ACTION ALERT

DOD OIG JEDI INVESTIGATION: TAKE-AWAYS

The Department of Defense (DoD) Office of Inspector General (OIG) released its 300+ page Report on the Joint Enterprise Defense Infrastructure (JEDI) Cloud Procurement in April 2020 (the Report). ***Spoiler alert***: the OIG concluded that the DoD conducted the procurement according to law and regulation. While the media primarily focused on this conclusion, the Report presents a rare, behind-the-scenes peek into a $10B government cloud procurement. Companies that do business with the government can benefit from several interesting take-aways. Estimated reading time: 4 minutes.

DEVELOP A PROCESS THAT ADDRESSES ACCESS TO NON-PUBLIC, PROPRIETARY, CONFIDENTIAL INFORMATION AND TRAIN YOUR EMPLOYEES

The OIG Report revealed that the DoD inadvertently gave Microsoft's source selection, trade secret information (in the Technical Evaluation Board Report, the "TEB Report") to Amazon as part of Amazon's debriefing. Report at 6, 81-90. Most TEB Reports cover the technical strengths and weaknesses of the offeror's proposed solution for each evaluation factor. Normally, the government *never* releases source selection documents even to the offeror, much less to a competitor in a debriefing. In fact, because these documents may give offerors unfair advantages in future procurements as well as proprietary trade secrets, the Procurement Integrity Act and Trade Secrets Act explicitly prohibit the release of non-public information to ensure an equal playing field and fair competition. The government presumes that the company receiving the non-public information received an unfair advantage. The recipient must prove that the information had no impact on their proposal or re-bid.

While companies cannot necessarily control the information a government agency releases to it, it can limit the exposure when/if it receives non-public information. Employees should: 1) identify non-public, sensitive information; 2) *recognize* that the disclosure was in error; and 3) apply the correct company policies and procedures on handling that information. If the competitor does not have a stated process, the offeror whose source selection or bid and proposal data is disclosed to a competitor can allege a conflict of interest or try to disqualify the competitor from a future procurement, claiming that the competitor has an unfair advantage. Inquiry, mitigation, and explanation add unnecessary complexity to the procurement for all parties.

Action Alert:

- ☐ Ensure that your government contracting compliance program and Contractor Code of Business Ethics and Conduct has a policy and process for handling non-public, source selection, trade secret, proprietary, confidential information and train your employees to identify sensitive information, where to find the policy and procedure, and how to follow it.
  Pro-Tip: A good rule of thumb is whether release of your company's similar information to your competitor would hurt or harm your competitive position – if the answer is yes, then you should treat similar information as non-public.
- ☐ Proactively develop a mitigation plan, to include isolating any bid response team from any employee and any other individuals who may have reviewed non-public information.

Unfortunately, once rung, you cannot unring a bell. Ensure that your employees respect all restrictions and will proactively recuse themselves from problematic discussions.

- ☐ If your company is the unfortunate competitor that has had its information disclosed, work with your legal team or outside counsel to determine how to disclose this fact to the contracting officer in every procurement, ask for disqualification of the other offeror and consider protesting.

IMPLEMENT A TEMPORARY MORATORIUM ON EMPLOYMENT DISCUSSIONS WITH EMPLOYEES OF THE GOVERNMENT CUSTOMER

The OIG report also investigated allegations of impropriety based on Amazon's employment of former government employees who had some connection to the JEDI procurement. The IG found no actual impropriety or influence of former government employees on Amazon's bid because the individuals had tangential access to information or were involved in such early discussions where the government found little to no impact on the procurement. Report at 123-227.

The Procurement Integrity Act again comes into play if a competitor alleges unequal access to information because of that former government employee's influence on or contact with source selection, other bid and proposal or proprietary information. Even if an investigation does not find actual impropriety, the mere appearance of impropriety can harm the company in several ways. The company may have to defend and litigate pre-award bid protests from competitors. In addition to the actual costs of defending such protests, a protest side trip can increase the award timeline even with an express protest option. Further, salacious allegations of impropriety can distract from the merits of the company's offer and impair the company's reputation among the government acquisition community.

Action Alert: The ethics rules on post-government employment allow government employees to talk with companies in certain given instances. However, the following steps aim to combat the optics of impropriety.

- ☐ Develop a process to identify large influential procurements that the company wishes to participate in and implement a moratorium on hiring from those government agencies during the government's acquisition timeframe. Create a procedure for exceptions with documented approvals and escalations to include the business executives that oversee the public sector work. Coordinate with HR, Recruiting and Hiring Managers to socialize the moratorium for the impacted teams. This step should inoculate the company from these allegations of impropriety.
- ☐ In instances where the company does decide to hire from a government agency before contract award, implement guardrails prior to the employee's start date. Inform all stakeholders regarding the cooling-off period and explicitly shield the bid response team and public sector team from that individual.

ETHICS & INTEGRITY: THE WEAKEST LINK

The OIG Report indicated that an Amazon employee allegedly lied not only to the government as he was leaving government service but also to Amazon. Report at 128-157.

A company's ethics and compliance program is only as strong as each of its employees. A company trusts its employees to do the right thing and abide by company policies and procedures. A dishonest employee can erode that trust. Further, retention of a duplicitous employee can negatively impact a company's culture of ethics and integrity.

Beyond the business concerns that a dishonest employee brings to the company, other offerors may claim that your company is not a responsible contractor to disrupt the government contracting process. The government only awards contracts to "responsible" contractors – those that "[h]ave a satisfactory record of integrity and business ethics." Federal Acquisition Regulation (FAR) Part 9.104-1. In fact, for large contracts (over $5M in value and over 1 year in performance), the FAR also requires a Contractor Code of Ethics and Conduct, training for employees, internal controls, and mandatory disclosure. Mere allegations of employee dishonesty can call into question the offeror's ethics and integrity and whether it can effectively prevent fraud and waste of government money.

Action Alert:

- ☐ Do not ignore credible red flags – no one ever goes looking for dishonesty and corrupt behavior, but reckless hires can taint even the most ethical companies.
- ☐ Confirm that your Contractor Code of Ethics and Conduct requires employee honesty and integrity to the company and a provision stating that violation of the Code can result in termination in accordance with local law and regulation. Investigate allegations of wrongdoing and keep records of findings and discipline to be able to defend against non-responsibility allegations.
- ☐ If you think that a competitor is acting dishonestly or unethically, disclose your responsibility concerns to the contracting officer. Understand that if you have credible evidence of fraud or other illegal activity that involves government funds, you have a mandatory disclosure obligation to the relevant inspector general. Consult your legal team or outside counsel to determine how best to handle these types of disclosures.

For more information or to receive future articles and firm updates by email, please contact Tong Tejani, PLLC attorneys Joyce Tong Oelrich, joyce@tongtejani.com or Zohra Tejani, zohra@tongtejani.com.

Note: Tong Tejani's client base includes global technology companies. The firm has not been engaged on any matters related to the JEDI procurement. These takeaways reflect the views of Tong Tejani attorneys alone.