laws to the detriment of government procurement programs at federal, state, and local levels. \(^6\) In announcing the new PCSF, Assistant Attorney General Makan Delrahim explained:

> When competitors in any given industry collude and conspire to rig bids, fix prices, or allocate markets—that is, commit criminal antitrust violations—they distort the free market and harm customers with high prices and lower quality goods and services. This is no less true in the area of public procurement, where the customer is the government and the American taxpayer foots the bill for artificially high prices. \(^7\)

The PCSF aims to accomplish this mandate through a three-pronged approach: first, by increasing the probability of detection; second, by imposing severe sanctions on bad actors; and third, by incentivizing compliance.

**Increasing the Probability of Early Detection of Potential Procurement Collusion.** The PCSF seeks to increase the probability of detection through the pooling of government resources, targeted outreach and education, and facilitation of whistleblowing. The announcement of the PCSF makes clear that one of the goals is to promote interagency information sharing to execute joint investigations and prosecutions under various federal laws. The PCSF includes representatives from the following agencies: the Antitrust Division, the FBI (including special agents assigned to 13 districts within the District of Columbia and eleven states\(^8\)), the DOJ’s Office of the Inspector General, the U.S. Department of Defense, the General Services Administration, and the U.S. Postal Service. \(^9\)

A unique feature of the PCSF is that it uses a “district-based” organization structure to streamline cooperation among the Antitrust Division, 13 U.S. Attorneys’ Offices, the FBI, and Inspector General Offices. The Antitrust Division has designated Trial Attorneys to serve as PCSF Liaisons for each of the 13 partner U.S. Attorneys’ Offices. Each U.S. Attorney has designated an Assistant U.S. Attorney to serve as a PCSF Liaison for that district. Finally, the FBI designated Special Agents from the field offices in each of the 13 districts to serve as PCSF Liaisons. Together, these teams will lead the outreach training in their districts. The PCSF has not released specifics about how this outreach will occur, but we would expect a large part of it would involve coordinated trainings by the participating groups.

The PCSF will conduct targeted outreach training and education programs to key constituencies on both the “sell” and “buy” sides of the public procurement field. On the “sell side,” the PCSF will contact government contractors, trade associations, and public contract lawyers to educate them about criminal antitrust laws to raise awareness of potential penalties for criminal and civil antitrust violations. On the “buy side,” the PCSF will educate federal, state, and local government

---

\(^6\) Delrahim, supra note 1.

\(^7\) Id.


\(^9\) Id.
procurement officials on identifying potential indicators (or “red flags”) of collusion and assist with structuring the acquisition process to remove vulnerabilities. With the acronym “MAPS,” the Antitrust Division has outlined four “red flags” of collusion it considers important to its review of procurement matters:

- **M**: Is the Market for the award dominated by a few participants or small group of competitors?
- **A**: Do the Applications or bids share similarities, such as the same typographical errors?
- **P**: Have Patterns developed among competitors for submitting bids, such as repeated rotation of similar awards across multiple vendors or the same group of competitors hired as subcontractors?
- **S**: Is there other Suspicious behavior evidencing some other form of collusion, such as competitors submitting proposals who lack the ability to provide the requested goods or services?

Further, the PCSF has invested in an improved data analytics program to better identify and analyze irregularities and “red flags” of anticompetitive conduct in government procurement data. The PCSF announced plans to coordinate an interagency roundtable in early 2020 to bring together data scientists from across the law enforcement and Inspectors General communities. Additionally, the PCSF has begun analyzing significant volumes of contracting data housed in government agencies to efficiently uncover signs of possible anticompetitive collusion for further investigation.

Lastly, the PCSF has increased the prospect of whistleblowers emerging from government contractors, competitors, and other third parties. In addition to both the DOJ’s general online complaint form and the Antitrust Division’s general Citizen Complaint Center, the PCSF maintains a dedicated webpage that offers training materials to the public and hosts a “citizen complaint” page that the public can use to report suspected antitrust violations with government procurement. The PCSF also created a Tip Center to receive and review complaints, concerns, or tips concerning potential antitrust crimes. A company or individual can submit a concern to the Tip Center via email or regular mail. The submission should identify the party or parties involved; describe the conduct suspected of violating the law, including the products and/or services that are the subject of the government contract, grant, or program; explain the suspected illegal conduct involved (e.g., bid rigging, price fixing, or market allocation); and detail when or where the illegal conduct allegedly occurred.

**Seeking Sanctions for Anticompetitive Conduct.** The second method for accomplishing its mandate is that the PCSF will seek severe sanctions on actors engaged in anticompetitive behavior. Beyond criminal penalties imposed for anticompetitive behavior, the DOJ has also sought civil penalties against these actors. In order to ensure that entities involved in anticompetitive conduct are held accountable, the Antitrust Division has also taken steps to increase the visibility of its enforcement efforts.

---

10 The DOJ has a history of working with state enforcers to educate state procurement officials but appears to be expanding its previous efforts. See, e.g., Christine A. Varney, Remarks as Prepared for the National Association of Attorneys General (Oct. 7, 2009), [https://www.justice.gov/atr/speech/antitrust-federalism-enhancing-federalstate-cooperation](https://www.justice.gov/atr/speech/antitrust-federalism-enhancing-federalstate-cooperation).


12 Powers, supra note 4.


16 Id.
penalties for FCA violations and will likely continue to leverage additional federal statutes to compound liability, such as Section 4A of the Clayton Act, which allows the government to recover treble damages when it is the victim of an antitrust violation. If the courts ultimately impose liability under these other statutes in addition to antitrust liability, it could compound immensely any financial penalties imposed.

Creating Incentives for Compliance. The third method that the PCSF is employing to fulfill its mandate is the creation of two primary incentives for compliance with antitrust laws: (1) the Antitrust Division’s Corporate Leniency Policy and Leniency Policy for Individuals (collectively, Leniency Program), and (2) a corporate compliance consideration policy. Through the Antitrust Division’s Leniency Program, an individual or company that discovers an antitrust violation and is the first to self-report (or “wins the leniency race”), cooperates with the Antitrust Division’s investigation, and meets other requirements, may avoid a criminal conviction, a criminal fine, and prosecution of a company’s directors, officers, and employees. For companies or individuals that “lose the leniency race,” the PCSF will investigate and likely prosecute remaining members of the conspiracy. This may present a harsh reality to many: win the leniency race or face potential criminal convictions with lengthy prison terms, severe monetary penalties, the risk of debarment, and full liability exposure in private litigation.

The second incentive—announced just in the past year—is that the Antitrust Division will consider and credit corporate compliance programs at the charging stage in criminal antitrust investigations. On July 11, 2019, AAG Delrahim announced that the Antitrust Division adopted a new policy to reward companies that invest in and instill a “culture of compliance.” Along with the policy changes, the Antitrust Division also published a guide for prosecutors evaluating a company’s compliance program. Thus, an effective antitrust compliance program may be the last line of defense against severe penalties and collateral consequences that an investigation and prosecution may cause.

Past Procurement Initiatives

The Antitrust Division’s recent decision to devote significant investigative resources to the public procurement space is neither new nor unique. The Division has a long history of prosecutingcriminal antitrust conspiracies that target government contracts, ranging from construction projects to food and hardware supply. In the 1970s and 1980s, the Division prosecuted hundreds of corporations and individuals for bid-rigging road construction projects across multiple states. In the

---


20 See Powers, supra note 4. The Antitrust Criminal Penalties Enhancement and Reform Act (ACPERA) provides that a leniency applicant can face liability only for single damages (not the treble damages otherwise provided for in antitrust litigation) and does not face joint and several liability with other defendants in private litigation.


early 1990s, the Division investigated and prosecuted multiple companies and individuals involved in a decade-long conspiracy to rig bids for frozen seafood contracts.

Consider one important example of successful antitrust enforcement—the Antitrust Division’s criminal cases against milk and dairy products suppliers. The Division uncovered evidence that dairy companies had been conspiring since at least the early 1980s to rig bids to supply milk and other dairy products to public school districts and other public institutions in several states. The Florida Attorney General’s Office first noticed suspicious bid patterns by milk suppliers and brought this information to the attention of the Antitrust Division’s Atlanta field office in 1986. The Division began a grand jury investigation, which uncovered a state-wide conspiracy to rig bids to public school districts in Florida and evidence of similar conspiracies in other states. The Division filed 134 milk bid-rigging cases involving 81 corporations and 84 individuals. Corporations and individuals received criminal fines totaling more than $69.8 million, and 29 individuals were sentenced to jail. Civil damage settlements between the Division and defendants exceeded $8 million.23

In the mid-2000s, the Division and its investigative partners prosecuted multiple individuals in several states for schemes to rig bids with the E-Rates program, which was designed to provide disadvantaged schools and libraries with internet access and telecommunications services. One of the primary defendants was convicted at trial, sentenced to over seven years in prison, and debarred for ten years. Most recently, in November 2018 and March 2019, the Division obtained guilty pleas from five South Korean oil companies for a decade-long bid-rigging conspiracy targeting contracts to supply fuel to U.S. military bases in South Korea. The companies agreed to pay $156 million in criminal fines and over $205 million in separate civil settlements.24

Moreover, the strategy of utilizing strike forces (sometimes also called “task forces”) is not new for the DOJ. The PCSF is modeled from prior initiatives25 that resulted in increased investigations and prosecutions in certain markets or industries the government believed were high risk for or had high instances of corruption. The PCSF was created to continue the DOJ’s trajectory of successful prior strike force deployments.

In March 2007, the DOJ launched the initial Health Care Fraud Strike Force (HCF Strike Force), a joint investigative and prosecutorial effort against Medicare fraud and abuse in South Florida.26 Using advanced data analytics to target suspicious billing patterns in cities with high levels of billing fraud, the HCF Strike Force charged over 4,200 defendants involved in approximately $19 billion in Medicare program billings. As of December 2018, based on the Strike Force’s success and increased federal funding, the DOJ has expanded the HCF to ten additional geographic

---


24 See Powers, supra note 4.

25 Some of these past initiatives include the Corporate Fraud Task Force, established in response to revelations about Enron and other major corporations, see U.S. Dep’t of Justice, President’s Corporate Fraud Task Force, https://www.justice.gov/archive/dag/cftf/; the Hurricane Katrina Task Force, established to combat fraud relating to Hurricane Katrina and its aftermath, see U.S. Dep’t of Justice, President’s Corporate Fraud Task Force, https://www.justice.gov/sites/default/files/criminal-disasters/legacy/2012/07/30/katrinareportfeb2006.pdf; and a Campaign Finance Task Force, established to investigate allegations of wrongdoing in the 1996 election cycle, see Gov’t Accountability Office, CAMPAIGN FINANCE TASK FORCE: PROBLEMS AND DISAGREEMENTS INITIALLY HAMPERED JUSTICE’S INVESTIGATION 1 (May 2000), https://www.gao.gov/assets/80/79297.pdf.

areas. In October 2006, the DOJ Criminal Division formed a similar National Procurement Fraud Task Force (NPF Task Force), targeting U.S. military procurement fraud tied to conflicts in Iraq and Afghanistan. The fraud included defective pricing, product substitution, misuse of sensitive information, false claims, accounting fraud, conflicts of interest, and other ethical breaches. By 2009, the NPF Task Force prosecuted and convicted over 35 criminals. Similarly, the Central District of California established a Procurement Fraud Task Force in 1991, focusing on alleged fraud in the defense industry. More recent DOJ initiatives have focused on elder fraud, organized crime, and human trafficking.

Since 2015, the DOJ has also increased its efforts to work cooperatively with state enforcers to educate state procurement officials about the warning signs of collaborative efforts by competitors in state contracting—which often include federal funds. This effort has included federal and state officials conducting joint trainings to educate state procurement officials and the sharing of enforcement experiences.

The collaboration among state and federal enforcers who share these initiatives led to the mobilization of government enforcement resources from various agencies to address a high priority issue.

**Practical Guidance: The Takeaways**

In light of this increased scrutiny and potential for severe consequences, companies contracting with federal, state, or local agencies should reexamine their internal compliance policies, business practices, and contract selection processes to ensure that policies are current and to consider these risks. Now is the time to look back at past and current behavior, to reexamine or create an antitrust compliance program, and to reaffirm to employees that the company expects strict compliance with these policies. Companies involved with government procurement should focus their attention on issues most related to the PCSF.

Effective compliance programs may help prevent any misconduct at the outset, thereby avoiding the costs of defending against or cooperating with a DOJ or state investigation and the enormous potential reputational costs of such a public investigation. Falling short of prevention, identifying the misconduct early will allow a company that discovers evidence of a possible violation to stop such conduct and possibly be the first to self-report to gain the benefit of the DOJ’s Leniency Program and its associated benefits. Lastly, if a company loses the leniency race yet demonstrates that it has an effective compliance program and culture, the company may still avoid criminal conviction if, after the company becomes aware of an antitrust violation, it promptly self-reports and begins cooperating. Such an approach has the potential to resolve the matter by a deferred prosecution agreement, rather than by guilty plea, and this can make an enormous difference when it comes to government contracting and the risk of debarment.

Although there are no formulaic requirements, an effective compliance program should be well-

---

27 These include Los Angeles, CA; Detroit, MI; Houston, TX; Brooklyn, NY; Southern Louisiana; Tampa, FL; Chicago, IL; Newark, NJ; Philadelphia, PA; and Dallas, TX. See id.


30 See Corporate Leniency Policy, supra note 18; Leniency Policy for Individuals, supra note 19.

designed, tailored to a company’s particular line of business, monitored, and updated regularly. A company should consider numerous factors when creating an effective compliance program:

1. **Address the MAPS factors.** When current and aspiring government contractors consider creating a truly effective antitrust compliance program and culture, we suggest focusing on the MAPS factors emphasized by the DOJ. Companies should be particularly cognizant of whether their industry is characterized by high market concentration, since the DOJ will be particularly attuned to parallel patterns of behavior.

2. **Create a team to oversee and manage the antitrust compliance program with a focus on government procurement.** As always, those responsible for the compliance program must have sufficient autonomy, authority, and seniority within the company’s governance structure, as well as sufficient resources for training, monitoring, auditing, and periodic evaluation of the program. They should also be knowledgeable in how the company competes in its industry and understand competitive trends. They should look out for patterns where successful bids are rotated among a select group of competitors. And they should be particularly aware of how government procurement works and thus the areas with the greatest risk of procurement fraud or manipulation.

3. **Tailor the compliance program to the company’s business,** consistent with industry best practices, and to detect particular types of misconduct most likely to occur within the company’s line(s) of business. An effective compliance program must be appropriately tailored to a company’s particular antitrust risks, including in the area of its government contracting.

4. **Collect, analyze, and leverage data/metrics to inform trainings and to make appropriate modifications to the compliance program or internal controls.** One new focus of the DOJ has been companies’ use (or failure to use) data/metrics to detect antitrust violations. On September 12, 2019, the DOJ announced that federal prosecutors will assess whether compliance officers make adequate use of data analytics in reviews of their companies’ compliance.

5. **Periodically review the company’s risk assessment and update policies or practices according to market, legal, or technical developments.** With respect to government procurement, a compliance team should track bid wins and losses so that any patterns regarding successes and losses can be detected.

6. **Use best practices to address and prevent any conduct that may be deemed anticompetitive.** For example, a common area of risk for collusion in government procurement is in the submission of joint bids. When jointly bidding on contracts, evaluate the bid information and changes in pricing to detect possible bid rigging or price fixing. It is crucial that you track various factors that can be used to demonstrate that the joint bid did not result from improp-
er collusion. Examples of best practices to address and prevent anticompetitive conduct in submitting joint bids may include the following:

- Document the factors that establish each company’s respective expertise that necessitates a joint bid for any contract to be completed, and document the plan to combine resources to complete the project. The documentation can include allocating different portions of the work to be performed separately where one party alone lacks the expertise to perform all the work itself. Demonstrating that each company provides complementary services will be viewed as a procompetitive justification for submitting a joint bid, thereby reducing the risk of an investigation or challenge.

- Ensure that each company does not discuss or coordinate its bid with any other competitors. Each company forming part of the joint bid should separately calculate and determine the cost for its respective work on the proposed project, which can then be combined as a total bid.

- Protect competitively sensitive information. Sharing sensitive information with competitors may expose companies to antitrust liability. The government recognizes that sharing information among competitors may be procompetitive and is often reasonably necessary to achieve the procompetitive benefits of certain collaborations. However, the competitive concern depends on the nature of the information exchanged, and understanding the boundaries is crucial. If there is any doubt, engage external counsel to assess the information exchanged. Even the mere appearance of collusion can lead to losing the bid and a costly investigation.

- Confirm whether the state of the project requires certification of non-collusion when submitting the bid.

**Conclusion**

Government contractors beware! The Antitrust Division has made it clear that it will aggressively enforce any antitrust violations in the public procurement space. The consequences of even giving an appearance of anticompetitive conduct can be costly, particularly when considering both the actual costs of defending or aiding in an investigation and the reputational damage such an investigation may have, including the loss of future contracts. Establishing an effective antitrust compliance program can safeguard a company and prevent severe civil or criminal consequences.