19-2326

IN THE UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

ORACLE AMERICA, INC.,

Plaintiff-Appellant,

v.

UNITED STATES,

AMAZON WEB SERVICES, INC.,

Defendants-Appellees.

On Appeal From The United States Court Of Federal Claims
Case No. 1:18-Cv-01880-EGB, Senior Judge Eric G. Bruggink

NON-CONFIDENTIAL OPENING BRIEF OF PLAINTIFF-APPELLANT ORACLE AMERICA, INC.

Of Counsel:

Kara L. Daniels
Dana E. Koffman
Nathaniel E. Castellano
Amanda J. Sherwood
ARNOLD & PORTER KAYE SCHOLER LLP
601 Massachusetts Ave., N.W.
Washington, D.C. 20001

Craig A. Holman
ARNOLD & PORTER KAYE SCHOLER LLP
601 Massachusetts Ave., N.W.
Washington, D.C. 20001
(202) 942-5722
craig.holman@arnoldporter.com

Counsel for Oracle America, Inc.

October 28, 2019

CERTIFICATE OF INTEREST

Counsel for Plaintiff-Appellant Oracle America, Inc. certifies the following:

1. The full name of every party or amicus represented by me is:

   Oracle America, Inc.

2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me is:

   N/A

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

   Oracle Corporation (NYSE: ORCL)

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court and who have not or will not enter an appearance in this court are:

   N/A

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal:

   N/A

Dated: October 28, 2019

/s/ Craig A. Holman
Craig A. Holman

TABLE OF CONTENTS

The material on pages 17 and 53 is redacted pursuant to the U.S. Court of Federal Claims Protective Order. The Sealed Memorandum Opinion and Order is omitted from the Addendum in its entirety pursuant to the U.S. Court of Federal Claims Protective Order and footnote 1 of the U.S. Court of Federal Claim's Reported Opinion at Appx64.

TABLE OF AUTHORITIES

CASES **Page(s)**

STATUTES

REGULATIONS

LEGISLATIVE AND REGULATORY HISTORY

SECONDARY SOURCES

STATEMENT OF RELATED CASES

Pursuant to Rule 47.5, Appellant Oracle America, Inc. ("Oracle") states that this case has had no prior appeals before this Court or any other appellate court, and that there are no related cases pending in this Court or any other court.

ORAL ARGUMENT STATEMENT

Oracle respectfully requests that the Court conduct oral argument in this matter.

JURISDICTIONAL STATEMENT

Oracle appeals a final Judgment by the United States Court of Federal Claims ("COFC") entered July 19, 2019. COFC had jurisdiction under 28 U.S.C. § 1491(b) to hear Oracle's pre-award bid protest alleging Department of Defense ("DoD") violations of law and arbitrary action in connection with Solicitation No. HQ0034-18-R-0077, commonly referred to as the Joint Enterprise Defense Infrastructure Cloud procurement ("JEDI"). Oracle timely noticed its appeal on August 26, 2019. This Court has jurisdiction under 28 U.S.C. § 1295(a)(3).

STATEMENT OF THE ISSUES

1. Whether COFC erred by failing to remand to the agency after finding the DoD decision to solicit JEDI as a single $10 billion Indefinite Delivery Indefinite Quantity ("IDIQ") contract contravened 10 U.S.C. § 2304a(d)(3).

2. Whether DoD violated the law by setting, as a gate to compete, a requirement that offerors demonstrate *at the time of proposal submission* three

existing datacenters each supporting Federal Risk and Authorization Management Program ("FedRAMP") moderate offerings, where DoD (i) knew that only two cloud providers could pass the gate but ignored the statutory Justification and Approval ("J&A") process for limited competition, (ii) violated the statutory process for imposing qualification requirements, and (iii) deviated from FedRAMP's prohibition against using authorization as a requirement to compete.

3. Whether the Contracting Officer ("CO") improperly decided to proceed with the procurement despite established violations of Federal Acquisition Regulation ("FAR") 3.101-1 and apparent violations of 18 U.S.C. § 208 by several government officials with prohibited interests in Amazon Web Services, Inc. ("AWS"), an interested JEDI competitor.

STATEMENT OF THE CASE

This appeal arises from a pre-award protest of JEDI, a massive, high-profile DoD procurement for enterprise-wide cloud services. Oracle alleged several violations of law, including that DoD (i) structured the $10 billion IDIQ contract for a single provider contrary to the statutory prohibition against such awards, (ii) specified qualifying criteria to limit the number of competitors without following the processes Congress requires in such circumstances, and (iii) proceeded with the procurement despite the prohibited conflicts of several officials arising from their relationship with AWS. COFC correctly determined that DoD's winner-take-all

approach violated 10 U.S.C. § 2304a(d)(3) but errantly assumed the parameters of the new competition and, based on such assumption, found no prejudice to Oracle. Significantly, the "at the time of proposal submission" FedRAMP criterion (Gate 1.2) itself violates various statutory provisions. COFC's decision also permits DoD to proceed with a procurement corrupted by the misconduct of several government officials tied to a competitor, a flawed result that contravenes Supreme Court precedent and procurement law.

I. DoD Solicits A Single JEDI Commercial Cloud Provider

In a September 13, 2017 memorandum, then-Deputy Secretary of Defense ("DSD") Patrick Shanahan established the Cloud Executive Steering Group ("CESG") and initiated JEDI to acquire enterprise-wide commercial cloud services. (Appx105955-105956.) DSD tasked the Defense Digital Service ("DDS") with leading the effort. (Appx105956.) DDS assigned four individuals (including Deap Ubhi) to run the acquisition. (Appx102793, Appx102813.)

The solicitation contemplates a ten-year, single IDIQ contract valued up to $10 billion, offering the potential for a monopoly over DoD's cloud needs in a highly competitive and rapidly evolving market. (Appx100730, Appx100734.) The contract contemplates an expansive scope, serving missions "at all classification levels, across the homefront to the tactical edge...." (Appx100608.) Tactical edge

means "[e]nvironments covering the full range of military operations...." (Appx100652.)

A. DDS Advocates for, and DoD Adopts, a Single-Award Approach.

Despite that the U.S. Code favors multiple IDIQ awards, the day after DSD initiated JEDI, the newly-formed CESG met and discussed a single IDIQ contract approach. (Appx105927-105928, Appx6.) Following several more CESG meetings, including one on October 16, 2017, where Ubhi "tackle[d] [the] question of one versus multiple cloud providers" (Appx160100), DoD confirmed publicly the chosen "Single-award [IDIQ] contract…" strategy. (Appx105957.) Following Ubhi's presentation, DDS counsel reported, "[s]ingle is assumed now," telling Ubhi: "Really glad you were here this week." (Appx160229.) A few days later, on October 22, 2017, the DDS Deputy Director confirmed the success of Ubhi's presentation: "The single [vs.] multiple conversation is done. Everyone that matters is now convinced." (Appx160239.)

B. DoD Recognizes the Dynamic Cloud Market and Includes a Bespoke Clause to Add New Services Throughout Performance.

DoD's research reported the "cloud market is an evolving and competitive landscape" where "new cloud providers are emerging monthly, and the service offerings of the vendors are rapidly shifting." (Appx109603.) To "keep[] pace with industry innovation and stay[] at the forefront of available technology" (Appx100472), the solicitation does not seek fixed services or pricing. Instead, the

JEDI contractor will continually update the services available. Specifically, DoD crafted a special provision, clause H2, under which DoD can constantly add "new services" to the contract, with pricing later determined. (Appx100740-100741, Appx106673-1006674 (internal J&A for Clause H2).)

When others questioned clause H2, the JEDI team explained that the cloud "offerings are not static and will be updated overtime [sic] both in terms of available services and applicable pricing." (Appx108721 (Q1115).) Industry advised DoD that clause H2 would result in "daily or weekly" updates to services and pricing, even during the competition. (Appx100660 (Q17), Appx100668 (Q86-87).)[1]

C. Congress Mandates Task Order Competition to the Maximum Extent Practicable and Prohibits Large Single-Award IDIQ Contracts Except in Limited, Inapplicable Circumstances.

Procuring agencies use IDIQ contracts, also known as task order contracts, where an agency "cannot predetermine … the precise quantities of supplies or services that the Government will require during the contract period." 48 C.F.R. § 16.504(b); *see also* 10 U.S.C. §§ 2304a-d. After award, the agency "places orders for individual requirements." 48 C.F.R. § 16.504(a); 10 U.S.C. § 2304c.

Numerous Congresses have placed limitations on agency use of single IDIQ contracts, favoring multiple awards to maintain task order competition throughout

[1] Gartner reports that major cloud providers may release 40 to 50 new features in any given month. Chris Pemberton, *Hidden Cloud Opportunities for Technology Service Providers*, Gartner (June 20, 2018), https://gtnr.it/2MJFx01.

performance. First, in 1994, Congress mandated that all agencies "give preference to making multiple [IDIQ] awards" to the "maximum extent practicable." 10 U.S.C. § 2304a(d)(4), 48 C.F.R. § 16.504(c)(1)(i); S. Rep. No. 103-258 at 15 (May 11, 1994) (noting "that all federal agencies should move to the use of multiple task order contracts in lieu of single task order contracts"). Before adopting a single-award approach, the CO must document the rationale, consistent with the prescribed criteria. 48 C.F.R. § 16.504(c)(1)(ii)(c).

Second, in 2008, frustrated with the continued, pervasive use of single-award IDIQ contracts, Congress prohibited the award of any such contracts valued at over $100 million, unless the senior procurement executive determines one of four limited exceptions exists. *See* 10 U.S.C. § 2304a(d)(3); 48 C.F.R. § 16.504(c)(1)(ii)(D).[2] This prohibition is distinct from the CO's obligation noted above, 75 Fed. Reg. 13416-01, 13420 (Mar. 19, 2010), and ensures that high dollar IDIQ contracts provide for task order competition "unless there is a compelling reason not to do so." S. Rep. No. 110-77 at 368 (June 5, 2007).

These provisions reflect Congress' determination that the government benefits from task order competition throughout contract performance:

> The major benefits of the continuous competition that can be achieved under multiple contracts are the ability to control the prices of individual task and delivery orders and the ability to award such orders

[2] Due to inflation, the $100 million prohibition was adjusted to $112 million in 2015. (Appx15 (n.7).)

> based on the past performance of the contractors. Multiple contracts also permit the agency to award IDIQ contracts to contractors with varying skills—giving the government access to a broader range of competence than would be possible with only a single contract.

John Cibinic, Jr., Ralph C. Nash, Jr., Christopher R. Yukins, FORMATION OF GOVERNMENT CONTRACTS 1395 (4th ed. 2011). DoD recognizes lower prices, innovation, better quality and performance, less fraud, and a stronger defense-industrial base as benefits of task order competition. (Appx105359-105362.)

The Office of Management and Budget ("OMB") documented the better prices and quality achieved through task order competition in the technology space, noting that costs after competition "averaged 16.7 percent less than the government's projected estimated costs." (Appx105310-105311.) OMB also reported that agencies relying on lengthy single-award IDIQ contracts "with technology refreshment and price reduction clauses" did not realize the economies and efficiencies afforded by competition. (Appx105310.)

The statutory and regulatory regime favoring multiple-award IDIQ contracts provides a necessary check on agency discretion, as procurement officials otherwise may forego the long-term benefits of task order competition in return for the ease of managing a single IDIQ contractor. DoD's continued disregard of the statutory single-award proscriptions has not escaped Congressional notice.[3]

[3] *Defense Contracting: Use by the Department of Defense of Indefinite Delivery Contracts from Fiscal Years 2015 through 2017* at 7 (May 10, 2018), https://bit.ly/2NbsfdS (Government Accountability Office Report to Congress

D. DoD Violates the Prohibition Against Large, Single-Award IDIQ Contracts.

In a July 17, 2018 memorandum, the JEDI CO purported to justify the earlier announced single-award approach. (Appx100455-100467.) Rather than give the required maximum practicable preference for multiple awards, the CO's one-sided analysis reflects the singular purpose of supporting the foregone single-award solicitation. (*Id.*)

Two days later, Under Secretary Lord, the senior procurement executive, determined that the JEDI contract will satisfy the following exception to the statutory prohibition: "the contract provides only for firm, fixed price (FFP) task orders or delivery orders for services for which prices are established in the contract for the specific tasks to be performed." (Appx100318.) The decision missed that clause H2 subverts the relied-upon exception. (Appx15-18, Appx42-45.) This clause exists to keep the JEDI contract current through the constant addition of new offerings. DoD cannot solicit fixed prices for the future, undefined, and unknown cloud services the awardee will deploy under clause H2.

---

noting DoD awarded over five times more single-award IDIQ contracts (8331) than multiple-award IDIQ contracts (1423)).

E. The Solicitation Incorporates Gate Criteria to "Get To One" Contractor Without Justification or Approval.

To limit the number of proposals received, DoD devised an evaluation using "gate criteria" requiring demonstration of certain capabilities at or before proposal submission. (*See* Appx100504.) A failure to pass a gate removes the proposal from evaluation and award consideration. (Appx100805.) The Acquisition Strategy explains the gates' purpose:

> The JEDI Cloud program schedule could be negatively impacted if source selection extends beyond the planned timeline due to an unexpected number of proposals or lengthy protest delays. To mitigate this risk, the solicitation will use a gated evaluation approach…. Offerors must meet the established minimum criteria in order to be considered a viable competitor.

(Appx100504, Appx105473 (78:5-11) (DDS Deputy Director testimony).)

DDS set the gates' metrics and capabilities to "get to one" JEDI contractor. During an internal discussion on Slack,[4] DDS counsel explained: "Let me put the metrics in this context. The agreed upon measures drive what acquisition strategy will be approved. So if multiple cloud providers can meet the metrics, then we won't get to one." (Appx103123, Appx7.)

[4] Much of the record consists of internal DDS communications on Slack, an electronic means for group discussions and private messages to share information, files, and more. (*See* Appx7 (n.4), Appx158699.) DoD provided a username key. (Appx102901, Appx102973.) Timestamps for each message may be converted using a publicly available epoch time converter. *See* https://www.epoch converter.com/ (last visited 10/28/19).

Despite extensive industry interest, after the solicitation release with its qualifying gates and single-award structure, only four companies submitted proposals. (Appx21, Appx158649.) Two of the four, Oracle and IBM, filed protests challenging the restrictive gates.[5] A third, Microsoft, publicly criticized the gates.[6] Another major cloud provider, Google, chose not to compete due to the restrictive terms.[7] The gates, as DoD's research suggested, reduced the field to two competitors. (Appx100369.)

Gate 1.2 mandates that each offeror have, at the time of proposal submission, no fewer than (i) three existing datacenters, (ii) within the customs territory of the United States, (iii) separated by at least 150 miles, (iv) capable of automated failover to the others, and (v) each "supporting at least one IaaS offering and at least one PaaS offering[8] that are FedRAMP Moderate 'Authorized' by the Joint Authorization

[5] Sam Gordy, *JEDI: Why We're Protesting*, IBM (Oct. 10, 2018), https://ibm.co/2oigbyR ("Certain requirements in the RFP either mirror one vendor's internal processes or unnecessarily mandate that certain capabilities be in place by the bid submission deadline versus when the work would actually begin. Such rigid requirements serve only one purpose: to arbitrarily narrow the field of bidders.").

[6] Billy Mitchell, *DOD defends its decision to move to commercial cloud with a single award*, FedScoop (Mar. 8, 2018), https://bit.ly/362rhZP.

[7] Aaron Gregg, *Google bows out of Pentagon's $10 billion cloud-computing race*, The Washington Post (Oct. 9, 2018), https://wapo.st/2BVbGh7.

[8] "IaaS" involves "[t]he capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources…." (Appx100649.) "PaaS" means "[t]he capability provided through software, on top of an IaaS solution, that allows the consumer to replicate, scale, host, and secure consumer-created or acquired applications on the cloud infrastructure." (Appx100650.)

Board (JAB) or a Federal agency as demonstrated by official FedRAMP documentation." (Appx100792, Appx100661.)[9]

FedRAMP is "a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services procured by federal agencies."[10] "FedRAMP Authorized" is a "designation that a contractor's systems have completed the FedRAMP authorization process," i.e., the government has found the systems meet the FedRAMP requirements.[11] The authorization process takes six months or longer to complete. *FedRAMP prohibits agencies from requiring authorization as a prerequisite to bid for a cloud services contract*. (Appx105292.)

DoD first included Gate 1.2's requirement to have three existing FedRAMP authorized datacenters by the time of proposal submission in the July 26, 2018 final solicitation. (*Compare* Appx106241 (requiring "FedRAMP Moderate *compliant*")[12] *with* Appx100792 ("FedRAMP Moderate '*Authorized*'").) Given the original submission deadline was less than two months later, DoD knew that interested providers without three existing datacenters running FedRAMP Moderate IaaS and

[9] Oracle also protested Gate 1.1, Elastic Usage, and Gate 1.6, Commercial Cloud Offering Marketplace, before the Government Accountability Office ("GAO") and COFC.

[10] FedRAMP.gov, FAQ, https://www.fedramp.gov/faqs/ (last visited 10/28/19).

[11] *Id.*

[12] All emphasis to quoted material has been added unless otherwise noted.

PaaS offerings could not pass Gate 1.2 and compete for JEDI. Indeed, DoD (part of FedRAMP) necessarily knew that only AWS and Microsoft could pass the gate.

The JEDI contract security requirements do not require FedRAMP authorization. (Appx105495 ("[W]e are not requiring, as part of the JEDI cybersecurity plan, that the winner go through the FedRAMP process before the DoD uses the final solution"), Appx105496 (same).) Instead, DoD will assess the awardee's infrastructure against the JEDI Cloud security requirements under Contract Data Requirements List ("CDRL") 11, a DoD-specific Security Authorization Package. (Appx105496-105498.) The contract instructs the awardee to submit CDRL 11 to DoD 30 days after award, and DoD does not commit to any approval timeframe. (Appx100159.)

II. Oracle's Protest And Subsequent Competitive Range Decision.

Before proposals were due, Oracle timely filed a protest at GAO challenging the single-award approach and gate criteria. (Appx21.) The abridged record produced at GAO partially revealed serious government conflicts infecting JEDI, causing supplemental challenges. (*See* Appx105187-105210.)

Oracle, IBM, Microsoft, and AWS submitted offers on October 12, 2018. (Appx158649.) Oracle's proposal demonstrated that, as of proposal submission, the estimated JEDI Cloud usage would not represent a majority of Oracle's total commercial cloud usage under each of the Gate 1.1 metrics—network, compute, and

storage. (Appx156783-156786.) Oracle's proposal also showed that Oracle operated three datacenters with FedRAMP Moderate PaaS offerings and expected to have FedRAMP High IaaS and PaaS authorized offerings running in five datacenters by the anticipated award date, i.e., by the award date Oracle would exceed Gate 1.2. (Appx156791-156792, Appx156807-156808, Appx123980-123981 (same).)

GAO subsequently denied Oracle's protest (Appx105899), and Oracle promptly filed its protest with COFC. During the COFC proceedings, DoD rated Oracle's proposal unacceptable under Gate 1.1 based on an arbitrary measurement period eight to nine months before proposal submission (Appx158649), and IBM's proposal unacceptable under Gate 1.2. (*Id.*) The AWS and Microsoft proposals passed all gates, but failed under other criteria. (*See* Appx158649-158662, Appx158758-158761.) The CO, however, included only AWS and Microsoft in the competitive range. (Appx158762.)

III. Numerous Procurement Officials And AWS Corrupt JEDI Through Prohibited Conflicts.

DDS ignored DoD's rules for screening conflicts and obtaining non-disclosure agreements ("NDA") *before* procurement involvement,[13] and allowed multiple

[13] *Compare* DoD Source Selection Procedures at 11, 36 ("To confirm statutory and regulatory compliance, ensure all persons receiving source selection information sign a [NDA] and a Conflict of Interest statement. Ensure Conflict of Interest Statements … are appropriately reviewed and actual or potential conflicts of interest are resolved prior to granting access to any source selection information.") at https://bit.ly/36ggcoi (last visited 10/28/19) *with* Appx123983-124126 (showing most JEDI NDAs were signed during Oracle's protest, if at all).

individuals with extensive, prohibited financial interests in AWS to participate personally and substantially in JEDI.

"During the pre-solicitation phase of the JEDI Cloud acquisition, incidents of potential conflicts of interest, often related to AWS, were brought to [the CO's] attention." (Appx158700 (¶22).) On July 23, 2018, three days before solicitation posting, the CO issued a memorandum addressing "four instances where individuals with potential financial conflicts of interest under 18 U.S.C. § 208 or impartiality restrictions under 5 C.F.R. § 2635.502 were provided with access to procurement sensitive information." (Appx100683.) Each "individual had either a financial interest in or a covered relationship with Amazon, Inc./Amazon Web Services (AWS)…. " (*Id.*) The individuals included Ubhi, who left DDS to rejoin AWS with a lucrative compensation package during JEDI, and Anthony DeMartino, a former AWS consultant, who served as the DSD's Chief of Staff and participated in JEDI *against DoD ethics advice*. (Appx100683-100687.) Apparently unaware of Victor Gavin's conflict at the time, the CO's initial memorandum did not mention Gavin, a former Navy official, who both participated in JEDI and accessed competition sensitive information *after* accepting employment with AWS. (*Compare id. with* Appx158744-158757.)

For the reported Ubhi conflict, the CO relied on a false narrative fabricated by Ubhi. (Appx25-28.) This false narrative permeated the GAO proceeding and only

surfaced as a result of Oracle's COFC protest. The CO believed Ubhi's AWS interest ended in January 2016, over a year before his JEDI participation, and that Ubhi "promptly recused himself" on October 31, 2017 after AWS sought to purchase Tablehero, a start-up owned by Ubhi. (Appx100686-100687.) But Ubhi's Tablehero story was a lie concocted to conceal that Ubhi and AWS negotiated employment during JEDI. (Appx160701-160704 (AWS belated notice regarding falsified Tablehero story).)

Consequently, the CO re-opened the Ubhi conflict review and DoD asked COFC to stay Oracle's protest. (Appx1114-1123.) The CO included Gavin in the re-opened review based on the AWS proposal identifying Gavin's AWS employment. (Appx158744-158748.) In parallel, the CO considered whether AWS' hiring of Ubhi, Gavin, and several other former DoD personnel gave AWS an unfair competitive advantage. (Appx158749-158757.)

On April 9, 2019, the CO asserted that the Ubhi and Gavin misconduct had not impacted JEDI (Appx58696-58743, Appx158744-158748), and that AWS' hiring of Ubhi and Gavin conferred no advantage (Appx158749-158757). Acknowledging that Ubhi and Gavin may have violated 18 U.S.C. § 208 and 5 C.F.R. Part 2635, the CO referred them to the DoD Inspector General ("IG"), which

reportedly had already commenced a JEDI investigation. (Appx158709 (¶63), Appx158747 (¶22).)[14]

A. Ubhi's Brief AWS Hiatus.

In 2016, Ubhi temporarily left AWS to serve as a DDS "Product Director," and, in September 2017, DDS' Director Chris Lynch hand-picked Ubhi for the JEDI team. (Appx100686, Appx102793, Appx102813, Appx105254, Appx158699.) The record contains no conflict-of-interest questionnaire or NDA for Ubhi. (Appx123983-124126.) The only purported vetting of Ubhi for JEDI is a September 27, 2017 Slack exchange in which DDS counsel Sharon Woods asked who should lead DDS' interactions with interested cloud providers. (Appx103049.) Ubhi responded "make it me please," followed by: "Unless you think my past in AWS biases me." (*Id.*) Woods responded—without asking any questions—"No. You have no conflict anymore." (*Id.*)

Had DoD vetted Ubhi, DoD would have prohibited Ubhi's participation in JEDI from its inception. In late August 2017, Ubhi advised AWS that he wanted to re-join the company, and by the time Ubhi volunteered to lead the JEDI discussions with AWS' competitors, Ubhi was actively negotiating his new AWS position. (Appx158701-158706.) By October 4, 2017, Ubhi had committed to return and

[14] *See* Frank Konkel, *DoD Inspector General Clarifies Office's Role in JEDI Cloud Decision*, Defense One (August 14, 2019) https://bit.ly/341VfLO (DoD IG press release regarding JEDI investigation).

negotiated his compensation package with AWS. (Appx160913.) Ubhi's new AWS position involved "leading a technical program office" and required "broad understanding of the cloud computing landscape, including the various players." (Appx160839-160840.) On October 25, 2017, Ubhi received a letter confirming his [redacted] base salary, signing bonuses of [redacted] and [redacted], and [redacted] shares of Amazon stock (valued at roughly $950-$960 per share in the relevant period). (Appx160719-160720.)[15] Ubhi formally accepted the offer on October 27, 2017. (Appx160973-160974.) Neither Ubhi nor AWS had timely disclosed the employment negotiations to DoD. (Appx158707-158708.) Instead, Ubhi sought to conceal the misconduct by offering DoD a false recusal tale about selling his company.

1. Ubhi's Influence and Access to Information

While finalizing his compensation package to rejoin AWS, Ubhi was busy at DDS (1) advocating the single-award approach favored by AWS, (2) securing valuable information regarding DoD's needs and requirements, (3) accessing proprietary information of JEDI competitors, and (4) framing the solicitation's eventual technical requirements. In Ubhi's own words to the DDS team, "I'm reviewing and writing more documents than a college professor!" (Appx160251.)

[15] DoD did not bother to ask how much stock Ubhi owns from his prior employment with AWS (yet another prohibited conflict—5 C.F.R. §§ 2635.402, 2635.403).

First, Ubhi drove the single-award approach—an acquisition strategy favored only by AWS. (Appx9.) In a September 29, 2017 message to Ubhi, Woods said: "I get nervous when I hear these arguments about multiple clouds. I really need to better understand from you [Ubhi] why only one provider makes sense." (Appx103114.) Ubhi created the DDS single-award "one-pager" used to "really drive [the approach] home!" (Appx160151.)[16] Ubhi also steered the DoD personnel needed to get single-award approval. (Appx160096-160098.) Ubhi told Woods that "if there are people in the building [Pentagon] that [he] need[s] to go see and school, or ally," he was ready. (Appx160176.) For instance, Ubhi lobbied Jane Rathbun (Under Secretary Lord's Deputy). (Appx160096-160097, Appx160150.)[17] In another instance, Ubhi reported, "Enrique is totally on our side now," after his discussion with Enrique Uti from the Defense Innovation Unit. (Appx160098, Appx160107.) DDS also relied on Ubhi to counter the multi-cloud proponents. (Appx158739, Appx103114, Appx160100.)

Second, for weeks after accepting AWS' oral offer, Ubhi gathered competitively valuable information regarding DoD's cloud needs. For example, two days after committing to rejoin AWS, Ubhi traveled to the Space and Naval Warfare

[16] In subsequent messages, Ubhi noted the one pager "puts multi vs. single to bed once and for all hopefully (at least from a technical standpoint)." (Appx160166.)

[17] Under Secretary Lord signed the flawed single-award determination. (Appx100318.)

Systems Command ("SPAWAR") for a JEDI needs meeting, during which SPAWAR's technical expert "school[ed] [Ubhi] on the tactical edge." (Appx103165-103167, Appx103170-103174.) Ubhi messaged his DDS team about the expert's "compelling takes on looking at hybrid options, i.e. Azure [Microsoft] Stack." (Appx103174.) Ubhi also participated in numerous other needs meetings. (*See e.g.*, Appx102941 (Ubhi offering to "huddle" on technical requirements), Appx102801 (Ubhi arranging meeting with Air Force personnel), Appx103065-Appx103075 (referencing Navy JEDI meeting), Appx160140 (discussing call with Air Force), Appx160158 (discussing three "in-depth tech docs" from Air Force).

In mid-September 2017, while negotiating AWS employment, Ubhi helped set up the DDS Google drive—a "repository for *everything*" JEDI related. (Appx102910.) Ubhi persuaded DoD participants "to data dump everything into the Google Folder." (Appx102986, Appx158699.) Ubhi managed untold amounts of nonpublic and acquisition sensitive JEDI-related information through the Google drive. (*See* Appx105532-105533.) At some point prior to rejoining AWS, Ubhi

synced the Google Team Drives to his laptop. (Appx607.)[18] The record lacks any investigation into what Ubhi did with that data.[19]

Third, after committing to rejoin AWS, Ubhi also interjected himself in the JEDI requirements drafting. As the CO's review acknowledged, Ubhi drafted and revised the ultimate JEDI requirements statement, the Joint Requirements Oversight Council Memorandum ("JROCM"), which "was essential to begin the process of drafting the Statement of Objectives and the RFP." (Appx160345-160347, Appx160777, Appx158715-158716 (¶73).)

Although the CO's no-impact determination asserts that DDS did not establish any key JEDI requirements during Ubhi's tenure (Appx158721-158722), the record evidences otherwise. The limited Google drive documents DoD produced confirm that Ubhi and DDS devised and edited material that DoD ultimately incorporated into the solicitation's Statement of Objectives ("SOO"). For example, the October 2017 "Problem Statement"—which Ubhi helped draft (Appx160782, Appx102985-

[18] DDS employee Jordan Kasper's Declaration (Appx604-607) indicates that Ubhi synced the Google team drive to his laptop to work offline. When Google drive syncs documents to work offline: "These are then treated as local files on the computer, so your important stuff is always up to date on every computer you own (and in the cloud)." Cameron Summerson, *How to Sync Your Desktop PC with Google Drive (and Google Photos)*, How-To Geek (July 21, 2017), https://bit.ly/2MLOQ1A.

[19] AWS did not implement any form of firewall to shield Ubhi from the JEDI Proposal team until six months after he rejoined AWS, when, on May 11, 2018, AWS circulated an email directing Ubhi and the AWS JEDI Teams to avoid communication. (Appx124546-124548 (¶¶6, 14).)

102986, Appx103053, Appx103006)—imposed a two minute "storage provisioning time" (Appx1706), and the final SOO likewise provides two minutes as the "time to spin up object storage." (Appx100620.)[20]

Ubhi also worked on JEDI's gated approach. (Appx103123.) Ubhi referred to the Problem Statement as the "gating factor." (Appx103053 ("So the problem stmt is gating factor").) The early Problem Statement metrics include, among other measures, network availability and resource availability (computing, storage, database)—the exact subjects covered by Gate 1.1. Ubhi also worked on "differentiators" that evolved into the gates. (Appx160237 (Ubhi: "So we need to come up with those 5-8 'differentiators' that help us meet mission better right … i.e. high availability, built-in redundancy and fail-over, true elasticity, AI\ML managed services available \'out of the box\'.").)

2. AWS Also Conceals the AWS-Ubhi Employment Negotiations.

Record documents establish AWS' knowledge regarding both Ubhi's central JEDI role as AWS courted him and Ubhi's failure to recuse himself as required. When Jennifer Chronis—AWS Director for DoD Programs, responsible for all aspects of AWS' JEDI proposal (Appx160811)—emailed Lynch on September 25,

[20] *Compare* also Appx1706 (October 2017 Problem Statement allowing two minutes for the "Virtual Machine Provisioning Plan") *with* (Appx100620 (final SOO allowing the same time to "provision new VM").)

2017 to schedule a JEDI meeting, Lynch responded, "adding Deap on our team to help get something scheduled." (Appx100699-100701.) Chronis acknowledged the response. (*Id.*) Shortly afterward, on October 2, 2017 (while AWS and Ubhi discussed his offer), Ubhi emailed the AWS team stating that he was "running point on all [JEDI] industry touch points." (*Id.*) AWS did not alert DoD of the employment negotiations as required. 48 C.F.R. § 3.104-8(b).

On October 18, 2017 (*two weeks after Ubhi had orally committed to return to AWS*), the AWS JEDI team visited DDS for a meeting, which Ubhi attended for DoD. (Appx158699.) Neither AWS nor Ubhi informed DDS that Ubhi had committed to rejoining AWS. A few days later, Ubhi submitted his resume to AWS describing his DDS work as "[l]eading the effort to migrate the entire Department of Defense enterprise to the commercial cloud…." (Appx160785, Appx160845.)

B. Gavin Accepts AWS' Offer to Lead Federal Business Development, Attends a JEDI Meeting, Obtains Source Selection Information, and Then Misrepresents His JEDI Participation.

AWS also negotiated employment with Gavin, a senior Navy official involved in JEDI, whose responsibilities included providing acquisition guidance, oversight, and policy expertise. (Appx158753, Appx124539, Appx124549.) Gavin (like Ubhi) participated in JEDI even after accepting AWS' offer.

In the summer of 2017, Gavin consulted with ethics counsel about engaging with defense contractors for future employment. (Appx158746-158747,

Appx160801-160802.) From August 2017 to early 2018, Gavin engaged with an AWS recruiter and Chronis about his post-government plans. (Appx158746-158747, Appx160802-160803.)

On January 11, 2018, Gavin belatedly advised the Navy of his AWS employment discussions and requested recusal from AWS matters. (Appx160806.) A few days later, Gavin interviewed for an executive-level position, received AWS' offer on March 29, and accepted on April 2. (Appx158746.) Gavin apparently did not advise DoD that he had accepted AWS' offer, and the record lacks evidence of his employment package.

On April 5, 2018, after accepting AWS' offer and despite his earlier recusal, Gavin attended a source selection sensitive JEDI meeting. (Appx158746-158747.) Three months later, Gavin joined AWS as a Principal handling "business, technology, and strategic development for federal AWS customers." (Appx124549, Appx160801-160803.) AWS did not instruct Gavin to avoid JEDI-related matters until July 26, 2018, and AWS did not circulate a "formalized firewall" email until July 31, 2018. (Appx124539.) Both Gavin and Chronis confirm that they discussed JEDI prior to the firewall. (Appx124550-124551, Appx124553, Appx56.)

AWS' Mitigation plan, including the October 8, 2018 Gavin declaration, contains incorrect statements. AWS claimed its firewalls "prevent any exchange of information related to JEDI between … Gavin and any AWS employees who are

currently, have previously, or will in the future participate in the JEDI proposal." (Appx124537.) But, as noted, Chronis and Gavin admitted to having JEDI discussions. (Appx124553, Appx160813 (¶11).)

Gavin also misstated his JEDI involvement and access to nonpublic, competitively useful information. In AWS' proposal, Gavin declared that he participated only in a fall 2017 JEDI meeting and did not access any "information that could conceivably provide a competitor an unfair competitive advantage…." (Appx124549-124550, Appx160803 ("I did not receive any nonpublic information about the JEDI procurement").) The CO, however, knew Gavin's statements were false based on his participation in the April 5, 2018 JEDI meeting, during which the attendees received and discussed the draft Acquisition Strategy, containing, among other procurement sensitive information, competitively-valuable cost estimates. (Appx158754, Appx158746-158747 (¶¶10, 16, 24-25).)

Despite finding that Gavin had violated FAR 3.101-1 and potentially 18 U.S.C. § 208, the CO deferred to the false assurances of AWS and Gavin that (1) Gavin lacked competitively-valuable information and (2) the untimely firewall purportedly prevented Gavin from sharing any JEDI information. (Appx158754.)

C. DeMartino Participates in JEDI Despite Direction to Avoid AWS Matters.

DeMartino served as a consultant for AWS through January 2017, when he became Deputy Chief of Staff for the Secretary of Defense. (Appx105231-105233.)

In March 2017, DeMartino transitioned to serve as the DSD Chief of Staff. (*Id.*) DeMartino reportedly declared income from AWS through August 2017—the same month in which Secretary Mattis visited AWS to learn its cloud capabilities.[21]

Due to his financial ties with AWS, DeMartino received a letter from DoD's Standards of Conduct Office ("SOCO") in April 2017 counseling DeMartino not to work on matters involving AWS. (Appx104345.) DeMartino, nevertheless, participated in JEDI from its inception. (Appx105233.) Eight months later—after DoD received Freedom of Information Act ("FOIA") requests raising concerns about DeMartino's JEDI involvement—DeMartino belatedly sought approval from SOCO and SOCO instructed DeMartino to recuse himself. (*Id.*)

As the DSD Chief of Staff, DeMartino routinely and materially participated in JEDI. DeMartino obtained and edited JEDI briefings on behalf of the Secretary of Defense and DSD, directed JEDI activities, and participated in JEDI strategy meetings covering the Acquisition Strategy, Security Strategy, Business Case, and single versus multiple-award approach. (Appx104351-104353, Appx104366-103468, Appx104390, Appx102926, Appx105676-105677, Appx105541, Appx103315-103316.) DeMartino supported DoD's efforts to garner external approval for the single-source approach. (Appx104366-104368.) DeMartino also

[21] Pete Sweeney, *Amazon Pentagon ties may receive greater scrutiny*, Reuters (Aug. 16, 2018), https://www.reuters.com/article/uk-usa-pentagon-breakingviews/breakingviews-amazon-pentagon-ties-may-receive-greater-scrutiny-idUSKBN1L10AS.

revised the JEDI industry day briefing and press communications. (Appx104402-104404, Appx103831, Appx103880, Appx103319.) DoD never obtained an NDA for DeMartino or screened him for conflicts.

In a decision that spans less than one page, the CO concluded that DeMartino's conflicts had no impact on JEDI based on the assumption that his role was "ministerial." (Appx100685.) No citation to or explanation of the materials supporting this conclusion appears in the record. The CO did not talk to DeMartino or review his emails, JEDI documentation, or SOCO discussions. (Appx105686, Appx105695, Appx105239 (¶33 ("there are relatively few documents that I considered in my investigation")).)

IV. COFC Agrees DoD Violated The Law But Finds No Competitive Prejudice.

After the remand to address the Ubhi misrepresentations infecting the record, COFC denied Oracle's motion for judgement and granted the DoD and AWS cross-motions. (Appx4.) Specifically, COFC agreed with Oracle that DoD's single-award approach violated the law because Under Secretary Lord relied on an inapplicable exception to the prohibition on large, single-source IDIQ awards. (Appx42-45.) COFC recognized that clause H2 would allow DoD to add new services to the contract throughout performance, and these services "could not be identified as 'specific tasks,' much less priced, at the same time as award." (*Id.*) Accordingly, "there is a logical disconnect between claiming that prices are 'established in the

contract' for 'specific tasks' while simultaneously acknowledging that those tasks, and their accompanying prices, do not yet exist." (Appx44.)

Nevertheless, COFC found that the unlawful solicitation did not prejudice Oracle. (Appx45-52, Appx62.) COFC held that Oracle would not have a substantial chance of receiving award because Gate 1.2 would appear in any re-solicitation for multiple awards. (Appx45-52.)

With regard to the JEDI procurement officials and AWS misconduct, COFC observed that "the CO concluded that at least two DoD officials disregarded their ethical obligations by negotiating for AWS employment while working on this procurement." (Appx53.) COFC recognized that "the individuals, the company, and the agency were slow to identify the potential this [misconduct] created …, particularly as it might relate to a procurement of this magnitude, and less than aggressive in heading off potential harm." (Appx62.) Nevertheless, COFC deferred to the CO's conclusion that the DoD officials' misconduct and AWS' hiring of Ubhi and Gavin did not impact the procurement. (Appx53-60.)

SUMMARY OF ARGUMENT

Few government contracts cases have caught the public's attention like JEDI. Established public corruption ties between (at least) three directly involved federal officials and one offeror (AWS) combined with a prohibited single-award approach that will lock DoD to one vendor for ten years, have yielded independent watchdog

alarm, sparked several (bi-partisan) Congressional rebukes, and necessitated an ongoing IG investigation. A remand to DoD to resolicit JEDI lawfully and restore the public trust in this high dollar acquisition is both required and needed. Oracle asks that the Court reverse COFC's decision for three independent reasons.

First, COFC correctly found that DoD violated 10 U.S.C. § 2304a(d)(3) by soliciting this $10 billion IDIQ contract, with near constant technology refresh requirements, as a single award. But, after declaring the single-award acquisition unlawful, COFC found that Oracle (one of the largest cloud providers in the world, a substantial federal cloud provider, and a JEDI competitor) did not suffer competitive prejudice. COFC relied on government counsel's belated claims that DoD would structure JEDI security the exact same way in a re-solicitation for multiple awards. Despite aptly characterizing counsel's argument as "Rayel on the facts," COFC relied on counsel's supposition, violating fundamental administrative law principles: "a federal court generally goes astray if it decides a question that has been delegated to an agency if that agency has not first had a chance to address the question." *Smith v. Berryhill*, 139 S. Ct. 1765, 1779-80 (2019) (reversing because a court "should allow the agency to address any residual substantive questions in the first instance").

It is no small irony that DoD premised much of its defense before COFC on deference purportedly due agency decisionmakers, but when it came to whether

Oracle suffered prejudice from DoD's violation of the single-award prohibition, government counsel urged COFC to decide how DoD would structure the multiple-award procurement.

Equally problematic, the record counters the supposition that DoD would apply the same gates that felled all but the world's two largest cloud providers in a new, multiple-award competition. Instead, a sensible agency would consider (even heed) the experience and best practices of the government as a whole, Congress' criticism, and FedRAMP's prohibition on using authorization as a barrier to competition. Regardless, whether Oracle exceeded Gate 1.2 in September 2018 has no bearing on whether Oracle can compete in a corrected, reopened competition. Oracle can do so.

Second, COFC erred in finding Gate 1.2 enforceable. DoD knew this requirement reduced the field to two providers (AWS and Microsoft) yet took no steps to comply with statutory constraints on restricting competition to a limited number of sources. DoD also violated the law by applying FedRAMP requirements earlier than DoD required and, indeed, at a time that FedRAMP itself *prohibits*. DoD further failed to comply with statutory provisions on imposing qualification requirements. COFC's treatment of the specific statutory requirements implicated by Gate 1.2 all but reads the requirements out of existence. Because COFC leveraged its flawed Gate 1.2 finding as a rationale for disregarding several Oracle

arguments, this error necessitates remand to address Gate 1.2 and several other issues.

Finally, COFC correctly noted the numerous ethical improprieties present in the procurement:

> The facts on which Oracle rests its conflicts of interest allegations are certainly sufficient to raise eyebrows. The CO concluded that at least two DoD officials disregarded their ethical obligations by negotiating for AWS employment while working on this procurement. Through lax oversight, or in the case of Ubhi, deception, DoD was apparently unaware of this fact. AWS, for its part, was too prepared to take at face value assurances by Mr. Ubhi that he had complied with his ethical obligations.

(Appx53, Appx55 (finding "well-supported" CO's conclusion that "Gavin violated FAR 3.101-1, and possibly violated 18 U.S.C. § 208 and its implementing regulations"), Appx56 (declaring Ubhi's misconduct "disconcerting," violative of FAR 3.101-1, and potentially 18 U.S.C. § 208).

COFC, however, broke from precedent, and deferred to the CO's flawed determination that the admitted misconduct did not corrupt the procurement:

> The limited question, however, is whether any of the actions called out make a difference to the outcome. And in particular, the even narrower question before the court is whether the CO's conclusion of no impact is reasonable.

(Appx53, Appx54 (n.11).) To be certain, the Procurement Integrity Act ("PIA") and FAR Part 9 (contractor-side conflicts) contemplate deference to the CO. But Oracle's allegations establish violations of even more significant laws that neither

the CO nor COFC can waive. 48 C.F.R. § 3.104-2(b) (cautioning agencies that PIA is just one statute addressing such conduct).

Section 208 of Title 18 and various related FAR and Office of Government Ethics ("OGE") regulations set an "objective standard of conduct" that agency officials cannot waive, relax, or alter. *United States v. Mississippi Valley Generating Co.*, 364 U.S. 520, 548-49, 565 (1961) (declaring contract invalid "to guarantee the integrity of the federal contracting process and to protect the public from corruption which might lie undetectable..."). Thus, where an official violates section 208, the conflicted participation in government business establishes the harm and the underlying contractual action is unenforceable:

> As *Mississippi Valley* makes clear, it is the potential for injuring the public interest created by a conflict of interest that requires invalidation of the tainted contract. It therefore is immaterial whether the particular taint has or has not in fact caused the government any financial loss or damages. What the statute condemns is the inevitable taint of the contract itself that results when it is the product of a conflict of interest.

K & R Eng'g Co., Inc. v. United States, 616 F.2d 469, 475 (Ct. Cl. 1980). Despite these and numerous other similar cases (including bid protests), COFC allowed JEDI to stand, providing judicial imprimatur to that which the law condemns.

ARGUMENT

I. Standard Of Review

When reviewing a COFC ruling on cross-motions for judgment on the administrative record, the Court applies *de novo* the standard of review set forth in

5 U.S.C. § 706. *Weeks Marine, Inc. v. United States*, 575 F.3d 1352, 1358 (Fed. Cir. 2009). Under this standard, a reviewing court shall set aside a procurement action if "(1) the procurement official's decision lacked a rational basis; or (2) the procurement procedure involved a violation of regulation or procedure." *Id.* (quotation omitted); *see also Palantir USG, Inc. v. United States*, 904 F.3d 980, 989 (Fed. Cir. 2018) (affirming injunction against contract award under protested solicitation). The Court limits its review of the decision to the agency record. *Fla. Power & Light Co. v. Lorion*, 470 U.S. 729, 743-44 (1985) (a court must base its review "on the record the agency presents").

II. After Correctly Finding That DoD Violated 10 U.S.C. § 2304a(d)(3), COFC Applied The Wrong Prejudice Test And Usurped The Agency's Role On Remand.

In 2008, Congress prohibited use of large, single-award IDIQ contracts absent a head-of-agency determination that one of four narrow exceptions existed. As relevant here, section 2304a(d)(3)(B) permits a single-award IDIQ contract valued over $112 million if "the contract provides only for firm, fixed price task orders or delivery orders for … services for which prices are established in the contract for the specific tasks to be performed." 10 U.S.C. § 2304a(d)(3)(B); 48 C.F.R. § 16.504(c)(1)(ii)(D). Documents DoD first produced in the COFC protest establish DoD's recognition that the cloud "offerings are not static and will be updated overtime [sic] both in terms of available services and applicable pricing."

(Appx108721 (1115).) To that end, JEDI includes a bespoke clause, allowing the awardee to continually add new services to the contract, at later determined prices. (Appx100740.) COFC correctly found that DoD violated 10 U.S.C. § 2304a(d)(3) by soliciting the 10-year, $10 billion IDIQ contract, with near constant technology refresh requirements, as a single award. (Appx42-45.)

Yet, rather than remand for DoD to compete JEDI lawfully, COFC declared that Oracle lacked prejudice based on the assumption that any multiple-award solicitation would include Gate 1.2, which Oracle did not meet before proposal submission. (Appx46 ("If Oracle cannot meet Gate Criteria 1.2 as currently configured, it is thus not prejudiced by the decision to make a single award.").) COFC's prejudice determination contains fatal legal and factual errors.

First, COFC applied the wrong prejudice test: "To show that it was prejudiced by an error, the protester must demonstrate 'that there was a substantial chance it would have received the contract award but for the [agency's] errors.'" (Appx38 (citations omitted).) Although a *post-award protester* demonstrates prejudice by showing "a substantial chance for award," a *different* standard applies where the protester timely challenges a solicitation. *Orion Tech., Inc. v. United States*, 704 F.3d 1344, 1348 (Fed. Cir. 2013) (distinguishing *Weeks Marine* because protester did not challenge solicitation). In pre-award protests, "non-trivial competitive injury which can be redressed by judicial relief" establishes prejudice. *Weeks Marine,* 575

F.3d at 1361-62. To show injury, the protester need not even submit a proposal; the law requires only a timely procurement structure challenge that, if remedied, could result in a rebid under which the protester could compete. *CGI Fed. Inc. v. United States*, 779 F.3d 1346, 1348-52 (Fed. Cir. 2015) (finding standing to challenge solicitation despite not bidding).

Oracle is an actual JEDI bidder, which, prior to the initial proposal deadline, challenged the unlawful single-award approach and sought a reopened procurement structured for multiple contract awards. (Appx104878, Appx156052.) That during the course of Oracle's protest, DoD excluded Oracle's initial proposal based on an evaluation under the challenged *single*-award procurement has no legal or factual relevance. *Cf. Rothe Dev. Corp. v. Dep't of Defense*, 413 F.3d 1327, 1334 (Fed. Cir. 2005) (quotation omitted) (assessing standing "as of the commencement of the suit"). COFC agreed that DoD's single-award approach violated the law and that DoD might reissue the solicitation for multiple awards. (Appx45-46.) DoD, accordingly, wrongfully deprived Oracle of the opportunity to compete under a multiple-award solicitation—a prejudicial injury. *See Palantir U.S.G., Inc. v. United States*, 129 Fed. Cl. 218, 283-89 (2016), *aff'd*, 904 F.3d 980 (Fed. Cir. 2018) (applying "non-trivial competitive injury standard" to pre-award challenge); *see also Alfa Laval Separation, Inc. v. United States*, 175 F.3d 1365 (Fed. Cir. 1999) (reversing COFC judgment based on flawed prejudice finding); *WinStar Comms.,*

Inc. v. United States, 41 Fed. Cl. 748, 763-64 (1998) (finding unlawful single-award approach prejudiced protester).

Second, COFC erred gravely in accepting government counsel's supposition about the hypothetical parameters of a multiple-award solicitation: "In other words, although [Gate 1.2] presumes a single award, the only logical conclusion is that, if multiple awards were made, the security concerns would ratchet up, not down." (Appx46.) How DoD would structure JEDI under a multiple-award solicitation with task order competition appears nowhere in the record and COFC could not fill this gap: "For purposes of affirming no less than reversing its orders, an appellate court cannot intrude upon the domain which Congress has exclusively entrusted to an administrative agency." *SEC v. Chenery Corp.*, 318 U.S. 80, 88 (1943); *I.C.C. v. Brotherhood of Locomotive Eng'rs*, 482 U.S. 270, 282 (1987) (holding court may not affirm based on discretionary decision agency did not make "since that would remove the discretionary judgment from the agency to the court").

Despite this established law, COFC relied on government counsel's argument that DoD would impose Gate 1.2 in a multiple-award procurement. (Appx51; Appx2296-2297 (116:1-117:18).) The following exchange occurred during oral argument:

> THE COURT: I understand that we're on Rayel on the facts as opposed to the administrative record.

> MR. RAYEL: Well, yeah, you asked me, Your Honor. So, yes, I mean, this isn't all --
>
> THE COURT: No, I understand.
>
> MR. RAYEL: Because, I mean, this was a single award. So the agency didn't -- I'll admit it doesn't say in Mr. Van Name's memorandum and my decision would be the same if there were multiple awards.
>
> THE COURT: Right.

(Appx2296 (115:16-25).) Government counsel's concession that DoD did not consider any gate criteria in a multiple-award context should end the matter. The law is clear—"Rayel on the facts" is not a source upon which COFC may rely.

Under the Administrative Procedure Act ("APA"), COFC may not presume how DoD would structure a multiple-award procurement as DoD must make that decision in the first instance. As COFC acknowledges, Oracle submitted "a serious proposal" (Appx39) under JEDI and would compete in a reopened competition, all that (absent the improper speculation) Oracle needed to demonstrate prejudice here.

Third, the record contradicts COFC's assumption that DoD would use Gate 1.2 in a multiple-award solicitation. DoD uses *hundreds of clouds* today (Appx100471), and the vast majority of DoD suppliers do not have the Gate 1.2 qualifications that JEDI demands. In fact, other finalized cloud-related solicitations in the record—selected by DoD for JEDI research—do not require FedRAMP authorization at the time of proposal submission. (Appx123506 (email as a service multiple-award work statement providing for FedRAMP authorization process ***to***

begin "[w]ithin 180 days of either [the FedRAMP] achieving Initial Operating Capability or BPA award, ***whichever comes later***"), Appx123613 (Navy commercial cloud solicitation requiring that offerors "***demonstrate[] experience for achieving an authorization*** to operate (ATO)"), Appx123432 (DoD cloud solicitation, requiring FedRAMP authorization ***six months after award***).

Further, FedRAMP prohibits authorization as a barrier to competition: "Federal Agencies cannot require CSPs [Cloud Service Providers] to be FedRAMP authorized as part of their RFP but can state that a CSP needs to be FedRAMP authorized once federal data is placed in the system." (Appx105291-105292.) Oracle also cited DoD guidance on the structuring of multiple-award procurements to demonstrate that DoD approaches single-award and multiple-award IDIQ procurements differently.[22] (Appx1997.) And *two Congresses* have directed DoD to rethink its JEDI approach and the associated harmful, restrictions on competition.[23] No factual basis exists for the apparent speculation that DoD would approach a remand with obstinate rigidity.

---

[22] DoD Guidelines for Creating and Maintaining a Competitive Environment for Supplies and Services in the Department of Defense at 3, 17 (Dec. 2014), at https://bit.ly/2pQbcpA (last visited 10/28/19).

[23] H.R. Rpt. No. 116-84, at 11-12 (2019) (expressing Committee on Appropriations concern with JEDI single-award approach and noting other federal agencies' multiple vendor strategy); Department of Defense and Labor, Health and Human Services, and Education Appropriations Act, 2019 and Continuing Appropriations Act, 2019, Pub. L. No. 115-245, § 8137, 132 Stat. 2981, 50-51 (2018) (requiring DoD to report JEDI acquisition strategy to "sustain competition and innovation

Fourth, COFC's no prejudice ruling fails because Gate 1.2 itself violates the law. (*See infra* at 40-48.)

Finally, even assuming *arguendo*, that the substantial chance test applies and Gate 1.2 would remain in any multiple-award solicitation, COFC asked the wrong question and consequently reached the wrong answer. It matters not whether Oracle met Gate 1.2 as of proposal submission in *October 2018.* The relevant inquiry is whether the protester has a substantial chance of securing the award in the corrected competition, i.e., whether Oracle would meet the same standard under a revised multiple-award solicitation in 2019. *COMINT Sys. Corp. v. United States*, 700 F.3d 1377, 1382 n.4 (Fed. Cir. 2012) (citing *Impresa Construzioni Geom. Domenico Garufi v. United States,* 238 F.3d 1324, 1334 (Fed. Cir. 2001)). Oracle also satisfies that test.

Oracle is among the largest cloud providers in the world and a major cloud provider to the U.S. Government. (Appx156872.)[24] Moreover, Oracle's proposal and protest showed that Oracle would satisfy Gate 1.2 by contract award and would meet the criterion in any new solicitation. (Appx156791-156792, Appx156807-

---

throughout the period of performance …, including defining opportunities for multiple cloud service providers and insertion of new technologies").

[24] Gartner identifies six major IaaS providers: Alibaba Cloud, AWS, Google, IBM, Microsoft, and Oracle. *Magic Quadrant for Cloud Infrastructure as a Service, Worldwide,* Gartner (May 23, 2018), https://www.gartner.com/en/documents/3875999/magic-quadrant-for-cloud-infrastructure-as-a-service-wor0.

156808 (evidencing Oracle had three datacenters with FedRAMP Moderate PaaS offerings at proposal submission, and FedRAMP High IaaS and PaaS authorization underway on five datacenters), Appx123981.)

Consistent with Oracle's proposal, the FedRAMP Marketplace website confirms that Oracle's Cloud Infrastructure holds the necessary FedRAMP Moderate IaaS and PaaS authorizations and has obtained "FedRAMP Ready" High status, an even higher security level than Gate 1.2 requires for five datacenters in three geographically dispersed locations.[25] "FedRAMP Ready" means the cloud provider has completed a report approved by the FedRAMP office,[26] documenting the cloud service's capability to meet FedRAMP security requirements,[27] and indicating the provider will likely obtain authorization.[28]

This Court, accordingly, should reverse the COFC judgment and either enter judgment in Oracle's favor or remand for further proceedings on prejudice.

[25] FedRAMP.gov, Database, https://bit.ly/346CRSa (last visited 10/28/19).

[26] FedRAMP.gov, Marketplace, https://www.fedramp.gov/make-the-most-of-the-fedramp-marketplace/ (last visited 10/28/19).

[27] FedRAMP.gov, FAQs, https://www.fedramp.gov/faqs/ (last visited 10/28/19).

[28] FedRAMP.gov, Marketplace, https://www.fedramp.gov/make-the-most-of-the-fedramp-marketplace/ (last visited 10/28/19).

III. Gate 1.2 Violates Procurement Law To Oracle's Prejudice, Necessitating Remand On Several Issues.

Gate 1.2 leverages FedRAMP authorization as a pre-qualification requirement by mandating that each offeror have, at proposal submission, no fewer than three existing datacenters, each supporting FedRAMP Moderate authorized offerings, and capable of automated failover. (Appx100791-100792, Appx100661 (Questions 26-27), Appx100946-100947, Appx105488-105489.) Each offeror must pass the gate to compete. (Appx105489.) Gate 1.2 violates the Competition In Contracting Act ("CICA") for several reasons.

A. Gate 1.2 Violates 10 U.S.C. § 2304.

In imposing Gate 1.2, DoD neglected CICA's mandatory J&A process, which applies *whenever* DoD has reason to conclude that its purported minimum needs "are available … from only a limited number of responsible sources…." 10 U.S.C. § 2304(c)(1); 48 C.F.R. § 6.302-1(b)(1)(ii). To proceed in these circumstances, DoD had to comply with the J&A procedures. 10 U.S.C. § 2304(f); 48 C.F.R. § 6.302-1(d); *Nat'l Gov't Servs., Inc. v. United States*, 923 F.3d 977 (Fed. Cir. 2019) (reversing COFC where agency limited competition without J&A).

DoD set Gate 1.2 knowing that it would limit competition to two offerors. Indeed, requiring offerors to meet Gate 1.2 at proposal submission (within two months of solicitation issuance) was substantively the same as stating: "Only AWS and Microsoft may compete." The government (with DoD involvement) runs the

FedRAMP process to approve cloud solutions for use by federal agencies.[29] FedRAMP maintains a Marketplace dashboard that "provides a searchable, sortable database of all cloud services that are FedRAMP authorized, FedRAMP ready, or in Process for an authorization."[30] It consequently is no secret which contractors hold FedRAMP authorizations and it certainly is no secret to DoD, whose Chief Information Officer participates on FedRAMP's primary governance and decision-making body.[31]

The record confirms that DoD devised the gated approach for the express purpose of limiting the number of proposals received. (Appx100422, Appx100504.) Internal Slack communications reveal that DoD crafted the gates to "get-to-one" awardee. (Appx103123, Appx103053.) DoD's market research showed that the gates would winnow the universe of JEDI competitors to a few providers (Appx100369), and the evaluation confirmed that only AWS and Microsoft met Gate 1.2. (Appx158649.)

DoD necessarily knew when it imposed Gate 1.2 that only two offerors had the FedRAMP authorization required at proposal submission (September 2018)—

[29] *See* FedRAMP.gov, FAQs, https://www.fedramp.gov/faqs/ (last visited 10/28/19).

[30] FedRAMP.gov, Marketplace, https://www.fedramp.gov/make-the-most-of-the-fedramp-marketplace/ (last visited 10/28/19).

[31] FedRAMP.gov, Governance, https://www.fedramp.gov/governance/ (last visited 10/28/19).

AWS and Microsoft. Gate 1.2 sidelined the other three U.S.-based large cloud providers. Google publicly acknowledged it could not compete based on this criterion, IBM protested prior to proposal submission and ultimately got excluded based on Gate 1.2, and Oracle also timely challenged the criterion. This gate (among others) led to countless articles alleging DoD wired this procurement.[32] Despite setting a criterion knowing it would limit the competition to AWS and Microsoft, DoD did not issue the J&A CICA required. 10 U.S.C. § 2304(f); 48 C.F.R. §§ 6.302-1(d), 6.303-1.

The Gate Memorandum (Appx100944-100952) is no proxy for Congress' J&A mandate. The CO did not write the memorandum, it does not contain the required contents, and neither Under Secretary Lord nor an authorized delegate approved it. (*Compare* Appx100944-100952 *with* 48 C.F.R. § 6.303-1(a)(3); 48 C.F.R. § 206.304.) COFC's determination that DoD lacked a "nefarious" purpose has no bearing. (Appx48.) Here, DoD knew (or should have known) that only two cloud providers could pass Gate 1.2, triggering CICA's J&A requirements. CICA's implementing regulations provide that where "there is a reasonable basis to conclude that the agency's minimum needs can only be satisfied by … (ii) … a limited number

[32] *See e.g.*, Paris Martineau, *How the Pentagon's Move to the Cloud Landed in the Mud*, Wired Magazine (Oct. 10, 2018), https://bit.ly/2Wm5tUM ("The Pentagon's 1,375-page winner-take-all request for proposal for JEDI is a web of restrictions and requirements that some critics allege leaves few viable candidates….").

of sources…," full and open competition does not exist and DoD must follow the J&A process. 48 C.F.R. §§ 6.302-1(b)(1)(ii), (d). Any contrary result relegates this statutory requirement to virtual irrelevance.

COFC's characterization of the competition as "full and open" because offerors without three FedRAMP authorized datacenters could technically submit a proposal, ignores that DoD deemed all such offerors ineligible to compete for the JEDI contract. (Appx158649.) This Court rejected a similar flawed view in *National Government Services, Inc.*:

> In light of the Award Limitations Policy, a responsible offeror that would exceed the workload caps is not given the same opportunity to win an award as other offerors that submitted awardable proposals. And the fact that an offeror that would exceed those caps was able to submit a proposal does nothing to address this concern.

923 F.3d at 985.

B. Gate 1.2 Violates 10 U.S.C. § 2319.

Gate 1.2 violates a separate statutory procedure triggered when DoD seeks to use a qualification requirement. Recognizing that such requirements discourage competition, Congress established mandatory procedures in 10 U.S.C. § 2319. Most notably, section 2319 requires that the agency head "prepare a written justification stating the necessity for establishing the qualification requirement and specify why the qualification requirement must be demonstrated before contract award." 10 U.S.C. § 2319(a). Section 2319 also prohibits exclusion of an offeror based on a

qualification requirement "*if the potential offeror … can meet such standards before the date specified for award of the contract*." 10 U.S.C. § 2319(c)(3). These safeguards exist "to ensure that qualification requirements are used only when … necessary to ensure product quality, reliability, and maintainability, rather than to inappropriately restrict competition." *W.G. Yates & Sons Constr., Inc. v. Caldera*, 192 F.3d 987, 992 (Fed. Cir. 1999).

Gate 1.2 contravenes the statute. The agency head did not issue a written justification explaining the necessity for Gate 1.2 or justifying its imposition at proposal submission. 10 U.S.C. § 2319(b)(1). Moreover, DoD did not allow offerors to otherwise demonstrate the ability to satisfy Gate 1.2 before the award date. *Compare id.* § 2319(c)(3) *with* Appx100792.

Section 2319 defines a "qualification requirement" as a "testing or other quality assurance demonstration that must be completed by an offeror before award of a contract." 10 U.S.C. § 2319(b). Gate 1.2 requires the offerors to have at proposal submission, three existing FedRAMP Moderate Authorized datacenters, 150 miles apart. (Appx100792.) But FedRAMP Authorized datacenters are not a JEDI Contract requirement. (Appx105495 ("[W]e are not requiring, as part of the JEDI cybersecurity plan, that the winner go through the FedRAMP process before DoD uses the final solution"), Appx105496.) Instead, DoD imposed Gate 1.2 as a "mechanism to validate" that the offerors' "core architecture" would "be able to meet

the JEDI Cloud requirements." (Appx100955.) The pre-bid quality assurance demonstration triggered section 2319, and DoD's failure to comply with the associated obligations renders Gate 1.2 invalid. *W.G. Yates*, 192 F.3d at 992-93.

COFC's reasons for declaring section 2319 inapplicable do not withstand scrutiny. It is irrelevant and wrong that Gate 1.2 does not invoke a qualified bidders list. *Id.* The qualification requirement invalidated in *W.G. Yates* did not involve a qualified bidders list. *Id*. at 993. The FedRAMP Marketplace serves as *a qualified offeror list* in any event.[33] Moreover, contrary to COFC's unsupported findings, FedRAMP authorization is "an independent, systematic requirement that DoD imposes in its procurements." (Appx50.) FedRAMP describes itself as "*a government-wide program* that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."[34]

COFC also errantly found that Oracle waived the qualification argument by purportedly not raising it until the post-hearing submission to GAO on October 18, 2019. (Appx48.) Not so. Oracle's revised and consolidated supplemental protest,

---

[33] *See* FedRAMP.gov, Database, https://bit.ly/2Wdt9dO (last visited 10/28/19).

[34] FedRAMP.gov, https://www.fedramp.gov/about/ (last visited 10/28/19). The government-wide FedRAMP authorization standards undermine COFC's reliance on *California Industrial Facilities Resources, Inc. v. United States*, 80 Fed. Cl. 633 (2008). In that case, the court found that the testing requirements did not relate to other contracts, products, or a system independent of the procurement and thus constituted specifications. *Id.* at 636, 642.

dated September 6, 2018 (before the October 9, 2018 bidding deadline), objected to Gate 1.2 as both violative of CICA and an unlawful "prequalification" requirement. (Appx104941 ("DoD also has no legitimate need for FedRAMP authorized offerings … *establishing a prequalification to compete*"), Appx104942 ("Thus, the FedRAMP *prequalification conflicts* with the commercial nature of the RFP."), Appx104941 ("DoD's latest responses to the many offeror concerns about the FedRAMP prequalification requirement are also contradictory…."); *see Palantir Techs. Inc. v. United States*, 128 Fed. Cl. 21, 41-44 (2016) (rejecting similar waiver argument).

C. Gate 1.2 Also Violates CICA's Prohibition on Unduly Restrictive Specifications.

Oracle also correctly objected to DoD's timing of demonstrating compliance with Gate 1.2—i.e., requiring each offeror to show three existing FedRAMP Authorized datacenters *at the time of proposal submission* versus a showing of how the offeror would meet the security requirements before datacenter use. Even if Gate 1.2 were a valid requirement, DoD could not impose it prior to DoD's actual needs. *See, e.g., USA Jet Airlines, Inc., Active Aero Grp., Inc.,* B-404666, Apr. 1, 2011, 2011 CPD ¶ 91 (solicitation exceeded needs by requiring certification before performance); *SMARTnet, Inc*., B-400651.2, Jan. 27, 2009, 2009 CPD ¶ 34 (requiring equipment certification at proposal submission unduly restricted

competition).[35] DoD's Gate 1.2 rationale establishes that DoD's need for the datacenters will not occur until after contract award. (Appx100947 (datacenter requirement served "to provide reliability and resiliency of services even in the unlikely circumstance that two datacenters are simultaneously affected"), Appx105487 (DDS Deputy Director testifying to same), Appx100675 (answer to Q157) ("three unclassified data centers must be online and available thirty days after … the post award kick-off event.").)

For the foregoing reasons, Gate 1.2 violates numerous statutory restrictions and the Court should reverse COFC's holding as related to Gate 1.2. Moreover, because COFC utilized Gate 1.2 as a rationale for disregarding several Oracle arguments (e.g., Oracle's assertion that Gate 1.1 also violates various statutory mandates), the Court should remand the matter for further proceedings regarding Gate 1.2, Gate 1.1, and other unaddressed arguments. (Appx19 ("The protest puts Gate Criteria 1.1, 1.2, and 1.6 at issue."); Appx46 ("We need not consider Gate Criteria 1.1, or 1.6 for that matter, because we are satisfied for reasons set out below, that Gate Criteria 1.2 is enforceable."); Appx1485-1489 (Oracle brief demonstrating that Gate 1.1 violates procurement law); Appx2006-2011 (Oracle reply). The Court,

[35] *Allied Tech. Grp., Inc. v. United States*, 649 F.3d 1320, 1331 n.1 (Fed. Cir. 2011) ("this court may draw on GAO's opinions for its application of [procurement] expertise.") (internal citation omitted).

accordingly, should reverse COFC's determination and enter judgment in Oracle's favor or remand for further proceedings.

IV. Numerous Prohibited Government Conflicts, All Tied To AWS, Corrupted The Procurement.

Multiple violations of FAR subpart 3.1, Title 18, and other ethics rules corrupt this procurement. As Professor Schooner, a leading government contracts academic, noted following the COFC decision:

> While DoD survived the protest, the judge's lengthy decision made clear that the procurement process left much to be desired, both with regard to an inordinate number of conflicts of interest—I'll stop there, *but the judge's deference to the contracting officer was as disappointing as it was unusual*—and a highly controversial and, to my mind, deeply flawed, acquisition strategy.[36]

Oracle did *not* protest run-of-the mill conflicts of interest. Instead, the record presented lies, graft, and section 208 violations. Yet, the CO—ignoring that the expenditure of public funds requires the highest degree of public trust and impeccable conduct—declared the violations had no procurement impact.

The CO's assessment contains numerous factual flaws and shortcomings. But, even more significant, the CO's decision *ignores* the very impact Congress crafted the law to prevent:

> The [conflict-of-interest] statute is directed at an evil which endangers the very fabric of a democratic society, for a democracy is effective

[36] Jason Miller, *DoD's Win In Federal Court Doesn't Mean JEDI Is Out Of The Woods, Experts Say*, Federal News Network (Aug. 2, 2019), https://federalnews network.com/reporters-notebook-jason-miller/2019/08/dods-win-in-federal-court-doesnt-mean-jedi-is-out-of-the-woods-experts-say/.

> only if the people have faith in those who govern, and that *faith is bound to be shattered when high officials and their appointees engage in activities which arouse suspicions of malfeasance and corruption*.

Mississippi Valley, 364 U.S. at 562; 48 C.F.R. § 3.101-1 ("*avoid strictly ... even the appearance of a conflict*"). Congress did not design section 208 and its objective test (with no impact analysis or agency deference) to protect DoD or avoid lost DoD effort. Instead, Congress recognized something far greater is at stake. COFC erred when holding that a CO could legally (much less rationally) find that section 208 violations did not impact a procurement: "It is this inherent difficulty in detecting corruption which requires that contracts made in violation of [the conflict-of-interest statute] be held unenforceable, even though the party seeking enforcement ostensibly appears entirely innocent." *Mississippi Valley*, 364 U.S. at 565. Reversal is necessary because COFC has "affirmatively sanction[ed] the type of infected bargain which the statute outlaws and … depriv[ed] the public of the protection which Congress has conferred." *Id.* at 563.

A. Ethics Laws Applicable to Procurement

The FAR mandates that the government conduct business "in a manner above reproach … with complete impartiality and with preferential treatment for none," and it demands personnel adhere to an "impeccable standard of conduct" and "avoid strictly … even the appearance of a conflict of interest." 48 C.F.R. § 3.101-1. The PIA and its regulations (FAR 3.104) provide but one strand of the statutory and

regulatory web designed to safeguard U.S. citizens from the corruption that plagues other governments. The FAR PIA provisions alert agencies to "other statutes and regulations that deal with the same or related prohibited conduct," including 18 U.S.C. § 208 and its regulations at 5 C.F.R. Part 2635. 48 C.F.R. § 3.104-2(b). Some of the rules (like the PIA) allow for CO discretion to address a violation, while others (like 18 U.S.C. § 208) set objective tests, recognizing that the covered misconduct causes harm in all circumstances.

Section 208—deemed by OGE as the "*cornerstone of the executive branch ethics program*"[37]—prohibits any Executive employee from participating "personally and substantially" in a "particular matter" that he knows will impact the financial interests of an organization with whom he is negotiating or has any arrangement regarding prospective employment. 18 U.S.C. § 208. Any contract formed under such influences is *void*: "Section 434 [predecessor to section 208] requires nonenforcement, and this is true even though the conflict of interest was caused or condoned by high government officials." *Mississippi Valley*, 364 U.S. at 563, 566.[38]

[37] *Report to the President and to Congressional Committees on the Conflict of Interest Laws Relating to Executive Branch Employment* 28 (2006), at https://bit.ly/2Pg2jQS (last visited 10/28/19).

[38] *Mississippi Valley* involved a prior, narrower version of section 208, codified at 18 U.S.C. § 434. *See K & R Eng'g*, 616 F.2d at 473.

The PIA and FAR require government employees, who are "seeking employment" with a contractor to notify the agency ethics official immediately and, either reject the overture or recuse themselves from any matter involving that contractor. *See* 41 U.S.C. § 2103(a); 48 C.F.R. § 3.104-3(c). The PIA also requires the contractor to notify the government where the contractor has reason to suspect that the official failed to recuse himself. 41 U.S.C. § 2103(c); 48 C.F.R. § 3.104-8(b). Unlike section 208, the CO investigates suspected PIA violations and determines if the "possible violation has any impact on the pending award or selection of the contractor." 48 C.F.R. § 3.104-7(a). The CO here conducted a PIA investigation and wrongly found "no impact." (Appx158696, Appx158744.)

Also, FAR Subpart 9.5's Organizational Conflict of Interest rules charge COs with ensuring that contract awards avoid conflicts of interest. 48 C.F.R. Subpart 9.5. Where, as here, the facts suggest that a competitor may have an unfair competitive advantage due to relationships with former government officials, FAR Subpart 3.1 controls with guidance from Subpart 9.5. *See Northrop Grumman Sys. Corp.*, B-412278.8, Oct. 14, 2017, 2017 CPD ¶ 312. The JEDI CO errantly determined that AWS' hiring of Ubhi and Gavin did not create an unfair competitive advantage. (Appx158757.)

B. The CO and COFC Cannot Sanction the Section 208 Violations Infecting JEDI.

JEDI suffers from corruption of a high order, including section 208 violations. Neither the CO nor DoD has discretion to proceed with a procurement indifferent to such misconduct. *Mississippi Valley*, 364 U.S. at 559.

1. COFC Had to Determine Whether the Procurement Officials Violated Section 208.

COFC's refusal to consider section 208 broke with Supreme Court, Federal Circuit, and COFC precedent and provided judicial imprimatur to a corrupt contract process under IG review. *Compare* Appx54 (n.11) *with Mississippi Valley*, 364 U.S. at 551-59; *CACI, Inc.-Fed. v. United States*, 719 F.2d 1567, 1576-78 (Fed. Cir. 1983) (conducting *de novo* section 208 analysis in bid protest); *Express One Int'l, Inc. v. United States Postal Serv.*, 814 F. Supp. 93, 97 (D.D.C. 1992) (rejecting "special deference" on protested government conflict); *TRW Envtl. Safety Sys., Inc. v. United States*, 18 Cl. Ct. 33 (1989) (applying *Mississippi Valley* in bid protest).

Here, little doubt exists that Ubhi and Gavin violated section 208. The CO recognized that Ubhi participated personally and substantially in JEDI during the fall of 2017, while negotiating employment with AWS, a JEDI "interested party." (Appx158709, Appx158716.) The CO noted that Ubhi concealed his employment discussions with AWS and fabricated his reason for subsequent recusal. (Appx158701-158704 (¶¶29-33).) DoD has conceded that Gavin participated

personally and substantially in JEDI *after* he accepted employment with AWS in early 2018. (Appx1696.)

Ubhi and Gavin each had essentially the same conflict as the government official in *Mississippi Valley*, i.e., a financial interest in a prospective contractor. Ubhi joined AWS as a Senior Manager and Gavin as a Principal for Federal Technology. (Appx160719-160720, Appx158746.) In addition to a substantial salary and massive signing bonuses, Ubhi received [redacted] shares (then worth over [redacted] dollars) of Amazon stock. (Appx160719-160720.) The CO never asked about Gavin's employment terms, which likely also involved a significant salary, bonuses, and substantial stock. (Appx1001 (n.33), Appx158711.)

COFC's reliance on the CO's finding that neither Ubhi nor Gavin steered the competition for AWS is misplaced. (Appx56-58.) First, the law does not require additional evidence of corruption beyond the section 208 violation. *See Mississippi Valley*, 364 U.S. at 559. Second, that the CO did not find any *quid pro quo* or other bias reflects the unremarkable fact that corrupt actors typically mask their conduct. *Id.* at 565. Third, section 208 does not criminalize a public official's participation *only* where there is evidence of a *quid pro quo* or bias in favor of the prospective employer.

By deferring to the CO, COFC broke from established law and injected uncertainty into an objective standard. The law required COFC to consider whether

Ubhi's and Gavin's conduct violated section 208, and void the procurement if it did. COFC's failure to do so requires reversal and remand for further proceedings.

C. The CO's No-Impact Determinations Also Cannot Survive APA Review.

Even if COFC properly limited its review to whether the CO's determination was reasonable, this Court also should reverse the decision because the CO's "no impact" determinations lacks a rational basis.

1. The Ubhi No-Impact Determination Missed Material Facts and Contains Flawed Findings.

First, COFC could not affirm the CO's determination because the CO proceeded without obtaining the results of the IG's investigation into Ubhi and Gavin. The CO recognized that Ubhi and Gavin likely violated section 208 and referred them to the DoD IG for further investigation, which is ongoing. (Appx158709 (¶63), Appx158746 (¶22).) The CO's no-impact determination was arbitrary and capricious because she "entirely failed to consider an important aspect of the problem"—i.e., whether Ubhi and Gavin violated section 208, corrupting the procurement and any associated contract. *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). [39]

Second, although COFC purported to affirm the CO's reasoning, COFC deemed the CO's determinations rational based on COFC's own conflicting

[39] Prior criminal proceedings are not a necessary predicate to considering such violations in the civil context. *K & R Eng'g.*, 616 F.2d at 474 (absence of section

reasoning. For instance, COFC held "that the CO correctly concluded that, although Mr. Ubhi should have never worked on the JEDI Cloud procurement, his involvement did not impact it." (Appx59.) To reach that conclusion, COFC made a series of findings, including that Ubhi's involvement occurred *too late* to influence the single-award decision:

> We are left with the firm conviction that the agency was headed in the direction of a single award from the beginning, indeed probably before Mr. Ubhi was enlisted to participate in the JEDI Cloud project. The CO is fundamentally correct: if there was a high speed train headed toward the single award decision, Mr. Ubhi was merely a passenger on the train, and certainly not the conductor.

(Appx59.) But the CO based her determination on the opposite conclusion that Ubhi's involvement occurred *too early*, i.e., "all the key decisions for the JEDI Cloud procurement, such as the actual RFP terms and whether to award one or multiple contracts, were made well after Mr. Ubhi recused himself." (Appx158719, Appx158721 (claiming that "single versus multiple award decision was still being vigorously debated" in April 2018).)

These contrary descriptions of Ubhi's involvement (the CO saying Ubhi was too early and COFC saying Ubhi was too late) evidence the severe fallacy in treating corruption this way. Regardless, under the APA standard, an agency decision must

208 conviction did not change need to disaffirm contract); *cf. United States v. ACME Process Equip. Co.*, 385 U.S. 138, 146 (1966) (contract void due to Anti-Kickback Act violation notwithstanding criminal acquittal).

stand or fall based on the agency's stated rationale. *OMV Med., Inc. v. United States*, 219 F.3d 1337, 1344 (Fed. Cir. 2000) (reversing and remanding COFC decision that affirmed CO award decision based on COFC's own rationale).

Third, the Ubhi no-impact determination also fails because the CO's rationale "runs counter to the evidence before the agency." *State Farm*, 463 U.S. at 43. For instance, the CO's consideration of Ubhi's involvement in the single-award decision ignores record evidence showing he deliberately, systematically, and successfully influenced individuals to adopt the single-award approach and that DoD's commitment to that approach after Ubhi's tenure never shifted. Tellingly, Ubhi met with individual members and the CESG as a whole to convert them to the single-award approach, and following his efforts, DDS counsel stated, "[s]ingle is now assumed … really glad you [Ubhi] were here this week" (Appx160229), and Deputy Director Van Name announced: "Everyone that matters is now convinced." (Appx160239.) None of these critical facts are acknowledged or considered by the CO, and her determination that Ubhi did not impact the single-award decision cannot stand in light of them.

The CO also contends that Ubhi "did not have the technical expertise to substantially influence JEDI Cloud requirement[s]," or the "level of technical understanding necessary to make the case for some of the most important foundational decisions." (Appx158719-158720.) But before the CO learned of

Ubhi's lies, the CO and Van Name testified to Ubhi's technical expertise before GAO. (Appx105445 ("Right, again, Deap is a technical expert. That's why he was hired on to the DDS team."), Appx105571 ("[T]he technical expert that was pegged to support this -- support aspects of this was Deap Ubhi.").) The record also confirms Ubhi's highly technical role. (Appx160621 (Ubhi email to Google: "we expect our conversation tomorrow to be highly technical (as it should be!).")))

The CO also errantly found "no evidence that … Ubhi's participation … had any substantive impact on the procurement decisions or documents," based on his early tenure in JEDI. (Appx158723.) But Ubhi edited material in October 2017 that DoD ultimately included in the solicitation. (*See supra* at 21 (n.20).) Ubhi also contributed to the DDS drafts of the JROCM (Appx158715-158716 (¶73), Appx160345, Appx160777), and discussed and drafted "differentiators" that became the gate criteria and other solicitation requirements. (*See e.g.,* Appx160237 (Ubhi: "So we need to come up with those 5-8 'differentiators'…).)

Finally, the CO finds "no evidence that … Ubhi obtained or disclosed any competitively useful nonpublic information." (Appx158723.) The CO reaches this flawed conclusion by declaring: (i) the vast government information worthless "because the acquisition was in its predecisional planning phase"; and (ii) competitor information Ubhi received not useful despite proprietary markings. (Appx158715-158716.) The CO does not grapple with Ubhi's meetings with DoD end-users about

their JEDI needs—needs like services for the tactical edge, an important solicitation factor. (Appx100796, Appx103172 (two days after committing to AWS, Ubhi describing SPAWAR as "schooling [him] on the tactical edge."), Appx160158 (Air Force meeting yielding "more in depth tech docs.") Recognizing the competition-sensitive information generated during Ubhi's tenure, DDS counsel cautioned Ubhi to be careful not to reveal information when talking to industry: "Need to be in receive only mode. Be careful not to reveal info from our side that is not public knowledge." (Appx160133.) In another instance, as to documents Ubhi reviewed just moments earlier, DDS counsel described them as "close hold" and "Acquisition sensitive," and directed: "No support contractors and only government folks that are read in so we protect integrity acquisition [sic]." (Appx160315.)

Further, prior to rejoining AWS, Ubhi synced the JEDI team's Google drive to his laptop. (Appx607.) Despite the purported significant security issues surrounding the JEDI cloud, the CO did not explore why Ubhi synced the drive to his laptop or what happened to the synched documents (many, as noted above, containing technical cloud information from user agencies). The CO ultimately only considered a handful of documents on the Google drive and left everything else Ubhi created, reviewed, revised, and downloaded unconsidered. (Appx158729-158735.) The record is silent as to what Ubhi did with the JEDI files because the CO did not even ask.

For all these reasons, the CO's Ubhi investigation was inadequate and the no-impact determination arbitrary and capricious.

2. The DeMartino No-Impact Determination Also Fails Against APA Standards.

This Court should set aside the DeMartino no-impact determination because the CO "entirely failed to consider an important aspect of the problem" and her conclusions "run counter to the evidence." *State Farm*, 463 U.S. at 43.

Absent authorization, a federal official may not participate in a matter involving "a person with whom he has a covered relationship" when "the circumstances would cause a reasonable person with knowledge of the relevant facts to question his impartiality…." 5 C.F.R. § 2635.502(a); 48 C.F.R. § 3.104-2(b)(2). The proscription generally lasts one year after the covered relationship ends, but Executive Order 13770 extends the restriction to two years for political appointees (like DeMartino). 82 Fed. Reg. 9333 (Jan. 28, 2017); 5 C.F.R. § 2635.502(b)(1)(iv). Given that DeMartino consulted for AWS through January 2017 and joined DoD in early 2017 (Appx100685), these rules prohibited DeMartino's participation in matters involving AWS before January 2019.

Due to his financial ties with AWS, DoD's SOCO issued an ethics letter in *April 2017*, warning DeMartino not to work on AWS matters without approval. (Appx104345.) DeMartino ignored the letter and participated in JEDI from its inception. (Appx105233.) More than eight months elapsed before DeMartino

finally sought approval from SOCO, apparently due to press inquiries and FOIA requests questioning his role. (*Id.*) In April 2018, SOCO instructed DeMartino to recuse himself immediately. (*Id.*)

The CO discounted DeMartino's defiance of the ethics rules by reasoning that his JEDI involvement was "ministerial and perfunctory in nature." (Appx100685.) In a single paragraph affirming the CO's determination, COFC concludes that the "CO considered all of the relevant facts regarding Mr. DeMartino's involvement." (Appx55.) Not so.

The CO never consulted SOCO, which both cautioned against DeMartino's involvement and later directed his JEDI recusal. (Appx105674-105675.) The CO did not collect DeMartino's documents, interview DeMartino, or even review SOCO's prior ethics warning before perfunctorily declaring that DeMartino complied with the rules. (Appx105669-105670.) Had the CO sought the relevant records she would have learned the opposite was true: DeMartino participated in JEDI contrary to SOCO's instruction and ethics laws. (Appx104345, Appx105233.) Despite re-opening her conflicts review in February 2019 due to the Ubhi lies, the CO still did not interview DeMartino, review his emails, or consider his work product. (Appx105686, Appx105695, Appx105239.)

Even the few DeMartino documents collected in response to Oracle's protest contradict the CO's characterization of DeMartino's role as "ministerial and

perfunctory." Just the contrary, these documents show that DeMartino participated personally and substantially in JEDI, shaping JEDI from a policy level all the way down to specific acquisition details. DoD concedes that the DSD, on whose behalf DeMartino oversaw JEDI, participated "personally and substantially." (Appx104862.) As the DSD Chief of Staff, DeMartino obtained and edited JEDI briefings on behalf of the Secretary of Defense and DSD, directed JEDI activities, and conducted meetings about the Acquisition Strategy, Security Strategy, Business Case, the single-award approach, among other matters. (Appx104351-104353, Appx104366-104368, Appx104390, Appx102926, Appx105676-105677, Appx105541, Appx103315-103316.)

DeMartino also directed efforts and strategy about the best way to garner external approval for the acquisition approach. (Appx104366-104367.) DeMartino coordinated with DoD's Cost Assessment and Program Evaluation office to obtain information to claim projected savings from the single source approach, among other data. (*Id.*) DeMartino received and commented on JEDI acquisition sensitive information. (*See* Appx103310, Appx103315-103316.) DeMartino revised the JEDI industry day briefing and coordinated and shaped the JEDI press strategy. (Appx104402-104404, Appx103831, Appx103880, Appx103319.) DeMartino met and substantively discussed JEDI with the DSD routinely. (Appx160139,

Appx160282, Appx160285.) But since the CO never interviewed DeMartino or collected his documents, the scope of such communications remains unknown.

For its part, COFC made alternate findings. COFC concluded that "Mr. DeMartino did not have a voice in whether DoD should use a single or multiple award approach and did not craft the substance of the evaluation factors." (Appx55.) The CO's investigation contains no such findings. (Appx100685.)

Accordingly, because the CO did not reasonably investigate DeMartino's improper involvement in JEDI, the no-impact determination fails under the APA.

3. The CO Irrationally Determined that AWS' Employment of Gavin Had No Impact.

The CO also arbitrarily found that AWS' hiring of Gavin, who the CO found to have participated personally and substantially in JEDI after accepting a job offer with AWS, did not provide AWS an unfair competitive advantage. The FAR directs COs to "'figure out potential organizational conflicts of interest before a solicitation is issued and either mitigate potential conflicts before award, include restrictions in the solicitation to avoid the conflict of interest, or disqualify an offeror from a competition.'" *NetStar-1 Gov't Consulting, Inc. v. United States*, 101 Fed. Cl. 511, 521 (2011) (quoting Ralph C. Nash & John Cibinic, *Conflicts of Interest: The Guidance in the FAR*, 15 No. 1 Nash & Cibinic Rep. ¶ 5 (2001)).

When a contractor hires a government official with procurement sensitive information, the law presumes a prejudicial unfair advantage unless the contractor

effectively mitigated the conflict. *See id.* at 529 (internal quotation and citation omitted) (recognizing "[a] long line of cases holds that when a potential significant [conflict] is identified, prejudice stemming from that [conflict] is presumed," and protester need not show "the information possessed by its competitor specifically benefitted the latter's proposal. That too is presumed."); *Int'l Res. Grp.*, B-409346.2 *et al.*, Dec. 11, 2014, 2014 CPD ¶ 369 (same).

Here, the CO found that Gavin obtained competition-sensitive information when (despite his earlier recusal and acceptance of AWS' job offer), Gavin attended the April 5, 2018 JEDI meeting and discussed the draft Acquisition Plan. (Appx158754, Appx158746-158747 (¶¶10, 16, 24-25.) For its part, AWS did not instruct Gavin to avoid JEDI-related matters until July 26, 2018, more than one month after Gavin joined AWS, and AWS did not circulate a "formalized firewall" email until July 31, 2018. (Appx124539.) Both Gavin and Chronis admitted they discussed JEDI prior to the firewall. (Appx124550-124551 (¶10), Appx160813 (¶11).) Indeed, COFC noted that Gavin and Chronis improperly communicated about JEDI after Gavin joined AWS, and stated, "we do not know exactly what Mr. Gavin communicated to AWS' JEDI proposal team lead prior to the information firewall." (Appx55-56.)

The recognition that Gavin and Chronis communicated about JEDI should have been dispositive regarding AWS' unmitigated and presumptively prejudicial

unfair competitive advantage. Yet, COFC held otherwise. That conclusion rests entirely on COFC's independent determination that Gavin lacked any competitively-valuable information when he joined AWS. (Appx56, Appx61.) This material, factual predicate to COFC's affirmance of the CO's decision contradicts the CO's own findings. (Appx158746-158747.) COFC has no authority to uphold the CO's decision under APA review based on a different rationale. *See OMV Med.*, 219 F.3d at 1344.

Accordingly, the CO's decision about Gavin's conflict and employment with AWS, and COFC's associated review, also fail against the APA.

CONCLUSION

The Court should reverse COFC's decision, vacate the judgment, and enter judgment and a permanent injunction in Oracle's favor against the award of a contract under JEDI (or against new task orders or options under any JEDI award) or remand the matter for further proceedings before COFC. *See CGI Fed.*, 779 F.3d at 1354 (reversing bid protest denial and remanding for further proceedings); *SMS Data Prod. Grp., Inc. v. United States*, 853 F.2d 1547, 1556-57 (Fed. Cir. 1988) (reversing denial and discussing relief where agency failed to meet competition requirements).

Dated: October 28, 2019

Respectfully submitted,

ARNOLD & PORTER KAYE SCHOLER LLP

/s/ Craig A. Holman

Craig A. Holman
Kara L. Daniels
Dana E. Koffman
Nathaniel E. Castellano
Amanda J. Sherwood
601 Massachusetts Ave., N.W.
Washington, D.C. 20001
(202) 942-5722
craig.holman@arnoldporter.com

Counsel for Oracle America, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on November 1, 2019, a true and correct copy of the foregoing Non-Confidential Opening Brief of Plaintiff-Appellant Oracle America, Inc. was served upon counsel of record via email through the Court's CM/ECF system.

/s/ Craig A. Holman
Craig A. Holman

CERTIFICATE OF COMPLIANCE

This Brief complies with the type-volume limitation of Federal Circuit Rule 32(a). The Brief contains 13,951 words, excluding the parts of the Brief exempted by Federal Rule of Appellate Procedure 32(f) and Federal Circuit Rule 32(b).

/s/ Craig A. Holman
Craig A. Holman

ADDENDUM

INDEX TO ADDENDUM

In the United States Court of Federal Claims

No. 18-1880C
(Filed: July 12, 2019)

* *

ORACLE AMERICA, INC.,

Plaintiff,

v.

THE UNITED STATES,

Defendant,

and

AMAZON WEB SERVICES, INC.,

Intervenor.

* *

ORDER

Pending in this pre-award bid protest are the parties' cross-motions for judgment on the administrative record. The court held oral argument on the parties' cross-motions on July 10, 2019. Following argument, the court indicated to the parties that we would issue an order stating our decision on the motions with a supporting opinion to follow shortly thereafter. The court now orders the following.

Because the court finds that Gate Criteria 1.2 is enforceable, and Oracle concedes that it could not meet that criteria at the time of proposal submission, we conclude that it cannot demonstrate prejudice as a result of other possible errors in the procurement process. We conclude as well that the contracting officer's findings that an organizational conflict of interest does not exist and that individual conflicts of interest did not impact the procurement were not arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. Plaintiff's motion for judgment on the administrative record is therefore denied. Defendant's and intervenor's

respective cross-motions for judgment on the administrative record are granted.

Entry of final judgment is deferred pending the issuance of our supporting opinion.

s/Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge

The following pages contain Confidential material and have been removed from this Non-Confidential Addendum

In the United States Court of Federal Claims

No. 18-1880 C
Filed: July 19, 2019

ORACLE AMERICA, INC.
Plaintiff

v.

THE UNITED STATES
Defendant

JUDGMENT

and

AMAZON WEB SERVICES, INC.
Defendant-Intervenor

Pursuant to the court's Opinion, filed July 19, 2019, denying plaintiff's motion for judgment on the administrative record and granting defendant's and defendant-intervenor's cross-motions for judgment on the administrative record,

IT IS ORDERED AND ADJUDGED this date, pursuant to Rule 58, that judgment is entered in favor of defendant. No costs.

Lisa L. Reyes
Clerk of Court

By: s/ Debra L. Samler

Deputy Clerk

NOTE: As to appeal to the United States Court of Appeals for the Federal Circuit, 60 days from this date, see RCFC 58.1, re number of copies and listing of all plaintiffs. Filing fee is $505.00.

In the United States Court of Federal Claims

No. 18-1880C
(Filed: July 19, 2019)
(Re-Filed: July 26, 2019)[1]

* *

ORACLE AMERICA, INC.,

Plaintiff,

v.

THE UNITED STATES,

Defendant,

and

AMAZON WEB SERVICES, INC.,

Intervenor.

* *

Pre-award bid protest; 10 U.S.C. § 2304a(d)(3)-(4) (2012); 48 C.F.R. § 16.504(c) (2018); single award determination; gate criteria; qualification requirement; individual conflict of interest; organizational conflict of interest.

Craig A. Holman, Washington, DC, for plaintiff. *Kara L. Daniels*, *Dana E. Koffman*, *Amanda J. Sherwood*, and *Nathaniel E. Castellano*, of counsel.

William P. Rayel, Senior Trial Counsel, United States Department of Justice, Civil Division, Commercial Litigation Branch, Washington, DC, with whom were *Joseph H. Hunt*, Assistant Attorney General, *Robert E. Kirschman, Jr.*, Director, *Patricia M. McCarthy*, Assistant Director, for defendant. *Christina M. Austin* and *Andrew Bramnick*, Washington

[1] This opinion was originally issued under seal to permit the parties an opportunity to propose redactions by July 25, 2019. The government and intervenor proposed two redactions; plaintiff opposed one. Because both proposed redactions address protected information, the court adopts both. The parties also identified several possible clerical mistakes or omissions; to the extent we agree that they were clerical mistakes or omissions, and not substantive changes, we corrected them. RCFC 60(a).

Headquarters Service & Pentagon Force Protection Agency, United States Department of Defense, Office of General Counsel, of counsel.

Daniel R. Forman, Washington, DC, for intervenor. *Robert J. Sneckenberg*, *Olivia L. Lynch*, *James G. Peyster*, *Christian N. Curran*, and *Gabrielle Trujillo*, of counsel.

OPINION

BRUGGINK, *Judge*.

This protest involves the Department of Defense's ("DoD") Joint Enterprise Defense Infrastructure ("JEDI") Cloud procurement. In the JEDI Cloud procurement, DoD is seeking an enterprise cloud services solution that will accelerate DoD's adoption of cloud computing technology. Oracle America, Inc. ("Oracle") initially filed this as a pre-award bid protest on December 6, 2018. After it was excluded from the competition during the protest and DoD completed several conflicts of interest determinations, Oracle amended its complaint. It currently has three primary challenges. First, it argues that the decision to use a single award as opposed to multiple awards was a violation of law. This argument has two components because the decision to use a single award had to be made both by an Under Secretary of Defense and independently by the contracting officer ("CO"). Second, it argues that the use of certain gate criteria, the application of which led to Oracle's exclusion, were improper for various reasons. Third, it contends that conflicts of interest on the part of DoD employees and Amazon Web Services, Inc. ("AWS"), one of the other bidders, prejudicially affected the procurement. AWS has intervened.

The parties filed cross-motions for judgment on the administrative record. The matter is fully briefed, and we held oral argument on July 10, 2019. As stated in the court's July 12, 2019 order, because we find that Gate Criteria 1.2 is enforceable, and Oracle concedes that it could not meet that criteria at the time of proposal submission, we conclude that it cannot demonstrate prejudice even if the procurement was otherwise flawed. Plaintiff's motion for judgment on the administrative record is therefore denied. Defendant's and intervenor's respective cross-motions for judgment on the administrative record are granted.

One feature of the protest makes resolution somewhat awkward. Although we ultimately conclude that Gate Criteria 1.2 is enforceable and thus a comprehensive answer to all of plaintiff's arguments, it is necessary to provide a virtually complete recitation of the facts and arguments because Oracle contends that two of the asserted errors—the decisions adopting a single award approach and the conflict of interest determinations—influenced the formulation of Gate Criteria 1.2. The critical question as to those two arguments, therefore, is whether, if Oracle is correct on the merits, they impacted the formulation of the criteria on which Oracle concedes it fails. We ultimately conclude that they did not taint the formulation of that criteria or other aspects of the solicitation.

BACKGROUND

DoD is ready to adopt an enterprise cloud services solution.[2] It plans to award the vast majority of DoD's cloud services business to a single vendor. Although DoD has been developing the JEDI Cloud procurement for several years, we enter the development timeline in August 2017, when the Secretary of Defense traveled to Seattle, Washington, and Palo Alto, California, to visit cloud services companies. Administrative Record ("AR") Tab 91 at 5955.

Following this trip, Deputy Secretary of Defense Patrick Shanahan sent a memorandum on September 13, 2017, to the secretaries of the military departments. He emphasized that certain technologies "are [1] changing the character of war; (2) commercial companies are pioneering technologies in these areas; [and] (3) the pace of innovation is extremely rapid." *Id.* The Deputy Secretary concluded that "accelerating [DoD's] adoption of cloud computing technologies is critical to maintain our military's technological

[2] The agency defines "cloud" as "[t]he practice of pooling physical servers and using them to provide services that can be rapidly provisioned with minimal effort and time, often over the Internet." Administrative Record ("AR") Tab 25 at 478. The agency explains, "The term is applied to a variety of different technologies (often without clarifying modifiers), but, for the purpose of this document, cloud refers to physical computing and storage resources pooled to provide virtual computing, storage, or higher-level services." DoD explains that "commercial cloud means that a commercial cloud service provider is maintaining, operating, and managing the computing, networking, and storage resources that are being made available to customers. Depending on the contract, the commercial cloud service provider may be performing in commercial facilities or on premises." *Id.*

advantage." *Id.* He explained that the adoption of cloud computing technology was "a Department priority" in which "[s]peed and security are of the essence." AR 5956. His memo went on to broadly outline the steps to set the JEDI Cloud procurement in motion.

To devise a strategy to accelerate the adoption of cloud services, the Deputy Secretary established the Cloud Executive Steering Group. The group would brief the Deputy Secretary on a bi-weekly basis on progress toward adoption of cloud computing technology. The Cloud Executive Steering Group consisted of Chair Ellen Lord, Under Secretary of Defense for Acquisition, Technology, and Logistics; Director Chris Lynch, Defense Digital Service; Director Will Roper, Strategic Capabilities Office; Managing Partner Raj Shah, Defense Innovation Unit Experimental; Executive Director Joshua Marcuse, Defense Innovation Board; and advisor John Bergin, DoD Chief Information Officer Business Technology Office.

Adoption of an enterprise cloud would proceed in two phases. First, DoD would use "a tailored acquisition process to acquire a modern enterprise cloud services solution that can support unclassified, secret, and top secret information." *Id*. The Deputy Secretary tasked the Defense Digital Service, under Mr. Lynch, with leading phase one. The Defense Digital Service is a team within DoD's United States Digital Service. Members of Defense Digital Service dedicated to the JEDI Cloud procurement at that time included Mr. Lynch, legal counsel Sharon Woods, industry specialist Deap Ubhi, Deputy Director Timothy Van Name, and engineer Jordan Kasper. In the second phase, the Cloud Executive Steering Group would "rapidly transition select DoD Components or agencies to the acquired cloud solution," using cloud services as extensively as possible. *Id*.

Early Commitment to a Single Award and Tailored Acquisition Plan

The Cloud Executive Steering Group held a meeting the day after the Deputy Secretary issued his memo.[3] AR Tab 86. In attendance were Mr. Lynch; Ms. Woods; a Defense Digital Service engineer; Mr. Ubhi; two representatives from the Strategic Capabilities Office; Mr. Shah; Mr. Marcuse; and a "C3 cyber and business systems AT&L" representative. AR 5927. The meeting notes record that Mr. Lynch stated "[o]ver time there ha[ve] been considerable changes to the tech world outside of the DoD that are so fundamental that they are now serious constraints on delivering the

[3] The government's AR index states this meeting occurred on September 14, 2017. The meeting notes do not state the date of the meeting.

mission of defense." *Id.* Mr. Lynch further noted, "If we feel uncomfortable moving forward, then we are probably headed in the right direction." *Id.* The group noted that "Sec Def/ DSD is afraid of vendor lock in." AR 5928.

The notes include the following comment: "Avoid specifying that there is a single vendor. This will create perception issues with vendors already in use." *Id.* This suggests that, from the beginning, the expectation was that there would be a single award.

The Cloud Executive Steering Group met again on September 28, 2017, and discussed when the problem statement draft, RFI, Business Case Analysis, and RFP would be developed. AR Tab 87. The meeting notes read: "Questions and inquiries form [sic] industry should be directed to Deap [Ubhi]." AR 5932. Procurement documents, such as the ones discussed at this meeting, were developed and stored in a Google Drive accessible by certain DoD personnel, including the Cloud Executive Steering Group and Defense Digital Service team.

In between meetings, members of the Defense Digital Service discussed the progress of the JEDI Cloud project on the agency's internal communication medium, Slack.[4] During this period, Defense Digital Service members discussed what to include in the problem statement. For instance, on October 2, 2017, they discussed whether "metrics" should be included in the problem statement or if they were too difficult to articulate at that point. Ms. Woods wrote, "Let me put the metrics in this context. The agreed upon measures drive what acquisition strategy will be approved. So, if multiple cloud providers can meet the metrics, then we don't get to one. The metrics drive how we solve the problem." AR 3123.

The "Draft Problem Statement" was complete October 3, 2017. The draft explained that DoD's "current computing and storage infrastructure environment and approach . . . is too federated, too slow, and too uncoordinated to enable the military to rapidly utilize DoD's vast information to make critical, data driven decisions." AR 60089. DoD

[4] "Slack is a communication tool utilized by [the Defense Digital Service], and other authorized collaborators, to facilitate timely communication and coordination of work activities . . . . Slack channels are comprised of distinct groups of Slack users and are organized by purpose." AR Tab 221 at 58699. The government provided an index of user names and the message timestamps can be converted using an epoch time converter.

envisioned acquiring services that "seamlessly extend[] from the homefront to the tactical edge."[5] *Id.* The authors concluded that DoD "cannot achieve this vision without a coordinated enterprise approach that does not simply repeat past initiatives." *Id.* The document repeated the ills of fragmented infrastructure in nearly every paragraph.

On October 5, 2017, the Cloud Executive Steering Group convened again.[6] According to the meeting notes, Under Secretary Lord explained that more than "600 cloud initiatives across" DoD currently exist and that the "cloud initiative is about implementing an enterprise approach rather than an uncoordinated eclectic approach that has resulted in pockets of cloud adoption." AR 5933. Mr. Lynch contributed: "[a] [s]ingle cloud solution [is] necessary for this enterprise initiative to be successful and allow DoD to achieve its mission objectives with cloud adoption." AR 5934.

Slack messages among the Defense Digital Service team members refer to a late October 2017 Cloud Executive Steering Group meeting at which Mr. Ubhi, along with others, argued for a single award approach. AR 60100, 60229. The messages suggest that attendees either already favored a single award or were persuaded at the meeting.

On October 27, 2017, Defense Digital Service's Mr. Kasper sent the Deputy Secretary a two-page update on the DoD Cloud efforts and the draft Request for Information ("RFI"). AR Tab 51. Under "Acquisition Strategy Approach," the update anticipated an Indefinite Delivery, Indefinite Quantity ("IDIQ") contract and "[f]irm-fixed pricing with commercial catalog." AR 4324. On "Single versus Multiple Providers," the update stated: "General consensus is that we should press forward with a single provider approach for now . . . The [Cloud Executive Steering Group] acquisition strategy is focusing on a single-award." AR 4325. The primary reasoning for a single rather than multiple award was "reduced complexity, ensuring security of information to the greatest degree possible, ease of use and limited barriers to entry, virtual private cloud-to-virtual private cloud peering, and seamless,

[5] DoD defines tactical edge as "[e]nvironments covering the full range of military operations, including, but not limited to forces deployed in support of a Geographic Combatant Commander or applicable training exercises, on various platforms . . . and with the ability to operate in austere and connectivity-deprived environments." AR Tab 25 at 479.

[6] The principal attendees were: Under Secretary Lord; Mr. Bergin; Mr. Lynch; Mr. Shah; Mr. Marcuse; and Dr. Roper. The notes list Ms. Woods among additional participants.

secure sharing of data across the enterprise through cloud peering." *Id*.

Development of the Tailored Solicitation Approach and Needs

DoD issued an RFI to the commercial world on October 30, 2017, inquiring into available cloud computing services. DoD emphasized its need to rely on "the cloud provider(s)" for all levels of data classification from the homefront to the tactical edge. AR 5936. Among other items, DoD asked for information about responders' third-party marketplace, failover and data replication architecture, ability to operate "at the edge of connectivity," and for an example of "a large commercial customer with worldwide presence that has migrated to your infrastructure and platform services." AR 5937-38.

Before DoD received responses, it completed a summary of the JEDI Cloud procurement effort to date on November 6, 2017. This included an "Acquisition Strategy" description: "Single-award [IDIQ] contract using full and open competitive procedures. A single Cloud Service Provider (CSP) to deliver services for cloud computing infrastructure and platform services. Up to ten-year ordering period." AR 5957.

The agency received RFI responses on November 17, 2017. Many responders questioned whether a single award would offer the best cost model, whether one vendor could possibly be the leader in all areas, and whether a single vendor would devalue investment made by existing vendors. Oracle argued that a single award would stifle adoption of market-driven innovation. Microsoft concurred: "DoD's mission is better served through a multi-vendor cloud approach," because "competition drives innovation," and offers "greater flexibility." AR 1545. Microsoft urged DoD to preserve its flexibility and agility to adopt the latest cloud technology and to avoid "a single point of failure." *Id*. IBM likewise responded: "Limiting the DoD to a single cloud provider will negatively impact DoD's source access to innovative cloud offerings and increase risk of deployment failure." AR 1983. Google argued that DoD must not become "beholden to monolithic solutions or single cloud providers." AR 1924.

AWS, on the other hand, argued that, although multiple awards might decrease the likelihood of protests, a single award would increase consistency, interoperability, and ease of maintenance. AWS posited that commercial parity requirements would guarantee innovation. AWS was not alone in noting that single awards had been used in the past and that they might offer advantages.

On December 22, 2017, the Joint Requirements Oversight Council issued a memo to twenty-two DoD stakeholders to address "Joint Characteristics and Considerations for Accelerating to Cloud Architectures and Services." AR Tab 17. The council "accept[ed] the Defense Digital Service cloud brief" and acknowledged that "accelerating to the cloud [is] critical in creating a global, resilient, and secure information environment that enables warfighting and mission command." AR 321. The memo repeated DoD's expectations: data exchange across all classification levels and DoD components; an environment that is scalable and elastic; security from persistent adversary threats; use to the tactical edge; and industry-standard high availability.

The memo identified "cloud characteristics and elements of particular importance to warfighting missions." AR 323. Those characteristics were: cloud resiliency without a single point of failure, support of DoD's cyber defenses, enabling cyber defenders, and role-based training. The attached presentation referred to a single "cloud provider." AR 330.

On January 8, 2018, Deputy Secretary Shanahan circulated a memorandum to the secretaries of the military departments providing an "Accelerating Enterprise Cloud Adoption Update." AR Tab 94. This memo stated that the Cloud Executive Steering Group had provided recommendations as requested and that "the Deputy Chief Management Officer (DCMO), in partnership with Cost Assessment and Program Evaluation, Chief Information Officer, and Defense Digital Service, [would now] take the lead in implementing the initial acquisition strategy." AR 5978. The memo also directed the Deputy Chief Management Officer to establish a Cloud Computing Program Manager. The Deputy Secretary directed the Deputy Chief Management Officer and the Chief Information Officer to work with "the Services; the Under Secretary of Defense for Intelligence; and the Under Secretary of Defense for Acquisition, Technology, and Logistics to build cloud strategies for requirements related to military operations and intelligence support." *Id.*

Three months later, DoD released the first draft RFP and held an industry day on March 7, 2018. DoD provided the draft RFP for "early and frequent exposure to industry of the Department's evolving requirement." AR 5995. DoD anticipated awarding a single award IDIQ that would issue firm fixed-price task orders. DoD would seek Infrastructure as a Service ("IaaS") and Platform as a Service ("PaaS").

IaaS is "[t]he capability provided to the consumer to provision

processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications." AR Tab 25 at 478. DoD explained, "The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)." *Id.*

PaaS is "[t]he capability provided through software, on top of an IaaS solution, that allows the consumer to replicate, scale, host, and secure consumer created or acquired applications on the cloud infrastructure." AR 479. As with IaaS, DoD explained, "The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations." *Id.*

The draft included a specially crafted "New Services" clause, providing that "DoD may acquire new products and/or services from the contractor for capabilities not currently provided in the Cloud Services Catalog Price List under this contract." AR 6013. The draft also introduced the concept of Factor 1 Gate Criteria, a number of metrics which offerors would have to meet to advance to consideration of other factors. Three of the criteria are at issue in this protest. Gate Criteria 1.1 required the offeror to "provid[e] a summary report for the months of January and February 2018 that depicts each of the four metric areas detailed below." AR 6083. Gate Criteria 1.2 required the offeror to have no fewer than three physical, unclassified data center locations at least 150 miles apart and to document network availability. An additional criteria (later numbered 1.6) required the offeror to provide a marketplace for both native and third-party programs.

On March 27, 2018, the Cloud Computing Program Office completed its Market Research Report, which DoD used to "inform the overall acquisition strategy." AR 366. Market research included vendor meetings held from October 12, 2017 to January 26, 2018, focus sessions within DoD and with industry leaders, intelligence community meetings, and the RFI.

The Cloud Computing Program Office found that "market research indicate[s] that multiple sources are capable of satisfying DoD's requirements for JEDI Cloud." *Id.* The office found, however, that "[o]nly a few companies have the existing infrastructure—in both scale and modernity of processes—to support DoD mission requirements, worldwide." AR 369. The office concluded that "[i]f the JEDI Cloud contract is sufficiently

flexible and requires maintaining technical parity with commercial solutions," DoD would be able to apply cloud solutions to the tactical edge. AR 366. The office also found that providers' information security and ability to operate in disconnected environments were still growing and that a "robust, self-service marketplace" is "essential." AR 369. The office found that the responses did not clearly demonstrate how multiple clouds benefitted the agency's security needs.

The Cloud Computing Program Office completed the Business Case Analysis on April 11, 2018. The summary provides that the Business Case Analysis, Acquisition Strategy, Statement of Objectives, and Cybersecurity Plan form the foundation of the procurement. The problem statement indicated that DoD's operations are hampered by fragmented, outdated computing and storage infrastructure; tedious, manual management processes; and lack of interoperability, seamless systems, standardization, and automation. "In short, DoD's current computing and storage infrastructure critically fails DoD's mission and business needs." AR 403. This gloomy assessment led to eight objectives: available and resilient services; global accessibility; centralized management and distributed control; ease of use; commercial parity; modern and elastic computing; storage; and network infrastructure, fortified security, and advanced data analytics.

The office turned to available alternatives. The analysis of alternatives was "based on outcomes when the overarching goal is for JEDI Cloud to host 80% of all DoD applications that currently reside in DoD on-prem[ise] centers, existing cloud offerings, and legacy systems." AR 405. The office assumed that the solution required "significant transformation," because "DoD needs to extricate itself from the business of installing, managing, and operating data centers." AR 406. The office also assumed that a high degree of integration is necessary and using multiple vendors would increase complexity and cost.

Four alternatives were considered: DoD retaining 80% of the workload; DoD splitting its workload with JEDI Cloud; a single JEDI Cloud provider managing 80% of the workload; and multiple JEDI Cloud providers splitting 80% of the workload. The office concluded that a single JEDI Cloud provider would fulfill seven of the eight objectives and partially fulfill the global accessibility objective. Multiple JEDI Cloud providers, on the other hand, would meet only four objectives and partially meet four objectives. The DoD-focused options all failed at least one objective.

The office did not see any disadvantage to adopting a single JEDI Cloud provider approach. It found that global accessibility is problematic in any scenario because the technology is evolving. This section concluded: "There are significant overlaps in the commercial cloud services offered by the various providers, such that any provider selected will meet the majority of Department needs." AR 410.

The office acknowledged that DoD would "benefit from the commercial parity, investment, innovation, and technical evolution of commercial cloud offerings driven by industry, and additional commercial service offerings [that] will be made available" if it chose a multiple award approach. AR 411. Ultimately, it concluded that this approach would be "technically more complex." *Id.* Using multiple vendors would "significantly complicate[] management," "raise[] the risk profile," compromise ease of use, create new security vulnerabilities, and impede interoperability. *Id.* The office recommended that the agency "proceed with the acquisition of services from a single" cloud services provider. AR 412.

The analysis set out nine "high-level programmatic success criteria" mapped to the eight objectives. AR 415. Among the criteria were "a commercial [cloud services provider] where total usage by DoD does not exceed 50% of the provider's total network, computing, and storage capacity;" "ongoing parity with commercial offerings for unclassified applications for pricing;" a "scalable, resilient, and accredited" cloud services solution that can manage needs from DoD's users; and ability to operate in disconnected and austere environments. AR 415-16.

The analysis addressed seven program risks. Oracle highlights the sixth risk assessed, which it believes indicates a connection between the desire for a single awardee and the metrics selected for the gate criteria:

> The JEDI Cloud program schedule could be negatively impacted if source selection extends beyond the planned timeline due to an unexpected number of proposals or lengthy protest delays. To mitigate this risk, the solicitation will use a gated evaluation approach that includes "go/ no-go" gate criteria. Offerors must meet the established minimum criteria in order to be considered a viable competitor. Also, [the Cloud Computing Program Office] will communicate those criteria through a draft solicitation process.

AR 422.

On April 16, 2018, DoD issued the second draft RFP, including a chart with DoD's responses to questions received from industry. Although many potential offerors questioned the gate criteria, DoD made only a few changes. For Factor 1.1, the relevant measuring period remained January through February 2018. For Factor 1.2, the location of the three data centers was broadened from the continental United States to "the Customs Territory of the United States." AR 6241. DoD added that the proposed data centers must contain hardware used to provide IaaS and PaaS services "that are FedRAMP Moderate compliant." *Id.* Factor 1.6, a marketplace containing native services and third-party services, remained unchanged, as did the "New Services" provision, which allowed the introduction of new services during the ten-year contract period.

CO's Justification of Single Award Approach

The agency was required to explain its decision to use a single award for the JEDI Cloud procurement. The agency must satisfy both a regulatory requirement for the CO to consider whether a multiple award was appropriate and a statutory requirement for the head of the agency to determine if a single award was permissible in an acquisition of this size. We discuss those requirements below.

On July 17, 2018, the CO issued her memo stating that the rationale for using a single award IDIQ contract overcame the multiple award preference stated in FAR 16.504(c) (2018). That regulation provides that, when planning an IDIQ acquisition, the CO must determine whether multiple awards are appropriate, giving preference to multiple awards to the "maximum extent practicable." FAR 16.504(c). The regulations set out six exceptions to the single award preference; if the CO determines any of those conditions exist, the agency "must not" use a multiple award approach. *Id.*

The CO relied on three exceptions to the multiple award preference. First, "[b]ased on the CO's knowledge of the market, more favorable terms and conditions, including pricing, will be provided if a single award is made." AR 455. Second, "[t]he expected cost of administration of multiple contracts outweighs the expected benefits of making multiple awards." *Id.* Third, "[m]ultiple awards would not be in the best interests of the Government." *Id.*

The CO explained that a vendor is more likely to offer favorable price terms and make the initial investment to serve DoD's needs if it can be assured it will recoup its investment through packaging prices for classified

and unclassified services. The CO next observed that administering multiple contracts is costlier and less efficient. Finally, she reasoned that "[p]roviding the DoD access to foundational commercial cloud infrastructure and platform technologies on a global scale is critical to national defense and preparing the DoD to fight and win wars." AR 461-62. "Based on the current state of technology, multiple awards . . . i) increase security risks; ii) create impediments to operationalizing data through data analytics, machine learning (ML), and artificial intelligence (AI); and iii) introduce technical complexity in a way that both jeopardizes successful implementation and increases costs." AR 462.

She explained that "multiple awards increase security risks," because a single cloud can offer data encryption but with the added benefit of seamless data transfer. *Id*. Multiple clouds, on the other hand, would "frustrate the DoD's attempts to consolidate and pool data so data analytics capabilities can be maximized for mission benefit." AR 463. The CO iterated that "[o]ne of the primary goals of" the procurement "is to decrease barriers to adoption of modern cloud technology to gain military advantage." *Id.* She found that multiple clouds inherently raise barriers, because they require additional training, interoperability, more space, and more investment. In the conclusion, the CO stated that a single award solution "achieves better security, better positions the DoD to operationalize its data, and decreases barriers to rapid adoption." AR 464.

The Under Secretary's Justification of Single Award Approach

Just two days after the CO signed her single award determination, on July 19, 2018, Under Secretary Lord signed a separate Determination and Findings ("D&F") stating that DoD was authorized to award the JEDI Cloud contract to a single cloud services provider. This separate determination was required, because in 2008 Congress prohibited DoD, among other agencies, from awarding task order contracts in excess of $112 million[7] to a single source. National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, § 843(a)(1), 122 Stat. 3, 236 (2008) ("Limitation on Single Award Contracts"). This added another level of scrutiny unique to large single award procurements in addition to the multiple award preference.

[7] 41 U.S.C. § 1908 (2012) (statutory inflation adjustment requirement); Inflation Adjustment of Acquisition-Related Thresholds, 80 Fed. Reg. 38293-01, 38997 (July 2, 2015) (adjusting the $100 million single award prohibition).

Exceptions are permitted, however, when the head of the agency determines that one of four exceptions to the single award prohibition exists. 10 U.S.C. § 2304a(d)(3)(A)-(D) (2012).

The Under Secretary based the D&F on one exception to the statutory prohibition: "the contract provides only for firm, fixed price (FFP) task orders or delivery orders for services for which prices are established in the contract for the specific tasks to be performed." AR Tab 16 at 318. Although the statute offers three other exceptions to the single award prohibition, the D&F only applied this single exception to the JEDI Cloud procurement.

The D&F then set out seven findings. The fourth through seventh findings provided more detail justifying a single award. The findings set out that the successful offeror's discount methodologies will be incorporated into the contract, thus presumably minimizing concern over pricing. The contract line item numbers for cloud offerings "will be priced by catalogs resulting from the full and open competition, thus enabling competitive forces to drive all aspects of [firm fixed] pricing." AR 319. The catalogs will cover the "full potential 10 years." *Id.* The successful offeror's catalog will be incorporated in the contract.

The Under Secretary's discussion acknowledged two pricing-related clauses in Section H of the contract that warranted mentioning: sections H2 and H3. Section H2 New Services, provides:

> 1. Subsequent to award, when new (including improved) IaaS, PaaS, or Cloud Support Package services are made publicly available to the commercial marketplace in the continental United States (CONUS) and those services are not already listed in the JEDI Cloud catalogs . . . the Contractor must immediately (no later than 5 calendar days) notify the JEDI Cloud Contracting Officer for incorporation of the new services into the contract . . . . At its discretion, the Contractor may also seek to incorporate new services into the contract in advance of availability to the commercial marketplace. The JEDI Cloud Contracting Officer must approve incorporation of any new services into the contract.
>
> 2. Any discounts, premiums, or fees . . . shall equally apply to new services, unless specifically negotiated otherwise.
>
> 3. The price incorporated into the JEDI Cloud catalog for new

unclassified services shall not be higher than the price that is publicly-available in the commercial marketplace in CONUS, plus any applicable discounts, premiums or fees . . . .

a. New services that are proposed to be incorporated into the contract in advance of availability to the commercial marketplace may potentially be considered a noncommercial item. The JEDI Cloud Contracting Officer will make a fact specific commerciality determination. If the new service is not a commercial item and no other exception or waiver applies, the JEDI Cloud Contracting Officer may require certified cost and pricing data or other than certified cost and pricing data under FAR Subpart 15.4 to make a fair and reasonable price determination.

i. If there are any new fees associated with a new service that is proposed to be incorporated into the contract in advance of availability to the commercial marketplace, the new proposed fee must be provided to the JEDI Cloud Contracting Officer for review and, if appropriate, approval and incorporation into the contract.

4. The price incorporated into the JEDI Cloud catalog for new classified services may include a price premium as compared to unclassified services because of the additional security requirements. . . .

AR Tab 35 at 740-41 (Final Amended RFP). The net effect of this provision is to permit the addition of wholly new services to the contract over time.

Section H3 provides:

1. Within 45 calendar days of the Contractor lowering prices in its publicly-available commercial catalog in CONUS, the Contractor shall submit a revised catalog for incorporation into Attachment J-1, Price Catalogs as follows:

a. For unclassified services, the revised catalog price shall match the commercially lower price.

b. For classified services, the revised catalog price shall be lowered by to be completed by Offeror percentage of

> the net value difference for the newly lowered rate for the unclassified service. . . .
>
> 2. Any discounts, premiums, or fees in Attachment J-3: Contractor Discounts, Premiums, and Fees shall equally apply to any services with price changes, unless specifically negotiated otherwise.
>
> 3. The Contractor may offer new or additional discounts at any time to be incorporated into Attachment J-3: Contractor Discounts, Premiums, and Fees only upon JEDI Cloud Contracting Officer approval.
>
> 4. When the JEDI Cloud Contracting Officer incorporates the revised price into the Attachment J-1, Price Catalogs and/or Attachment J-3: Contractor Discounts, Premiums, and Fees, as appropriate, the Contractor shall update the listing of services and corresponding prices in the online pricing calculator and APIs for JEDI Cloud within 24 hours.

AR 741. This section would apparently offer some assurance that the prices of new services would be moderated.

The attraction of these clauses was that DoD could take advantage of changes in new cloud services that likely will emerge in the marketplace over the ten year lifetime of the contract. They would also ensure that the awardee could not price the new service "higher than the price that is publicly-available in the commercial marketplace in the continental United States." AR 740. The CO could then choose to approve the addition of these services to the contract. The Under Secretary reasoned that, because the CO had to approve the new service, once the service was added, its unit price would be fixed, and that the contract thus remained one in which all task orders had "established" firm fixed prices within the terms required by the chosen exception.

JEDI Cloud RFP

On July 26, 2018, DoD issued the RFP for the JEDI Cloud. DoD anticipated awarding a single IDIQ contract, incorporating the awardee's fixed unit price information and catalog offerings to serve as the basis for firm-fixed price task orders. The performance period could extend over ten years: a two-year base period, two three-year option periods, and a final two-

year option period.

Section M provides that the agency will evaluate proposals according to the RFP requirements and for best value to the government. The evaluation includes two phases. First, the agency will evaluate the offeror's submission against the seven gate criteria. An offeror which receives an "Unacceptable" rating for any gate criteria "will not be further evaluated." AR 805.

The second phase begins with the agency evaluating the remaining proposals against Factors 2 through 6 (non-price) and Factor 9 (price). After applying those factors, the agency will establish a competitive range. Offerors in the competitive range will be invited to submit materials for evaluation on non-price Factors 7 and 8 and to engage in discussions. The agency will eliminate any offerors that are rated "Marginal" or "Unacceptable" for Technical Capability or are rated "High" risk under Factor 8 Demonstration. Once any discussions conclude, remaining offerors will be permitted to submit a final proposal revision. The agency will evaluate final proposals, eliminate any proposals with a "High" risk rating or that are rated below "Acceptable" on non-price factors, and determine the proposal that offers the best value.

We return now to phase one, application of the seven gate criteria from Factor 1: 1.1 Elastic Usage; 1.2 High Availability and Failover; 1.3 Commerciality; 1.4 Offering Independence; 1.5 Automation; 1.6 Commercial Cloud Offering Marketplace; and 1.7 Data. The protest puts Gate Criteria 1.1, 1.2, and 1.6 at issue.

Under Gate Criteria 1.1, the agency evaluates offers for whether "the addition of DoD unclassified usage will not represent a majority of all unclassified usage." AR 806. To comply with this gate criteria, the offeror must submit a summary report reflecting its capacity in terms of "Network," "Compute," and "Storage" parameters for the period of January to February 2018. AR 791. "JEDI unclassified usage [must be] less than 50% of the [Commercial Cloud Offering] usage as demonstrated by" the three metrics: Network, Compute, and Storage. *Id.* Under Network, for the selected two months, offerors had to assume JEDI Cloud unclassified ingress was 10.6 Petabytes and 6.5 Petabytes for unclassified egress. Under Compute, offerors had to assume the JEDI Cloud unclassified average physical compute cores in use by application servers was 46,000 cores. Under Storage, offerors had to assume JEDI unclassified data storage usage averaged 50 Petabytes online, 75 Petabytes nearline, and 200 Petabytes

offline across the 2 months.

Three days prior to the release of the JEDI Cloud RFP, Timothy Van Name, Deputy Director of the Defense Digital Service, submitted a memorandum to the CO justifying the use of the gate criteria. It states that Gate Criteria 1.1 exists "to ensure that JEDI Cloud: 1) is capable of providing the full scope of services even under surge capacity during a major conflict or natural disaster event; and 2) experiences ongoing innovation and development and capability advancements for the full potential period of performance (10 years)." AR 944.

Mr. Van Name continued, "Not including this criteria will risk future military operations that depend on the overall ability of the Offeror to support surge usage at vital times." *Id.* He explained that, "Limiting JEDI Cloud to 50%, excluding the Offeror's own usage, is essential to ensuring the Offeror's ability to support commercial innovation by requiring a critical mass of non-JEDI customers and usage that will drive further development of the service offerings." AR 945. Mr. Van Name justified the requirement for offerors to present summary reports based on data from January 2018 and February 2018 as necessary in order "to facilitate fair competition, as this prevents potential Offerors from taking measures to change their numbers once they became aware of this [Gate Criteria] requirement at the release of the draft RFP in March 2018." *Id.*

The next challenged Gate Criteria is 1.2. There are four elements within Gate Criteria 1.2, but only the first is relevant to this protest:

> No fewer than three physical existing unclassified [Commercial Cloud Offering] data centers within the Customs Territory of the United States . . . that are all supporting at least one IaaS offering and at least one PaaS offering that are FedRAMP Moderate "Authorized" by the Joint Authorization Board (JAB) or a Federal agency as demonstrated by official FedRAMP documentation.

AR 792.

Concerning Gate Criteria 1.2, Mr. Van Name wrote, "The rationale for including these minimum requirements in the RFP is to validate that JEDI Cloud can provide continuity of services for DoD's users around the world." AR 947. He notes that "[h]igh availability and failover requirements are long standing within the DoD, particularly around the critical infrastructure that

supports warfighters." *Id.* Plaintiff specifically challenges the inclusion of the FedRAMP Moderate "Authorized" requirement, which it was admittedly unable to meet at the time of proposal submission. Mr. Van Name explained at the time that, even though the successful offeror would not have to be FedRAMP Moderate "Authorized" during performance, such authorization "is the Federal cloud computing standard and represents the Department's minimum security requirements for processing or storing DoD's least sensitive information." *Id.* (emphasis added). The authorization process "validates [that] the physical data center security requirements are appropriately met." *Id.* Upon award, the offeror has thirty days to "meet the more stringent security requirements outlined in the JEDI Cyber Security Plan for unclassified requirements, but being able to meet the more stringent requirements are contingent on the underlying physical data center security requirements that are approved during the FedRAMP Moderate review process." *Id.*

The third gate criteria at issue is 1.6. The marketplace will be used "to deploy [Commercial Cloud Offering] and third-party platform and software service offerings onto the [Commercial Cloud Offering] infrastructure." AR 793. It exists "to enable DoD to take advantage of the critical functionality provided by modern cloud computing providers to easily 'spin up' new systems using a combination of IaaS and PaaS offerings as well as offerings provided through the vendor's online marketplace." AR 950-51. The marketplace provides ease of use and rapid adoption. Mr. Van Name concluded that "all [s]ub-factors under Factor 1 Gate Criteria are necessary and reflect the minimum requirements for JEDI Cloud." AR 952.

Post-Solicitation Events

Oracle filed a pre-bid, pre-award protest at the GAO on August 6, 2018, challenging the single award approach. The agency then amended the RFP, and Oracle filed a supplemental protest on August 23, 2018, challenging the three gate criteria discussed above. The agency amended the RFP again on August 31, in relevant part permitting an offeror to demonstrate that it met Gate Criteria 1.2, FedRAMP Moderate "Authorized," through authorization by the Joint Authorization Board or by an agency. Oracle then filed a consolidated protest on September 6, 2018, raising its conflicts of interest argument (the facts of which are discussed in the next section).

Four offerors, including Oracle, submitted proposals on October 12, 2018. GAO subsequently denied Oracle's protest. Oracle filed its protest in this court on December 6, 2018. Oracle did not move for a preliminary

injunction. The agency informed the court that it did not intend to make an award until midsummer 2019.

Meanwhile, the agency continued to perform its evaluation, starting with Factor 1 Gate Criteria. On December 12, 2018, the Technical Evaluation Board ("TEB") found Oracle's proposal "Unacceptable" under Factor 1 Gate Criteria 1.1 and it ended evaluation of Oracle's proposal.

Oracle was found "Unacceptable" under the Network component of Gate Criteria 1.1 because its "proposal does not specify a comparison of the aggregate network usage as required, it only specifies a comparison against installed network capacity in the Summary Report." AR 57848. The board also found Oracle's proposal unacceptable for the Compute component, because Oracle placed its table for JEDI Cloud and Cloud Commercial Offering average physical compute cores in use in its Tab A narrative instead of in its Summary Report. For the Storage component, the board concluded, "The JEDI Cloud RFP requires that 'JEDI unclassified usage must be less than 50% of the [Commercial Cloud Offering] [average storage] in use'. This proposal is found 'Unacceptable' for Subfactor 1.1(2) because the calculated JEDI Cloud daily average storage usage is 50.79%." AR 57849. The proposal also failed to provide detailed storage information in bytes for each of the required categories, instead providing an aggregate for all types of storage. *Id.* Because Oracle did not meet Gate Criteria 1.1, the agency did not consider whether it met the other five criteria.

The TEB also completed the gate criteria evaluations for the other three offerors. The board found AWS and Microsoft "Acceptable" under all gate criteria. It found IBM "Unacceptable" under Gate Criteria 1.2 and ended its evaluation.

On February 19, 2019, the TEB completed its evaluation of the only two remaining offerors, AWS and Microsoft, for non-price Factors 2-6. [

]

In late February 2019, the Source Selection Evaluation Board completed its Executive Summary Reports, confirming that it had reviewed the technical evaluations. The Source Selection Advisory Council then affirmed the TEB's consideration of the gate criteria submissions and completed the Executive Summary Report. The Source Selection Advisory Council Chair concluded: "[I]t is not recommended that the SSA make award

based on the initial proposal, as both [AWS] and [Microsoft] proposals have deficiencies that make them unawardable." AR 58641. After discussion with the Source Selection Authority Council, however, the Chair recommended "that the [Procuring Contracting Officer] make a competitive range determination of two, to include both AWS and Microsoft." *Id.* The CO determined that AWS and Microsoft would be the competitive range. The evaluation process is ongoing.

Conflicts of Interest Relating to the JEDI Cloud Procurement

Oracle alleges that, throughout this procurement, three individuals with conflicts of interest (Deap Ubhi, Tony DeMartino, and Victor Gavin) affected the integrity of the JEDI Cloud acquisition and that AWS has an organizational conflict of interest. On July 23, 2018, the CO completed a memo for the record stating her assessment that the possible conflicts of interest of five individuals, including Mssrs. Ubhi and DeMartino, had "no impact" on the procurement. She applied FAR 3.104-7. Her initial analysis is considered below.

Tony DeMartino

Mr. DeMartino was an AWS consultant prior to joining DoD. In January 2017, he became the Deputy Chief of Staff for the Secretary of Defense. In March, he transitioned to Chief of Staff for the Deputy Secretary.

On April 24, 2017, a Senior Attorney in the Office of General Counsel, Standards of Conduct Office, emailed Mr. DeMartino a "Cautionary Notice." AR 4345. The attorney wrote: "[Y]ou may have a regulatory prohibition under 5 C.F.R. § 2635.502 on participating in matters where one of the entities for whom you served as a consultant during the last year is or represents a party to the matter." *Id.* The attorney reminded Mr. DeMartino that DoD does business with "Amazon" and that he must "be vigilant and consult with our office before participating in any matters involving these entities until the one-year period has expired." *Id.* The email concluded, "If you have potentially conflicting duties, please discuss with your supervisor and coordinate with our office to ensure that any conflicts are properly resolved." *Id.*

As a part of his duties as Chief of Staff, Mr. DeMartino performed work related to the JEDI Cloud procurement. He did not, however, have access to the Google Drive or the Slack channels. He coordinated staffing of the September 13, 2017 Accelerating Enterprise Cloud Adoption

Memorandum. In October 2017, he participated in editing an opinion piece for the Deputy Secretary regarding the procurement just before the release of the RFI. He coordinated meetings for the Deputy Secretary relating to the procurement through early 2018.

Mr. DeMartino's position required him to communicate the Deputy Secretary's questions to members of the Cloud Executive Steering Group and the Defense Digital Service, among others. He also attended meetings where the development of procurement documents was discussed.

Mr. DeMartino worked for the Deputy Secretary through March 2018. He then returned to his position as Deputy Chief of Staff for the Secretary of Defense. Inquiries arose in 2018 regarding his former position as an AWS consultant. Only then did Mr. DeMartino seek advice from the Standards of Conduct Office. The office determined that Mr. DeMartino had not participated in the JEDI Cloud procurement in a manner covered by regulations. The office verbally advised Mr. DeMartino, however, that given the high visibility of the procurement, he should consider recusing himself from anything to do with the acquisition. The office also notified those working on the JEDI Cloud procurement of that warning.

On April 2, 2018, Mr. DeMartino communicated with Defense Digital Service Director Lynch regarding a JEDI Cloud Update document, providing comments and questions on that document. Between April 4 and June 5, he emailed with members of the Defense Digital Service about an unrelated matter, received a final briefing paper for the Secretary of Defense, and was copied on an email from Ms. Woods regarding the second draft RFP. Mr. DeMartino resigned from federal employment in July 2018. The record does not reflect Mr. DeMartino negotiating for or returning to any form of AWS employment after his resignation.

The CO considered whether Mr. DeMartino was impartial in performing his official duties. She found that he did not have "input or involvement in the reviewing or drafting of the draft solicitation package, the Acquisition Strategy, Business Case Analysis, or other pre-decisional sensitive documents relative to the JEDI Cloud acquisition." AR 685. She also found that he "worked with [Standards of Conduct Office] throughout his DoD employment to ensure compliance with all applicable ethical rules." *Id.* The CO concluded that his "involvement was ministerial and perfunctory in nature" and he "did not participate personally and substantially in the procurement. Therefore, Mr. DeMartino's involvement did not negatively impact the integrity of the JEDI Cloud acquisition." *Id.* In her testimony

during the GAO hearing in Oracle's bid protest, the CO repeated this conclusion. The CO did not revisit her conclusion on Mr. DeMartino's actions in her 2019 assessment.

Deap Ubhi

The CO also evaluated Mr. Ubhi's impact on the JEDI Cloud procurement. She listed five findings. First, "Mr. Ubhi was previously employed with AWS, which ended in January 2016." AR 686. Second, "Mr. Ubhi was employed with Defense Digital Service from August 22, 2016 to November 27, 2017." *Id.* Third, "Mr. Ubhi was involved with JEDI Cloud market research activities between September 13, 2017 and October 31, 2017." *Id.* Fourth, "[b]ecause greater than one year had lapsed between when his AWS employment ended and when his participation in JEDI Cloud started, no restrictions attached to prohibit Mr. Ubhi from participating in the procurement." *Id.* Her fifth finding was:

> In late October 2017, AWS expressed an interest in purchasing a start-up owned by Mr. Ubhi. On October 31[,] 2017, Mr. Ubhi recused himself from any participation in JEDI Cloud. His access to any JEDI Cloud materials was immediately revoked, and he was no longer included in any JEDI Cloud related meetings or discussions.

Id.

The CO detailed what the agency knew at the time. Mr. Ubhi had access to the Google Drive and Slack channels. He attended meetings within DoD and with industry, acting as a point of contact for industry representatives. He participated in drafting and editing some of the first documents shaping the procurement. He argued that DoD should adopt a single award approach. In short, Mr. Ubhi was involved in developing the JEDI Cloud procurement until he left DoD on November 24, 2017.

On October 31, 2017, Mr. Ubhi emailed Mr. Lynch and Mr. Van Name, copying counsel for the Standards of Conduct Office and Ms. Woods. Mr. Ubhi wrote:

> As per guidance from [Standards of Conduct Office] (Eric Rishel) and our in-house general counsel Sharon Woods, I am hereby recusing myself from the [Defense Digital Service's] further involvement in facilitating SecDef and

> [Defense Digital Service's] initiative to accelerate adoption of the cloud for the DoD enterprise, due to potential conflicts that may arise in connection to my personal involvement and investments. Particularly, Tablehero, a company I founded, may soon engage in further partnership discussions with Amazon, Inc., which also owns and operates one of the world's largest cloud service providers, Amazon Web Services, fulfilling that responsibility to my fullest. This project is critical to the national security of our country, and I regret that I can no longer participate and contribute.

AR Tab 45 at 2777. Although the agency was not aware at the time, Mr. Ubhi's reason for leaving DoD was fabricated. On November 13, 2017, Mr. Ubhi resigned.

Although the agency listed Mr. Ubhi on its list of individuals submitted to GAO who were personally and substantially involved in the JEDI Cloud procurement, the CO nevertheless concluded that Mr. Ubhi's participation did not negatively affect the integrity of the procurement, because (1) his impartiality restriction had expired prior to working on the JEDI Cloud procurement; (2) his participation was limited; and (3) Mr. Ubhi "promptly recused himself." AR 687.

Oracle challenged the CO's conclusions before GAO and before this court. Oracle also raised a question as to whether AWS had an organizational conflict of interest and whether the actions of another individual, Anthony DeMartino, tainted the integrity of the JEDI Cloud procurement. During the early stages of this protest, the agency represented that it was evaluating whether AWS had an organizational conflict of interest.

Shortly after Oracle filed its original motion for judgment on the administrative record, the agency filed a motion to stay this case, prompted by an unsolicited letter it had received from AWS pointing out that some of the information provided by Mr. Ubhi to the agency was false. The agency therefore decided to reevaluate the impact of Mr. Ubhi's actions in light of the new information. The agency also planned to complete its organizational conflict of interest evaluation of AWS. The court granted the motion to stay. On April 15, 2019, the government filed a status report updating the court that the agency had completed those evaluations.

When she reassessed the facts, the CO determined that, even with the new information, Mr. Ubhi's conflict of interest had not tainted the JEDI

Cloud procurement. The reassessment began with Mr. Ubhi's involvement. Mr. Ubhi was selected by Mr. Lynch to serve as "a product manager with a business focus" on the Defense Digital Service JEDI Cloud team. AR 58699. Mr. Ubhi was involved in acquisition planning. He had administrative privileges on the Google Drive and participated in vendor meetings, although it was DoD's practice to have two representatives present at those meetings.

The information supplied by AWS related to Mr. Ubhi's relationship with AWS during his Defense Digital Service employment. AWS maintained throughout its communication with the CO that it hired Mr. Ubhi without knowing that he had lied to DoD about his reason for resigning and lied to AWS about complying with DoD ethics rules. Mr. Ubhi in fact hid relevant information and misdirected both DoD and AWS. The CO recited: "'AWS did not offer to purchase Tablehero . . . at any time, while he was engaged in market research activity or otherwise. . . . Those discussions concluded (with no deal and no future business relationship) in December 2016, long before the JEDI Cloud procurement began.'" AR 58701-02. Mr. Ubhi's discussions with AWS regarding Tablehero thus ended after he started at Defense Digital Service but before he began working on the procurement.

AWS further informed DoD that Mr. Ubhi had communicated with AWS as early as April 26, 2017, to discuss future AWS employment.[8] Prior to beginning work on the procurement, Mr. Ubhi had applied for, been offered, and declined a job at AWS. Mr. Ubhi indicated in August 21 and 23, 2017 emails that he would be interested in future employment at AWS.

At nearly the same time he began work on the JEDI Cloud procurement, Mr. Ubhi had discussions "with his former Supervisor at AWS regarding the possibility of rejoining AWS in a commercial startup role unrelated to AWS's government business." AR 58702. On October 4, 2017, Mr. Ubhi made a "[v]erbal commitment to rejoin AWS." AR 58703.

Throughout October, Mr. Ubhi "[m]et with companies as part of market research" related to the JEDI Cloud project. AR 58703. In that same period, on October 17, 2017, he applied for "an open position in AWS's commercial organization." AR 58702. On October 19, 2017, Mr. Ubhi completed an AWS Government Entity Questions form on which he "specifically represented to AWS that he 'confirmed by consulting with [his]

[8] After AWS's February 12, 2019 letter, the CO and AWS communicated through March 2019.

employer's ethics officer' that he was permitted to have employment discussions with AWS." AR 58702 (alteration original). On that form he also represented that he did not have "any employment restrictions [preventing him] 'from handling any specific types of matters if employed by Amazon or its subsidiaries.'" AR 58705. Both representations were false.

AWS made Mr. Ubhi an offer on October 25, 2017, which Mr. Ubhi accepted two days later. Mr. Ubhi sent the email recusing himself to Mr. Lynch on October 31, 2017, which falsely represented his reason for leaving DoD. He resigned on November 13, 2017. He worked at Defense Digital Service until November 24, 2017. He rejoined AWS as "Senior Manager, Startup Programs Management in AWS Business Development" on November 27, 2017. [9] *Id.*

When considering Mr. Ubhi's impact on the procurement, the CO placed his actions in the context of the RFP-drafting process, which included multiple stages and involved various DoD offices. She noted, "[M]ore than 70 individuals participated personally and substantially in the JEDI Cloud acquisition prior to the receipt of proposals." AR 58700. Under Secretary Lord considered many documents that "had extensive reviews," including technical and legal review. AR 58699. The draft RFP went through a Defense Procurement and Acquisition Policy peer review in April 2018. The DoD Chief Information Officer also performed "a full top-down, bottom-up independent review of JEDI Cloud pre-solicitation acquisition documents, including the RFP." *Id.* He consulted security, technical, and acquisition experts. Additionally, industry offered comment on the RFI and draft RFPs.

The CO held eight interviews and reviewed numerous documents in an effort to determine whether anyone knew that the information in the 2018 determination was inaccurate, whether anyone would adjust their opinion about Mr. Ubhi's influence based on the new information, and whether there was any other undisclosed information. The CO spoke with Mr. Lynch, Mr.

[9] Beyond the 2019 investigation materials, the CO also refers to AWS's Organizational Conflict of Interest Mitigation Plan, submitted with its proposal, which included an affidavit from Mr. Ubhi. In it he stated that he was only involved in the planning stages of the JEDI Cloud procurement and that he did not provide input regarding any draft of the RFP. She relied on her personal knowledge of the procurement development to corroborate Mr. Ubhi's statements. Mr. Ubhi stated that he had complied with AWS's information firewall and had not and would not share nonpublic information or documentation with AWS.

Van Name, Ms. Woods, Mr. Kasper, Mr. Daniel Griffith, two other Defense Digital Service representatives, and an attorney with the Standards of Conduct Office. The CO also spoke with Ms. Christina Austin, who is Associate General Counsel at the Washington Headquarters Service & Pentagon Force Protection Agency within DoD.

The CO reviewed documents that she believed "were apropos to the timeframe when Mr. Ubhi was actively involved with JEDI Cloud related details." AR 58707. She reviewed the draft problem statement, the notes and questions from vendor meetings that Mr. Ubhi attended, the RFI, and Slack conversations. She also considered AWS's employment offer to Ubhi to determine if it reflected payment in exchange for information.

The CO reached six conclusions. First, Mr. Ubhi violated the FAR 3.101-1 requirement that officials "avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-contractor relationships" and the matter therefore had to be referred to the DoD Inspector General. AR 58707-09. The CO reported that interviewees were surprised by Mr. Ubhi's lie that AWS had or would be acquiring Tablehero. He apparently did not mention any other communications with AWS. The CO found that Mr. Ubhi had been aware of his ethical obligations and had ignored them. She found that he should have ceased work on the procurement after he began employment discussions with AWS. She was "disconcert[ed]" that Mr. Ubhi's actions called into question the integrity of the procurement. In this section, the CO also found that the facts "warrant further investigation concerning whether Mr. Ubhi violated 18 U.S.C. § 208, 5 CFR § 2635.604, and 5 CFR § 2635.402." AR 58709. She referred the issue for assessment to the Inspector General and concluded, "Whether Mr. Ubhi's conduct violated these particular laws does not affect my determinations below that his unethical behavior has no impact on the [] pending award or selection of a contractor in the JEDI procurement." *Id.*

Second, she found that there was no violation of FAR 3.104-3(a) by Mr. Ubhi and no violation of FAR 3.104-3(b) by AWS. FAR 3.104-3(a) prohibits officials with access to contractor, proposal, or source selection information from "knowingly disclos[ing] contractor bid or proposal information or source selection information before the award of a Federal agency procurement to which the information relates." FAR 3.104-3(b) prohibits "knowingly obtain[ing] contractor bid or proposal information or source selection information before the award of a Federal agency procurement contract to which the information relates."

The CO broadly investigated "whether there was any evidence of quid pro quo between AWS and Mr. Ubhi." AR 58709. The CO examined the emails between Mr. Ubhi and his former supervisor and that supervisor's affidavit. She found that it was apparent that "Mr. Ubhi wanted to return to AWS dating back to at least February 2017," and AWS wanted him to return as of April 2017. AR 58710. She concluded that "the AWS hiring efforts, which started long before the JEDI Cloud, were not related to JEDI Cloud even though the hiring occurred after the JEDI Cloud initiative started." AR 58711.

The CO compared his employment offer to "a review of Glassdoor and discussion with others about typical AWS employment offers." *Id.* She found that his [ ] employment package was "relatively standard," even if the bonus was slightly higher due to his "personal relationship with" his former supervisor. *Id.* Because the offer did not appear connected to the JEDI Cloud procurement or the sharing of nonpublic information, the CO found that neither Mr. Ubhi nor AWS entered into the discussions or job offer for the exchange of non-public information.

Regarding FAR 3.104-3(a)-(b), the CO noted that Mr. Ubhi stated that he had not shared any non-public JEDI Cloud information and that, in any event, he did not have access to RFI responses, RFP drafts, or other acquisition sensitive documents. The CO also evaluated AWS's statements. Based on the company's Organizational Conflict of Interest Response and its emails with the CO, she concluded that it had not received non-public JEDI Cloud information. The Senior Manager of United States Federal Business Development and JEDI Proposal Manager provided an affidavit stating that Mr. Ubhi had not provided any information to him, or anyone else, on the AWS JEDI team that would have affected AWS's proposal. AWS's DoD Programs Director represented that no one from the AWS Commercial Startup team had anything to do with AWS's JEDI proposal. AWS's DoD Programs Director also represented that Mr. Ubhi was "organizationally and geographically" prevented from providing nonpublic information to her team. *Id.* She had "confidence that Mr. Ubhi had absolutely no involvement whatsoever in the AWS JEDI capture effort and that he has been truly firewalled." *Id.* The Director of Startups at Amazon Web Services World Wide Commercial Sector Business Development stated that Mr. Ubhi "has never revealed or attempted to reveal nonpublic information to me about the JEDI Cloud procurement or any of the offerors involved." *Id.* The CO noted that Mr. Ubhi has not been assigned to any tasks or teams interacting with the AWS JEDI proposal team. *Id.* Based on this review, she found that neither Mr. Ubhi nor AWS violated FAR 3.104-3(a)-(b).

Third, she concluded that even if there had been a violation of FAR 3.104-3(a) and (b), Mr. Ubhi could not have provided competitively useful information. Regarding the vendor meetings, she found that the information would not have been useful to AWS and, in any event, her research indicated that the information regarding a competitor such as Microsoft was publicly available. Nor was the CO convinced that any DoD meetings in which Mr. Ubhi participated were competitively useful, because they occurred prior to the decisional documents and addressed individual needs rather than the actual procurement strategy. Furthermore, she concluded that much of his information relating to costs or needs would be outdated.

Fourth, there was no violation of FAR 3.104-3(c). FAR 3.104-3(c) requires officials such as Mr. Ubhi to promptly report contacting or being contacted "by a person who is an offeror in that Federal agency procurement regarding possible non-Federal employment for that official" and then to disqualify himself from further personal and substantial participation in the procurement. The CO found that although Mr. Ubhi failed to promptly report the contact with AWS in writing to his supervisor and the agency ethics official and failed to timely recuse himself from JEDI Cloud activities, because the offers were not submitted until October 12, 2018, AWS technically was not an "offeror" until then and therefore Mr. Ubhi did not violate the regulation. *Id.* She nevertheless found "Mr. Ubhi's actions to be unethical and improper." *Id.*

Fifth, Mr. Ubhi's participation in the preliminary stages of the JEDI Cloud procurement did not introduce bias in favor of AWS. Mr. Ubhi was involved in JEDI Cloud for seven weeks during the preliminary stages of planning and no "critical decisions" were made during this period. AR 58716. The CO apparently asked "[a]ll individuals directly involved in the JEDI Cloud effort" whether the revelations in the AWS letter changed their opinion on Mr. Ubhi's effect on the procurement. They uniformly said no.

She reviewed Slack messages to determine whether Mr. Ubhi expressed bias toward any potential offeror. She determined that he did not, because, although Mr. Ubhi had strong, sometimes coarsely-expressed opinions, he did not show bias in favor of AWS in particular.[10] Instead, he

[10] The court reviewed hundreds of pages of Slack messages—generally an unedifying exercise, except as a cautionary tale about ill-considered use of instant messaging. One would have thought that in this litigious culture, people would be less promiscuous about sharing every stray mental hiccup.

believed that there were very few companies who could offer the services that DoD would need to adopt an enterprise cloud solution; those companies apparently included both Microsoft and AWS. The CO also reviewed Mr. Ubhi's emails and found similar sentiments. The CO pointed out that, if anything, the Slack channels demonstrate that no one person could have swayed the planning decisions because so many people contributed.

Sixth, even if Mr. Ubhi had attempted to introduce bias in favor of AWS, he did not impact the procurement, for three reasons. First, Mr. Ubhi lacked the technical expertise to substantively influence the JEDI Cloud procurement. Second, his actual attempts to influence the procurement were limited. "Third, and most importantly, all the key decisions for the JEDI Cloud procurement, such as the actual RFP terms and whether to award one or multiple contracts, were made well after Mr. Ubhi recused himself, after being vetted by numerous DoD personnel to ensure that the JEDI Cloud RFP truly reflects DoD's requirement." AR 56719-23. The CO reiterated that Mr. Ubhi was a product manager focused on market research, not an engineer. In her interview with Mr. Lynch, Mr. Lynch explained that Mr. Ubhi was one member of a large group of people including "engineers, business owners, and entrepreneurs" who favored a single provider strategy absent Mr. Ubhi's influence. AR 58720. The other interviewees expressed the view that Mr. Ubhi was effective at his job, but he did not have the ability to bias vendor meetings, RFI questions, or the single award decision.

The CO then turned to Mr. Ubhi's contributions to procurement documents. Regarding the problem statement, the CO found that Mr. Ubhi contributed 100 changes to the document, along with other collaborators. She concluded that his contributions were outdated, because the Defense Digital Service Product Manager who was tasked with drafting the Business Case Analysis after Mr. Ubhi left found the Problem Statement tone helpful, but the content too limited to form the basis of the Business Case Analysis. The CO determined that Mr. Ubhi's RFI edits were minor, relating to how responders discussed Tactical Edge abilities. Technical interviewees expressed the view that Mr. Ubhi lacked the technical expertise to contribute substantively to those documents.

Procurement documents created or received after Mr. Ubhi's departure included the RFI responses, Market Research Report, Joint Requirements Oversight Council Memorandum, Single Award D&F, the

---

Mr. Ubhi, in particular, contributed any number of banal, puerile, profane and culinary messages.

CO's justification for a single award, Business Case Analysis, Acquisition Strategy, RFP and draft RFPs, and justification for the gate criteria. She iterated that multiple DoD teams developed the documents. She concluded that, even if Mr. Ubhi had exhibited bias in favor of AWS, he had not impacted the procurement. In summary, "[e]ven though I find that Mr. Ubhi violated FAR 3.101-1 and may have violated 18 U.S.C. § 208 and its implementing regulations, I determine that there is no impact on the pending award or selection of a contractor in accordance with FAR 3.104-7." AR 58720.

Victor Gavin

The CO also investigated the potential impact of Victor Gavin on the integrity of this procurement and completed that investigation during the stay in the protest. During the procurement, Mr. Gavin was a Deputy Assistant Secretary of the Navy for C41 and Space Programs. In the summer of 2017, Mr. Gavin discussed with Navy ethics counsel future employment with defense contractors. He then discussed retirement plans with an AWS recruiter and with AWS Director of DoD programs from August 2017 to January 2018.

Mr. Gavin attended the October 5, 2017 meeting of the Cloud Executive Steering Group to share the Navy's experience with cloud services. He submitted a Request for Disqualification from Duties on January 11, 2018, requesting he be excluded from matters affecting the financial interests of AWS. He interviewed with AWS on January 15, 2018. On March 29, 2018, AWS offered Mr. Gavin a position and he accepted.

Mr. Gavin then attended a JEDI Cloud meeting on April 5, 2018, where, among other things, the attendees discussed the draft Acquisition Strategy. The CO attended the meeting as well. She recalled that Mr. Gavin did not show bias toward a particular vendor and advocated for a multiple-award approach. He did not edit the Acquisition Strategy.

Mr. Gavin retired from the Navy on June 1, 2018. He began work at AWS on June 18 as Principal, Federal Technology and Business Development. After he began work at AWS, but before AWS implemented an information firewall, he "had a few informal conversations with AWS's Director, DoD, Jennifer Chronis, in which JEDI came up." AR 24550. He "provided only general input on DoD acquisition practices and Navy cloud usage based on [his] years of experience as an information technology acquisition professional at the Navy." AR 24550-51. He represented to DoD

that he did not provide any JEDI Cloud procurement information to AWS's Director of DoD Programs.

AWS first informed Mr. Gavin of an information firewall on July 26, 2018. In separate emails on July 31, AWS informed Mr. Gavin that he is "strictly prohibited from disclosing any non-public information about DoD's JEDI procurement (were he to have any) to any AWS employee" and informed the AWS JEDI team of the firewall. AR 24544-45. Mr. Gavin said that he would comply with the firewall.

The CO determined that, although Mr. Gavin's attendance at the October 5, 2017 meeting did not constitute personal and substantial participation in the JEDI Cloud procurement, his attendance at the April 5, 2018 meeting may have constituted such participation. The CO did not consider his participation of any significance, however, but referred the issue to ethics counsel for further review.

The CO decided that Mr. Gavin violated FAR 3.101-1, and possibly 18 U.S.C. § 208 (2012), but that his involvement did not taint the procurement. The CO specifically found that he had limited access to the draft Acquisition Strategy and did not furnish any input on the document; he did not disclose any competitively useful nonpublic information; he did not obtain or disclose other bid information to AWS; and he did not introduce bias into the meetings he attended. Regarding AWS, she concluded that it had not received any competitively useful information or an unfair advantage through Mr. Gavin.

Organizational Conflict of Interest

Finally, the CO determined that AWS did not receive an unfair competitive advantage in the JEDI Cloud procurement and that no organizational conflict of interest exists. She relied on FAR 9.505 as she considered whether a significant potential conflict exists, particularly whether AWS has received an unfair competitive advantage. She considered whether AWS possesses "[p]roprietary information that was obtained from a Government official without proper authorization; or [s]ource selection information (as defined in 2.101) that is relevant to the contract but is not available to all competitors, and such information would assist that contractor in obtaining the contract." FAR 9.505(b).

When submitting a proposal, the offeror was required to disclose any actual or perceived conflicts of interest and identify measures to avoid or

mitigate those conflicts. The CO reviewed the AWS Organizational Conflicts of Interest Response and supplemental materials. She considered whether Mr. Ubhi, Mr. Gavin, and two other individuals, Brandon Bouier and Cynthia Sutherland, could provide information to AWS that would give it an unfair competitive advantage.

The CO began with AWS's plan as it relates to Mr. Ubhi. Due to Mr. Ubhi's misrepresentations, she understandably "did not give much weight or credibility to the statements Mr. Ubhi provided in his declarations." AR 58750. Instead, she relied on AWS's Organizational Conflicts of Interest Response, which offered three assurances: (1) Mr. Ubhi has not supported the AWS sector handling its JEDI Cloud proposal and has not been involved in any JEDI Cloud proposal activities. (2) He has not had "any substantive communications" with any AWS employee regarding the JEDI Cloud procurement and has not disclosed nonpublic information. *Id.* (3) AWS implemented an information firewall on May 11, 2018, sending the notice to both Mr. Ubhi and the AWS JEDI Cloud team. It prohibited any contact, disclosure, or discussion of information between Mr. Ubhi and AWS's JEDI Cloud team.

AWS's letter provided more information regarding the information firewall. The letter represents that, upon arrival, Mr. Ubhi "'informally firewalled himself by duly notifying his manager that he should not be involved in JEDI Cloud activities because of potential conflict issues.'" AR 58751. The formal information firewall has functional, organizational, and geographic components. The AWS Senior Lead Recruiter, the Director of Startups of AWS Commercial Sector Business Development, the AWS JEDI Proposal Team Lead, and the Director of DoD Programs at AWS each provided an affidavit regarding whether Mr. Ubhi shared nonpublic information. The materials consistently described Mr. Ubhi's exclusion from working with AWS's JEDI Cloud proposal team.

The AWS Senior Lead Recruiter stated that Mr. Ubhi represented during the hiring process, falsely as it turned out, that he had spoken with DoD ethics officials and was engaging in employment discussions with AWS. The recruiter also stated that Mr. Ubhi did not provide detail regarding his work at Defense Digital Service; this was consistent with Mr. Ubhi's application materials. The Director of Startups of AWS Commercial Sector Business Development—Mr. Ubhi's manager—stated that no one on his team, including Mr. Ubhi, worked with the AWS JEDI Cloud proposal team. Although the CO could not determine exactly when Mr. Ubhi's manager became aware of Mr. Ubhi's conflict, she explained that the exact date did

not matter since the manager was aware of the conflict and his sector did not overlap with the AWS JEDI Cloud proposal team. Both the AWS JEDI Proposal Team Lead and the Director of DoD Programs at AWS stated that Mr. Ubhi had not communicated information to them and that they would not seek any in the future.

Based on the mitigation plan and AWS's representations, the CO determined that "Mr. Ubhi's employment with AWS Commercial Sector Business Development does not create an [organizational conflict of interest]." AR 58752. The CO also found that "AWS did not receive any nonpublic information or documentation JEDI Cloud-related, including potential competitors, from Mr. Ubhi." AR 58753. She iterated that, even if Mr. Ubhi had shared the early planning information, that information would not have been competitively useful.

The CO next turned to AWS's Organizational Conflicts of Interest Plan as it related to Mr. Gavin. The plan stated that Mr. Gavin was not involved in the AWS JEDI Cloud proposal preparation; had not seen AWS proposal materials; had not provided input on the AWS proposal; and had not disclosed nonpublic information to anyone at AWS. AWS emailed notices to Mr. Gavin and the AWS JEDI Cloud proposal team on July 31, 2018, establishing an information firewall. Mr. Gavin provided an affidavit stating that he participated in only one JEDI Cloud procurement meeting while he was with the Navy (which was an inaccurate statement because he attended a second meeting); he had no access to competitively useful information; and he has not shared JEDI Cloud procurement information. The CO concluded that Mr. Gavin's employment at AWS did not create a potential organizational conflict of interest and that Mr. Gavin had not provided competitively useful information to AWS because he did not have any to provide.

Reaching beyond the AWS Organizational Conflicts of Interest Plan, the CO requested information relating to Brandon Bouier, who was employed at Defense Digital Service in 2017. He resigned from Defense Digital Service on August 18, 2017 and concluded his employment there on September 1, 2017. He began work at AWS on September 25, 2017. AWS submitted an affidavit from him. The CO noted that Mr. Bouier departed Defense Digital Service prior to the Deputy Secretary's September 14, 2017, Accelerating Enterprise Cloud Adoption Memorandum. The CO, and others at Defense Digital Service, did not recall him working on the JEDI Cloud procurement. She thus found that he did not have nonpublic information

related to the procurement and that his employment at AWS did not create an organizational conflict of interest.

The CO considered one last person: Cynthia Sutherland. Dr. Sutherland worked for the Cybersecurity and Defenses Branch, Cyberspace Division, Joint Chiefs of Staff. Dr. Sutherland reached out to the CO on February 26, 2019. She was the cloud expert for the Joint Staff Chief Information Officer. Dr. Sutherland was personally and substantially involved in the JEDI Cloud procurement, "principally" in November and December 2017. AR 58755. She contributed work to the Joint Requirements Oversight Council Memorandum. She addressed cloud concerns from council members and adjusted the memo based on the council's feedback. Dr. Sutherland attended the Cloud Cybersecurity Working Group's initial conversations, recommended how to shape cybersecurity requirements, and provided a data dictionary to that group. She "led the development of the cloud characteristics/requirements for the JEDI Cloud based on the needs of the Combatant Commands, warfighter." *Id.* After the Joint Requirements Oversight Council Memorandum was signed, she provided bi-weekly updates to the Vice Chief of the Joint Chiefs of Staff regarding the JEDI Cloud procurement and other cloud efforts through April 2018. At that point she only relayed information without providing input on decisions.

Dr. Sutherland applied to be an AWS Public Sector Specialist on January 9, 2019, approximately a year after her work on the JEDI Cloud procurement. Between her application date and February 26, 2019, she completed four interviews with AWS. During those interviews, she discussed "'her level of understanding and creation of cloud requirements for her current customers, the warfighter.'" *Id.* She had a final interview on February 27, 2019. Dr. Sutherland represented that she did not discuss the JEDI Cloud procurement in any of her conversations with AWS, instead sticking to her understanding of cloud computing generally and her work developing cybersecurity requirements for "global customers." AR 58756.

AWS offered Dr. Sutherland the position of Industry Specialist on AWS's Security Assurance team on March 11, 2019. She accepted on the same day. When she was communicating with the CO, she had not started working at AWS. The AWS JEDI Proposal Team Lead and the Director of DoD Programs at AWS stated that they were unaware that AWS had interviewed Dr. Sutherland. AWS represented that Dr. Sutherland had not contributed to the AWS JEDI Cloud proposal submitted in October 2018.

The CO found that, other than the drafts of the Joint Requirements Oversight Council Memorandum and the initial conversations of the Cloud Cybersecurity Working Group, Dr. Sutherland did not have access to nonpublic information related to the JEDI Cloud procurement. The CO concluded that Dr. Sutherland had not provided nonpublic information to AWS, that Dr. Sutherland's prospective employment did not create an organizational conflict of interest, and that AWS's plan to institute an informational firewall when Dr. Sutherland began work was reasonable.

In conclusion, the CO decided that AWS had proposed a reasonable risk mitigation plan, did not have an organizational conflict of interest, and had not received nonpublic information. In its amended complaint and supplemental motion for judgment on the administrative record, Oracle challenges the 2019 conflicts of interest determinations.

After we lifted the stay in this protest, the parties briefed cross motions for judgment on the administrative record. We held oral argument on July 10, 2019. On July 12, 2019, we issued an order denying plaintiff's motion and granting defendant's and intervenor's motions because Oracle has not shown prejudice as a result of the errors discussed below.

DISCUSSION

This court has jurisdiction over actions "objecting to a solicitation by a Federal agency for bids or proposals for a proposed contract . . . or any alleged violation of statute or regulation in connection with a procurement or a proposed procurement." 28 U.S.C. § 1491(b)(1) (2012). We review such actions for whether the agency decision was "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A) (2012); 28 U.S.C. § 1491(b)(4). In other words, the court's "task is to determine whether the procurement official's decision lacked a rational basis or the procurement procedure involved a violation of a regulation or procedure." *Tinton Falls Lodging Realty, LLC v. United States*, 800 F.3d 1353, 1358 (Fed. Cir. 2015) (citation omitted).

If we conclude that DoD's conduct fails under this standard of review, we then "proceed[] to determine, as a factual matter, if the bid protester was prejudiced by that conduct." *Bannum, Inc. v. United States*, 404 F.3d 1346, 1351 (Fed. Cir. 2005). To show that it was prejudiced by an error, the protestor must demonstrate "that there was a 'substantial chance' it would have received the contract award but for the [agency's] errors." *Id.* at 1353. The "substantial chance" standard has been applied in pre-award bid protests

in which offerors have submitted their proposals, the protestor has been evaluated and excluded from competition, and the agency has established the competitive range. *E.g.*, *Orion Tech., Inc. v. United States*, 704 F.3d 1344, 1348-49 (Fed. Cir. 2013); *Ultra Elecs. Ocean Sys., Inc. v. United States*, 139 Fed. Cl. 517, 526 (2018).

Plaintiff argues that, in a pre-award bid protest, the court applies the "non-trivial competitive injury" standard articulated in *Weeks Marine, Inc. v. United States*, 575 F.3d 1352, 1358 (Fed. Cir. 2009). But the court in *Weeks Marine* applied the "non-trivial competitive injury test" where the potential offeror had not submitted a bid, "because at that stage it is difficult, if not impossible, to establish a substantial chance of winning the contract prior to the submission of any bids." *Orion*, 704 F.3d at 1348. Here, on the other hand, we cannot ignore the fact that it is now possible to determine whether Oracle had a substantial chance of winning this award. We have the necessary factual predicate, because Oracle's proposal was evaluated and excluded from competition based on its failure to meet Gate Criteria 1.1 and Oracle concedes that it also could not meet Gate Criteria 1.2. Thus, while Oracle meets the most basic element of standing—it submitted a serious proposal—we have to consider whether it was prejudiced, even if some of its substantive arguments are valid.

For this reason, defendant contends that it is pointless to consider most of plaintiff's arguments. Plaintiff responds, however, that its inability to meet the gate criteria is not dispositive if the gate criteria are unenforceable, either because they violate the law or because they would have been drafted differently if the agency had not employed a single award strategy. That question, in turn, depends in part, on whether the single award determination was tainted by the participation of, among others, Mr. Ubhi. In short, the merits of Oracle's arguments are wrapped around the axle with the prejudice question. We believe the tidiest approach, therefore, is to deal with the merits of Oracle's arguments, and if any survive, determine if they are nevertheless off limits because Oracle cannot demonstrate that it was prejudiced. We begin with Oracle's initial contention that the single award determinations of the Under Secretary and the CO were flawed. We conclude that one was, and one wasn't.

I. The Contracting Officer Reasonably Justified Her Determination Under 10 U.S.C. § 2304a(d)(4) And FAR 16.504(c) To Use A Single Award Approach.

As discussed in the background, two single award determinations

were made, by different officials under different standards. This is because, as currently codified, 10 U.S.C. § 2304a (2012) is a mixture of different legislative efforts at promoting competition in IDIQ contracts. Separate legislative and regulatory efforts have been layered on top of one another over time, resulting in the two distinct single award determinations in the JEDI Cloud acquisition.

First, Congress directed that regulations be developed to implement a multiple award preference that would "establish a preference for awarding, to the maximum extent practicable, multiple task or delivery order contracts for the same or similar services or property." 10 U.S.C. § 2304a(d)(4). The implementing regulation is FAR 16.504(c)(1)(i) (2018), which states the multiple award preference and sets out the circumstances in which a single award is appropriate for an IDIQ contract of any value. The CO made her singe award determination under this regulation.

Section 2304a(d)(3), discussed in the next section, followed after the codification of the multiple award preference. In that section, Congress prohibited single awards in task or delivery order contracts valued at more than $112 million in the absence of a written finding from the head of the agency that one of four conditions exist. For aught that appears, these requirements operate independently—different officials make the determination considering different factors—although they involve very similar subject matter. The underlying goal is certainly the same: to protect competition.

With respect to the CO's decision under FAR 16.504(c)(1)(i), when the agency is considering using an indefinite-quantity contract, "the CO must, to the maximum extent practicable, give preference to making multiple awards of indefinite-quantity contracts under a single solicitation for the same or similar . . . services to two or more sources." But FAR 16.504(c)(1)(ii)(B) adds that "[t]he contracting officer must not use the multiple award approach if—

> (1) Only one contractor is capable of providing performance at the level of quality required because the supplies or services are unique or highly specialized;
>
> (2) Based on the contracting officer's knowledge of the market, more favorable terms and conditions, including pricing, will be provided if a single award is made;

> (3) The expected cost of administration of multiple contracts outweighs the expected benefits of making multiple awards;
>
> (4) The projected orders are so integrally related that only a single contractor can reasonably perform the work;
>
> (5) The total estimated value of the contract is less than the simplified acquisition threshold; or
>
> (6) Multiple awards would not be in the best interests of the Government.

Here, the CO found that multiple awards must not be used for three reasons: "(2) Based on the CO's knowledge of the market, more favorable terms and conditions, including pricing, will be provided if a single award is made;" "(3) The expected cost of administration of multiple contracts outweighs the expected benefits of making multiple awards;" and "(6) Multiple awards would not be in the best interests of the Government." AR 455.

The regulation is unambiguous: even in light of the multiple award preference, "[t]he contracting officer must not use a multiple award approach if" one of six listed conditions exist. FAR 16.504(c)(1)(ii)(B) (emphasis added). The question is whether the CO rationally determined that any of the three chosen conditions exist. We believe she did.

Oracle argues that the CO's memorandum did not properly balance the multiple award preference against a single award approach. It contends that the CO "did not meaningfully consider the benefits of competition, arbitrarily inflated the cost of competition, and violated Congressional policy." Pl.'s Suppl. Mot. at 26. Oracle challenges the CO's assessment of whether more favorable terms and conditions are available if a single award is made, but "the CO's knowledge of the market" is the standard set out in the regulation. She explained her understanding of cost and vendor investment in a multiple award and single award context and drew the reasonable conclusion that a single award was more likely to result in favorable terms, including price. The CO also considered the fact that even if price might not be more favorable in a single award, two other conditions also exist that mandate a single award.

She asserted that multiple awards are costlier to administer and that multiple awards simply cannot meet DoD's expectations from cloud

services, whether security concerns, interoperability, or global, seamless reach. In particular, the CO considered which approach would best serve the agency's security needs and concluded that a single cloud services provider would be best positioned to provide the necessary security for the agency's data. She was careful to document several conditions that led the agency to conclude it must not use multiple awards and we will not second guess her conclusion. Plaintiff offers us no real no basis for questioning any of these conclusions. They were completely reasonable, and we have no grounds to disturb her conclusion that multiple awards cannot be used.

II. The D&F Relies On An Exception To The 10 U.S.C. § 2304a(d)(3) Single Award Prohibition That Does Not Accurately Reflect The Structure Of The JEDI Cloud Solicitation.

Separate from the CO's single award determination, DoD was also required to decide whether it was permitted to use a single award approach in a procurement of this size. DoD anticipates awarding a task order contract for cloud services to a single vendor that, including the full ten-year period, is valued at $10 billion. This triggers the application of 10 U.S.C. § 2304a(d)(3), which prohibits awarding such large task order contracts to a single vendor, unless the agency finds that one of four exceptions to the prohibition exist. Section 2304a(d)(3) states,

> No task or delivery order contract in an amount estimated to exceed [$112 million] (including all options) may be awarded to a single source unless the head of the agency determines in writing that—
>
> (A) the task or delivery orders expected under the contract are so integrally related that only a single source can efficiently perform the work;
>
> (B) the contract provides only for firm, fixed price task orders or delivery orders for—
>
> (i) products for which unit prices are established in the contract; or
>
> (ii) services for which prices are established in the contract for the specific tasks to be performed;
>
> (C) only one source is qualified and capable of performing the

work at a reasonable price to the government; or

(D) because of exceptional circumstances, it is necessary in the public interest to award the contract to a single source.

DoD, through Under Secretary Lord's D&F, decided that the second exception applies to this procurement: "the contract provides only for firm, fixed price (FFP) task orders . . . for services for which prices are established in the contract for the specific tasks to be performed." AR 318.

At first blush, DoD's D&F tracks precisely with the chosen exception: the JEDI Cloud RFP provides only for firm, fixed price task orders. It solicits IaaS, PaaS, and support services for which offerors will propose a catalog of prices; that catalog will be incorporated into the contract, i.e., established, at the time of award. If the prices of all possible tasks were "established" in this fashion, then we would agree that exception (B)(ii) could be relied upon. That is not the case, however.

The D&F acknowledged that, during the possible ten-year life of the contract, services not contemplated at the time of initial award would likely be needed and added to the contract through the technology refresh provision, Section H2 New Services. Section H2 was crafted because DoD knows that the cloud computing sector is constantly evolving. *E.g.*, AR Tab 130 at 8721 ("IaaS/PaaS offerings are not static and will be updated overtime both in terms of available services and applicable pricing. The clauses are necessary to maintain commercial parity with how cloud services evolve and are priced."); AR Tab 137 at 9603 ("The landscape of cloud offerings is evolving. . . . With growing demand comes an evolving landscape of supply. It seems new cloud providers are emerging monthly, and the service offerings of the vendors are rapidly shifting.").

If at some point over the ten years of the contract the cloud services provider creates a new service, Section H2 requires it to offer that new service to DoD at a price not "higher than the price that is publicly-available in the commercial marketplace in the continental United States." AR 318. The CO will then decide whether to add the new service. The clause also permits DoD to acquire services before they are available on the commercial market or that will not be offered on the commercial market. After the award, and perforce, after any competition, these new services could only be obtained from the single awardee. Of necessity, then, these services could not be identified as "specific tasks," much less priced, at the time of the award.

Recognizing the apparent inconsistency between Section H2 and the requirements of § 2304a(d)(3)(B)(ii), the D&F attempted to reconcile the use of Section H2 with the exception DoD chose to justify a single award: "As with any other cloud offering, once the new service is added to the catalog, the unit price is fixed and cannot be changed without CO approval." *Id.* In other words, even though the tasks are different than those described and priced in the original contract, the contract eventually will still use only firm, fixed price task orders. The agency found that its custom-made technology refresh provision therefore is consistent with "[firm, fixed price] task orders for services for which prices are established in the contract for the specific tasks to be performed." *Id.* It is difficult to treat this as anything more sophisticated than the assertion that "these are established fixed prices for specific services because we say they are."

As Oracle points out, there is a logical disconnect between claiming that prices are "established in the contract" for "specific tasks" while simultaneously acknowledging that those tasks, and their accompanying prices, do not yet exist. While the government and intervenor respond that Oracle is improperly reading a term into the text of § 2304a(d)(3)(B)(ii) that is not present, namely "at the time of entering the contract," plaintiff does not have to "read" this interpretation into the statute. It is already present in the use of the term, "established," and in the language of the prohibition itself that "no contract may be awarded." Reading this as a present tense description of the status of the contract terms is much less tortured than inserting a phrase with a future spin: "or which may be established in the contract prior to placing future task orders." We see no ambiguity in the language. In an ordinary reading, prices for specific services must be "established" at the time of contracting. Prices for new, additional services to be identified and priced in the future, even if they may be capped in some cases, are not, by definition, fixed or established at the time of contracting. It should go without saying that the exception must be true at the time of award—no task order contract exceeding $112 million "may be awarded"—and exception (B)(ii) speaks of prices and specific tasks as "established in the contract," not that "will be" established in the future. Given the tenor of the language employed in describing the need for cloud computing, Section H2 is not a trivial addition.

The government argues that requiring prices for specific tasks to be established at the time of contracting would prevent DoD from modifying the contract during performance in any way. This is not entirely accurate. It is true that the statutory prohibition prevents a particular type of change—

the contractor and agency cannot add new tasks at new prices after entering the contract. Other types of modifications that fall outside of the bespoke Section H2 are not affected, however. The use of a technology refresh provision thus appears to be at odds with § 2304a(d)(3)(B)(ii), and the Under Secretary apparently chose an exception under § 2304a(d)(3) which does not fit the contract.

This conclusion is obviously somewhat in tension with our previous decision upholding the CO's decision that multiple awards are not allowed. This peculiar state of affairs is an artifact of a code section which is a mixture, rather than an alloy, of various pieces of legislation. Not surprisingly, the parties have different views about the implications of this possible result and whether Oracle is prejudiced by the flawed D&F.

III. Oracle Cannot Demonstrate Prejudice As A Result Of The Flawed D&F.

Oracle argues that the requirements are independent and that it is prejudiced by the agency's failure to comply with 10 U.S.C. § 2304a(d)(3) because Oracle could have competed in a properly structured multiple award procurement. Oracle's argument assumes there would be some purpose to remanding to the agency to obtain a new D&F, despite the CO's conclusion. And not operating on that assumption treats § 2304a(d)(3) as superfluous, which the court is reluctant to do. Moreover, Oracle argues that it is prejudiced because the agency's needs, as expressed in the gate criteria, could well be different in a multiple award procurement. It argues that the single award determination and the gate criteria are necessarily connected: the agency improperly decided to award the majority of its cloud computing business to one provider and, thus, the agency must have a monolithic provider to meet its minimum needs.

The government and AWS first respond that if the CO's decision is upheld, the Under Secretary could not have sanctioned the use of multiple awards, so a remand would be pointless. This assertion strikes us as a tad sophistical, but, in any event, and fortunately for the defendant, we think their next argument concerning prejudice has merit.

The government and intervenor argue that Oracle cannot demonstrate prejudice as a result of the flawed D&F because the agency's minimum needs would not have changed in a multiple-award scenario. In other words, Gate Criteria 1.1 and 1.2 are enforceable, Oracle cannot meet them, and there is no connection between the single award determination, the gate criteria, and

possible ethics violations. Under any scenario, Oracle would be out of the competition.

In substance we agree, at least with respect to Gate Criteria 1.2. While Oracle may well be correct that some aspects of the gate criteria are driven by the agency's insistence on using a single provider to manage an immense amount of data, one critical aspect of the gate criteria is not connected to the choice of a single provider: data security.

The security concern is explicit in Gate Criteria 1.2. The security component of Gate Criteria 1.2 is based on DoD's "minimum security requirements for processing or storing DoD's least sensitive information." AR 947. Mr. Van Name explained that the challenged portion of Gate Criteria 1.2 reflects the "minimum criteria necessary for DoD to have confidence that the Offeror's proposed data centers have met the underlying physical security requirements necessary to successfully perform the contract." *Id.* Many of the acquisition documents bolster the agency's conviction that use of multiple cloud service providers exponentially increases the challenge of securing data. We have no reason to doubt the agency's many representations that the Gate Criteria 1.2 security requirements are the minimum that will be necessary to perform even the least sensitive aspects of the JEDI Cloud project.

In other words, although this criteria presumes a single award, the only logical conclusion is that, if multiple awards were made, the security concerns would ratchet up, not down. They are, indeed, minimally stated. If Oracle cannot meet Gate Criteria 1.2 as currently configured, it is thus not prejudiced by the decision to make a single award. The agency's needs would not change, so Oracle would not stand a better chance of being awarded this contract if the agency determined that the procurement must be changed to multiple award.

Thus, in order to prevail, Oracle must show that both Gate Criteria 1.1 and Gate Criteria 1.2 are otherwise unenforceable. It would not be sufficient for Oracle to demonstrate that Gate Criteria 1.1 alone is unenforceable, because it also cannot not meet Gate Criteria 1.2. We need not consider Gate Criteria 1.1, or 1.6 for that matter, because we are satisfied for reasons set out below, that Gate Criteria 1.2 is enforceable.

IV. Gate Criteria 1.2 Is Enforceable.

Oracle argues that Gate Criteria 1.2 is unenforceable because it exceeds the agency's minimum needs, that it is in fact an unauthorized qualification requirement, and it amounts to the use of "other than competitive procedures" without proper justification.

Oracle first argues that DoD did not identify an underlying need before imposing Gate Criteria 1.2. When preparing to procure services, the agency must "specify the agency's needs and solicit bids or proposals in a manner designed to achieve full and open competition for the procurement." 10 U.S.C. § 2305(a)(1)(A)(i) (2012). The solicitation must "include specifications which[,] consistent with the provisions of this chapter, permit full and open competition; and include restrictive provisions or conditions only to the extent necessary to satisfy the needs of the agency or as authorized by law." § 2305(a)(1)(B). The specifications "shall depend on the nature of the needs of the agency and the market available to satisfy such needs." § 2305(a)(1)(C). The agency may state specifications for "(i) function, so that a variety of products or services may qualify; (ii) performance, including specifications of the range of acceptable characteristics or of the minimum acceptable standards; or (iii) design requirements." *Id.*

Oracle alleges that the requirement in Gate Criteria 1.2 that certain offerings must be FedRAMP Moderate "Authorized" by the proposal deadline exceeds DoD's minimum needs. Oracle does not challenge any other aspect of Gate Criteria 1.2 in terms of the agency's need. Oracle also does not argue that the agency could not require some security assurance at the time of proposal, just that the agency improperly chose FedRAMP authorization. The government responds that the agency has properly justified the criteria based on its needs.

We agree with the government that Gate Criteria 1.2 is tied to the agency's minimum needs. Mr. Van Name's memorandum explained that "FedRAMP Moderate is the Federal cloud computing standard and represents the Department's minimum security requirements for processing or storing DoD's least sensitive information." AR 947. The cloud services provider will be required to work with the agency to meet the "more stringent security requirements outlined in the JEDI Cyber Security Plan" shortly after award, and if the cloud services provider cannot meet even the FedRAMP Moderate standard at the time of proposal the agency will not be able to move forward with implementing the JEDI Cloud in a timely manner. *Id.* Furthermore, even though the JEDI Cyber Security Plan is a separate requirement, Mr. Van Name explained that "FedRAMP Moderate is the minimum criteria necessary for DoD to have confidence that the Offeror's

proposed data centers have met the underlying physical security requirements necessary to successfully perform the contract." AR 947-48. It is a useful proxy, in other words, for the agency's real need. If an offeror were unable to meet the lower threshold, it could not hope to meet the higher.

Oracle argues by pointing to Slack messages and risk statements that DoD's security requirements are not the real reason for this Gate Criteria 1.2 component; rather the agency wanted to decrease the possibility of too many proposals or protests. *E.g.*, AR 422, 3123. The Slack messages and risk sections in acquisition planning documents that Oracle points to do not, however, undermine Mr. Van Name's justification. The agency's concern about being inundated with too many unqualified offers or protests does not reveal a nefarious purpose for the gate criteria; that concern can coexist with legitimate security risks. The agency's justification provides a rational basis for why it chose FedRAMP Moderate "Authorized" to satisfy itself that a bidder's offerings would be eligible to house DoD data.

Alternatively, Oracle argues that Gate Criteria 1.2 is a qualification requirement subject to the provisions of 10 U.S.C. § 2319 (2012). The government responds that Oracle waived this argument, because it had the opportunity to object to the terms of Gate Criteria 1.2 as improperly imposed qualification requirements prior to the close of the bidding process and failed to do so. *See Blue & Gold Fleet, LP v. United States*, 492 F.3d 1308, 1313 (Fed. Cir. 2007). The government is correct—Oracle's more generalized challenges to the criteria did not raise this precise argument until post-hearing comments submitted to GAO on October 18, 2018, after the close of bidding. In any event, even if the qualification requirement argument was timely raised, Gate Criteria 1.2 is not a qualification requirement.

A qualification requirement is "a requirement for testing or other quality assurance demonstration that must be completed by an offeror before award of a contract." 10 U.S.C. § 2319(a). If using one, the agency must prepare a written justification stating the requirement and explaining why it must be completed pre-award, specifying a cost estimate, providing for a prompt opportunity for an offeror to demonstrate its ability, and ensuring that the offeror is provided specific information if it fails the qualification requirement. A qualification requirement is generally "a qualified bidders list, qualified manufacturers list, or qualified products list." § 2319(c)(3).

This distinguishes a specification from a qualification requirement. Specifications, the subject of 10 U.S.C. § 2305(a)(1)(A)(i)-(B)(ii), "are the requirements of the particular project for which the bids are sought, such as

design requirements, functional requirements, or performance requirements." *W.G. Yates & Sons Const. Co., Inc. v. Caldera*, 192 F.3d 987, 994 (Fed. Cir. 1999). "Qualification requirements, on the other hand, are activities which establish the experience and abilities of the bidder to assure the government that the bidder has the ability to carry out and complete the contract." *Id.*

In *W.G. Yates*, the Federal Circuit found that the Army had improperly established a qualification requirement. The Army required a potential bidder "to have designed, manufactured, and installed ten similar door systems in satisfactory operation for a minimum of five years" prior to award. *Id.* at 993. The Federal Circuit concluded that the requirement was not a specification, because it pertained to "to successful completion of other, similar hangar door projects," unrelated to the Army's solicitation. *Id.* at 994. A specification would relate to the project at hand, such as "the size of the doors, structural steel requirements, ability to withstand wind loads, and the like." *Id.*

By comparison, in *California Industries Facilities Resources, Inc. v. United States*, this court considered whether the Air Force improperly imposed qualification requirements when it required liner system, wind gust, and snow load testing for certain military shelters prior to award. 80 Fed. Cl. 633, 641-43 (2008). The court compared the Air Force's requirement to the Army's requirement in *W.G. Yates* and also explored GAO's explanations of qualification requirements. GAO considers a qualification requirement "a systematized quality assurance demonstration requirement on a continuing basis as an eligibility for award," *Aydin Corp.*—Reconsideration, B–224185, 87–1 CPD ¶ 141 (Feb. 10, 1987), or "a system [that] is intended to be used prior to, and independent of, the specific procurement action." *Scot, Inc.*, B–292580, 2003 CPD ¶ 173 (Oct. 3, 2003). The court concluded that the Air Force's testing requirements were specifications, because they did not relate to other contracts, products, or a system independent of the procurement but were focused on the particular features of the shelters that the offerors would propose.

Oracle argues that the FedRAMP Moderate "Authorized" requirement in Gate Criteria 1.2 is a qualification requirement, specifically because that authorization would have been acquired in the past through either the Joint Authorization Board or from another agency. The substance of this requirement is that an offeror must show that a sampling of its offerings, at datacenters 150 miles apart, have certain security features. Oracle contends that this is a backwards-looking, independent quality assurance mechanism

because the awardee will not be subject to the FedRAMP approval process and DoD described using FedRAMP as a "mechanism to validate that the core architecture is extensible and likely to be able to meet the JEDI Cloud requirements across all service offerings." AR Tab 43 at 955.

The FedRAMP authorization requirement does resemble an independent quality assurance system in some respects, but a few facts distinguish this component of Gate Criteria 1.2 from the "ten similar door systems in satisfactory operation for a minimum of five years" requirement in *W.G. Yates*. First, the agency did not require an offeror to prequalify in order to submit a proposal or to be on qualified bidders list prior to submitting its proposal. In that way the JEDI Cloud gate criteria are distinctly unlike classic qualification requirements. Second, as Oracle acknowledges, FedRAMP authorization is not an independent, systematic requirement that DoD imposes in its procurements. Third, the security features that FedRAMP authorization includes are the security features that DoD believes are in fact the minimum necessary to store DoD data for the JEDI Cloud project itself. The agency is not using the FedRAMP process as a way to examine the offeror's past performance storing government data. Rather it is a uniform way to determine which offerors have certain security capabilities on a number of their cloud offerings. The offeror cannot store even the least secure data without such security features. DoD can specify that an offeror must show that some of its offerings can meet certain security baselines, using a uniform tool to measure that security baseline, without triggering a qualification requirement.

Finally, Oracle argues that Gate Criteria 1.2 transforms this procurement into one that uses other than competitive procedures. The agency "(A) shall obtain full and open competition through the use of competitive procedures in accordance with the requirements of this chapter and the Federal Acquisition Regulation; and (B) shall use the competitive procedure or combination of competitive procedures that is best suited under the circumstances of the procurement." 10 U.S.C. § 2304(a)(1). The agency "may use other than competitive procedures," when one of seven conditions is present. § 2304(c).

Relevant here, the agency may forgo competitive procedures when the services "are available . . . only from a limited number of responsible sources and no other type of property or services will satisfy the needs of the agency," § 2304(c)(1), or the agency's need "is of such an unusual and compelling urgency that the United States would be seriously injured unless the agency is permitted to limit the number of sources . . . ." § 2304(c)(2).

Even if the agency has grounds to forgo competitive procedures, it must not award a contract under such circumstances "unless the contracting officer . . . justifies the use of such procedures in writing and certifies the accuracy and completeness of the justification;" the justification is properly approved; and any required notice is given. § 2304(f)(1).

Oracle alleges that the agency chose the gate criteria specifically to limit the number of bidders, effectively resulting in "other than competitive procedures." The statements that Oracle points to, however, are not in the gate criteria justification memorandum. They appear either in Slack messages between members of Defense Digital Service, or in the risk section of acquisition planning documents.

The Federal Circuit recognized in *National Government Services, Inc. v. United States*, "the unremarkable proposition that "a solicitation requirement (such as a past experience requirement) is not necessarily objectionable simply because that requirement has the effect of excluding certain offerors who cannot satisfy that requirement." 923 F.3d 977, 985 (Fed. Cir. 2019). The few record statements Oracle highlights are insufficient to demonstrate that the agency is using "other than competitive procedures" in the JEDI Cloud procurement. The agency structured this procurement to use full and open competition and the gate criteria are just the first step in the evaluation of proposals. The government aptly pointed out that the substance of the gate criteria evaluation could have occurred at any point in evaluation of proposals; the agency simply put the gate criteria first to ensure its evaluation was not wasted on offerors who could not meet the agency's minimum needs. As Mr. Van Name's memorandum reflects, the gate criteria are based on more than the agency's awareness that its timeline would be delayed if it received too many proposals. While the gate criteria certainly had the effect of excluding some offerors, that does not transform the procurement into less than full and open competition.

Specific to the Gate Criteria 1.2 component that certain offerings must be FedRAMP Moderate "Authorized," Oracle argues that the agency knew at the time of issuing the RFP that only two companies could meet that gate criteria. As such, the agency knew that the necessary cloud services are available from only a limited number of responsible sources. Because the agency knew that only a limited number of responsible sources could offer the services, the agency necessarily chose less than open competition without following the proper procedure. Oracle bases this argument on the fact that "the FedRAMP approval process is government-run (with DoD involvement). DoD necessarily knew that only two offerors could meet this

requirement—Microsoft and AWS." Pl.'s Suppl. Mot. 41. In its response and reply brief, Oracle adds that "[b]ased on its market research, DoD necessarily knew that only two cloud service providers had the existing infrastructure with FedRAMP authorized offerings to meet the gate." Pl.'s Resp. & Reply 23.

The government is correct, however, that evaluation criteria which have the effect of limiting competition do not necessarily trigger the procedures required by § 2304(c). Full and open competition "means that all responsible sources are permitted to submit sealed bids or competitive proposals on the procurement." 41 U.S.C. § 107 (2012); 10 U.S.C. § 2302(3)(D) (2012). Here, they were. The solicitation permitted all responsible sources to submit proposals. Four offerors submitted proposals. Even if the agency knew that as of early 2018 only certain firms would survive the gate criteria, it nevertheless chose to accept proposals from all responsible sources. Indeed, the CO in her memorandum documenting the rationale for a single award contract stated, "The results of market research indicate that multiple sources are capable of satisfying DoD's requirements for JEDI Cloud and that commercial cloud services customarily provided in the commercial marketplace are available to meet a majority of DoD's requirements." AR 457. The FedRAMP authorization component does not transform the solicitation into one for less than full and open competition.

Having considered both the single award determinations and Gate Criteria 1.2, we can return to the question of prejudice. Assuming the agency relied on a flawed D&F, would Oracle have had a better chance of competing for this contract? We can confidently answer, no, because Oracle could not meet the agency's properly imposed security requirements.

This conclusion might normally be the natural stopping point in our decision, but Oracle raises a few other arguments that it contends present an independent prejudicial error requiring this procurement to be set aside. We thus address the competitive range briefly before turning to the conflicts of interest determinations.

V. The CO Rationally Set The Competitive Range.

Oracle's next argument is that, regardless of the propriety of the gate criteria, the agency unequally considered offerors when she permitted Microsoft and AWS to advance to a competitive range, despite the fact that they were both considered unawardable on several factors. Since all four offerors failed some factors, Oracle contends that the agency should have

established a range of all four offerors.

Oracle is incorrect. DoD reasonably evaluated the offerors according to the terms in Section M of the solicitation. Section M unambiguously provided that any offeror who failed Factor 1, the gate criteria, would be immediately eliminated from consideration. Oracle and IBM failed Factor 1 and were thus properly eliminated. According to the terms of Section M, only AWS and Microsoft were eligible for further evaluation. The agency took the next step of evaluating both under the non-price factors and, finding both unawardable and in need of significant revisions, chose to set the competitive range of those two offerors and continue on to discussions and revisions. The evaluation thus equally treated all offerors in accordance with the process set out in Section M.

VI. The CO's Determinations Regarding Conflicts Of Interest Are Rational And Consistent With FAR Subparts 3 And 9.

Oracle challenges the CO's determination that the involvement in the procurement by Mssrs. Ubhi, DeMartino, and Gavin did not taint the process. It also argues that the CO irrationally determined that AWS does not have an organizational conflict of interest. Oracle contends that its conflicts of interest arguments are independent bases on which to set aside this procurement, because the individual conflicts tainted the structure of the procurement, particularly the single award determinations and the substance of the gate criteria.

The facts on which Oracle rests its conflicts of interest allegations are certainly sufficient to raise eyebrows. The CO concluded that at least two DoD officials disregarded their ethical obligations by negotiating for AWS employment while working on this procurement. Through lax oversight, or in the case of Ubhi, deception, DoD was apparently unaware of this fact. AWS, for its part, was too prepared to take at face value assurances by Mr. Ubhi that he had complied with his ethical obligations. While there is nothing per se illegal about capitalizing on relevant experience in moving to the private sector, the larger impression left is of a constant gravitational pull on agency employees by technology behemoths. The dynamic apparently is real enough that one would hope the agency would be more alert to the possibilities of an erosion of public confidence, particularly given the risk to the agency in having to redo procurements of this size.

The limited question, however, is whether any of the actions called out make a difference to the outcome. And in particular, the even narrower

question before the court is whether the CO's conclusion of no impact is reasonable. The court is fully prepared to enforce the agency's obligation to redo part or all of this procurement if the CO's conclusion that there was no impact was unreasonable in any respect, but our ultimate conclusion, after a detailed examination of the record, is that the CO's work was thorough and even-handed. She understood the legal and factual questions and considered the relevant evidence. It is unfortunate that the employees in question gave her so much evidence to consider, making it is easy for Oracle to cherry pick from the vast amount of communications and isolate a few suggestive sound bites. But that volume should not compel an unreasoned leap to the conclusion that there was fire as well as smoke.

1. Individual Conflicts of Interest

We review the CO's determinations for a rational basis and consistency with the applicable law. Regarding the personal conflicts of interest, "[a] contracting officer who receives or obtains information of a violation or possible violation of 41 U.S.C. 2102, 2103, or 2104 (see 3.104-3) must determine if the reported violation or possible violation has any impact on the pending award or selection of the contractor." FAR 3.01-7(a) (2018). If the CO determines that there is no impact on the procurement, she must forward the information to a designated individual within the agency. *Id.* If that individual concurs with the CO, the procurement may proceed.[11] *Id.*

Here, the CO determined that, although there were some violations or possible violations of law relating to conflicts of interest, those conflicted individuals did not impact the decision to use a single award approach or the substance of the evaluation factors. It is easy to critique uncritically her analysis and characterize it as, "there were lots of people involved in the decisions here, so it's unlikely the persons in question impacted the result." We are satisfied that would be a simplistic and inaccurate critique. In fact, there were a lot of people involved in this procurement, and the ones called

[11] Oracle argues that the court must go beyond the CO's determinations in this matter and consider whether these personal conflicts of interest constitute a violation of certain statutes, particularly 18 U.S.C. § 208 as it relates to Mr. Ubhi. We disagree. Our standard of review is explicitly set out in 28 U.S.C. § 1491(b)(4) and does not include this court holding a mini criminal trial in the course of deciding a bid protest. In any event, the CO here considered possible violations of 18 U.S.C. § 208 and performed an "even if" analysis as a part of her FAR Subpart 3 determination.

out by the ethics investigations indeed were a very small part of the substance of the procurement, both as a result of their limited roles and as a result of the timing of important decisions.

We think that the conclusion the CO in effect asks us to draw, that these individuals were bit players in the JEDI Cloud project, is correct. They were not members of the Cloud Executive Steering Group, the Cloud Computing Program Office, the Joint Requirements Oversight Council, or the Cost Assessment and Program Evaluation, and that is only a partial list of the many DoD offices and officials who had a role in the structure of this procurement. *See, e.g.*, AR Tab 64, 91, 94. Nor were they acting as the CO, Under Secretary, the Chief Information Officer, the Deputy Chief Management Officer, or other official who developed or signed off on challenged components of this procurement. While they should not have had the opportunity to work on the JEDI Cloud procurement at all, or at least for certain periods of time, nevertheless, their involvement does not taint the work of many other persons who had the real control of the direction of the JEDI Cloud project.

A. Mr. DeMartino

The CO considered all of the relevant facts regarding Mr. DeMartino's involvement. None of the facts contradict her ultimate conclusion that his involvement with JEDI did not impact the procurement. While we might view the CO's characterizations as a bit generous (for instance, Mr. DeMartino clearly did not work with government ethics personnel "throughout" his DoD employment), nevertheless, she rationally determined that he was merely a go-between for the Deputy Secretary and did not have substantive input into the structure or content of the solicitation. Specifically, Mr. DeMartino did not have a voice in whether DoD should use a single or multiple award approach and did not craft the substance of the evaluation factors. His employer, the Deputy Secretary, was expressly "open" to either single or multiple award at least into late 2017. AR 4352. Moreover, DeMartino did not leave DoD to work for AWS during, or apparently after this procurement. We view him as not relevant to the AWS organizational conflict of interest analysis.

B. Mr. Gavin

The CO likewise considered all of the relevant facts regarding Mr. Gavin's involvement. First, her conclusion that "Mr. Gavin violated FAR 3.101-1, and possibly violated 18 U.S.C. § 208 and its implementing

regulations," is well-supported. The CO properly went on to ask whether, in light of the conflict, Mr. Gavin impacted the procurement. The record supports her conclusion that Mr. Gavin was involved only to offer his knowledge of the Navy's cloud services experience. He was not a member of the Cloud Executive Steering Group, Defense Digital Service, the Chief Information Office, or any other team tasked with spearheading aspects of this procurement. As far as we can tell from the record, he did not assist in crafting the single award determinations or the technical substance of the evaluation factors. At most, he attended a few JEDI Cloud meetings. He does not appear to have obtained any contractor bid or proposal information nor does he appear to have introduced any bias toward AWS into the meetings he attended. It would have been proper for the CO to discount Mr. Gavin's affidavit as she did Mr. Ubhi's, because she felt he had violated FAR 3.101-1. Even when his involvement is considered without his own assurances that he did not act improperly, the CO's review of the record was reasonable that Mr. Gavin was involved solely to offer his past experience with cloud computing contracts.

Oracle is correct that we do not know exactly what Mr. Gavin communicated to AWS's JEDI proposal team lead prior to the information firewall. Mr. Gavin acted improperly in that regard, as did the AWS employee who spoke with him. But the CO reasonably determined that Mr. Gavin simply did not have access to competitively useful information to convey to AWS. By the time Mr. Gavin began working at AWS, the draft RFP had been released, providing AWS access to the relevant information that also appeared in the draft Acquisition Strategy. We thus find that the CO's conclusion regarding Mr. Gavin was rational.

C. Mr. Ubhi

The last individual who worked on the procurement despite a personal conflict of interest was Mr. Ubhi. We agree with the CO that his behavior was disconcerting. Despite being aware of his ethical obligations, he ignored them. The CO drew six conclusions regarding Mr. Ubhi; we will consider each in turn.

First, the CO reached the obvious conclusion that Mr. Ubhi violated the FAR 3.101-1 requirement that officials "avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government contractor relationships" and thus the matter had to be referred to the DoD Inspector General. AR 58707-09. She also considered related prohibitions and reasonably concluded that Mr. Ubhi's behavior must be referred to the

Inspector General for investigation of "whether Mr. Ubhi violated 18 U.S.C. § 208, 5 CFR § 2635.604, and 5 CFR § 2635.402." AR 58709. The CO continued her analysis, as FAR 3.104-7 directed her to do, assuming that Mr. Ubhi's participation was unethical and might have impacted events he participated in. We find nothing irrational in this first conclusion.

Next, the CO concluded both that Mr. Ubhi's employment package did not reflect a quid pro quo for nonpublic information relating to the JEDI Cloud procurement and that there is no evidence that Mr. Ubhi shared nonpublic information with AWS. To reach this conclusion, she considered all of the employment negotiations between Mr. Ubhi and AWS (beginning before the JEDI Cloud procurement) and his employment offer. Based on discussions and research, she concluded that AWS was interested in hiring Mr. Ubhi regardless of his JEDI Cloud involvement and that his substantial employment package did not appear to be tied to receiving nonpublic information. Her conclusion here is reasonable and highlights an important aspect of Mr. Ubhi's post-DoD work: he did not return to AWS to work on its JEDI Cloud proposal team, for its Federal Business Sector, or for the DoD Programs section.

She went on to consider the communications DoD had with AWS and the affidavits submitted from AWS employees stating that they had not received, or hoped to receive, any information from Mr. Ubhi. She considered affidavits from individuals both within AWS's commercial sector (where Mr. Ubhi is now employed) and AWS's federal business sector (where the AWS JEDI Team works). None of those affidavits suggest that Mr. Ubhi shared any information with the JEDI Cloud team or that the team would welcome his input. The CO did not find any evidence to suggest that he had shared nonpublic information with AWS or that AWS had solicited such information. The CO took the whole record into account, discounted Mr. Ubhi's assurances, and considered AWS's apparent motivations and the statements made by its employees under penalty of perjury. We did not find any critical facts that she overlooked in reaching this conclusion and thus find no reason to disturb it.

The CO's third conclusion was that even if Mr. Ubhi had disclosed nonpublic information, none of it would have been competitively useful. The CO detailed both potential offeror information and DoD information that Mr. Ubhi had access to as a member of the Defense Digital Service team. She detailed her analysis that the vendor meeting information would not have been competitively useful to AWS and that much of the DoD information was premature, based on incorrect assumptions, and, in any event, was

revealed to the public during meetings and industry research. Again, the CO considered this question closely and we have found nothing in the record to suggest that her explanation was unsatisfactory.

Oracle takes issue with the fact that the CO, in her fourth conclusion, applied FAR 3.104-3(c) too literally. The section requires officials such as Mr. Ubhi to promptly report contacting or being contacted "by a person who is an offeror in that Federal agency procurement regarding possible non-Federal employment for that official" and then to disqualify himself from further personal and substantial participation in the procurement. FAR 3.104-3(c) (emphasis added). The CO repeated that Mr. Ubhi was personally and substantially involved. She found that Mr. Ubhi failed to "promptly report the contact with AWS in writing to his supervisor and the agency ethics official" and failed to timely recuse himself from JEDI Cloud activities. But Mr. Ubhi did not violate this particular section of FAR Subpart 3 because AWS was not an offeror at the time. The CO repeated that Mr. Ubhi behaved unethically and improperly and she read and applied FAR 3.104-3(c) as written. We find nothing objectionable in her analysis under FAR 3.104-3(c).

Fifth, the CO concluded that Mr. Ubhi's seven-week contribution to the planning stage of the JEDI Cloud procurement did not introduce bias in favor of AWS. The CO reviewed Mr. Ubhi's work and found that, despite often expressing vehement opinions about various people and companies, he did not lobby in favor of a particular cloud services provider. Her conclusion is supported in the record.

Sixth, the CO concluded that even if Mr. Ubhi tried to introduce bias into the procurement process, he failed. Oracle argues that the reasoning behind this determination was flawed. First, the CO found that Mr. Ubhi did not have the technical expertise to substantially influence the procurement. Second, she concluded that his actual attempts to influence the procurement were limited. Third, the key decisions were made after Mr. Ubhi recused himself.

As to Mr. Ubhi's technical expertise, or lack thereof, the record reflects that Mr. Ubhi' specialty was lead product manager. The CO placed Mr. Ubhi's participation in the broader context of the Defense Digital Service team, which was only one team among at least half a dozen DoD organizations that contributed to and reviewed the content of the JEDI Cloud solicitation. Mr. Van Name explained in his GAO testimony that Mr. Ubhi was indeed conversant in cloud computing, as one must be to work as an

industry specialist in cloud computing. But his involvement early in the planning stage of this procurement does not reflect any meaningful role in crafting the technical aspects of this solicitation, particularly the gate criteria. We are not aware of any step in the procurement that required his approval. By the time DoD finished its decisions and amendments to Gate Criteria 1.2, Mr. Ubhi had long since left DoD. In reality, the gate criteria, particularly the security requirements, were crafted by a number of DoD teams which focused on technical and security requirements. Mr. Ubhi's primary role was industry liaison; the record does not warrant attributing to him any serious involvement in the technical or security aspects of the gate criteria.

While Oracle points to Mr. Ubhi's loud advocacy for a single award approach, real DoD decisionmakers had been independently in favor of a single award approach both before and after Mr. Ubhi's involvement. As early as September 14, 2017, the Cloud Executive Steering Group (of which Mr. Ubhi was not a member) expressed a preference for a single award approach. On the other hand, after Mr. Ubhi left DoD, the Deputy Secretary remained unconvinced regarding which approach to use; he was "[o]pen to the first cloud contract being single source OR multiple source" and asked for a "layout [of] all options and recommendations from Team Cloud" in November 2017. AR 4352. The CO recalled being in a meeting in April 2018 in which "the single award decision was still being vigorously debated." AR 58721. Nor is it credible to suggest that Mr. Ubhi was steering DoD toward AWS. Our narrative began with the visit to AWS (among other cloud service providers) by DoD top brass, before Mr. Ubhi's involvement surfaces.

Ultimately, we find that the CO correctly concluded that although Mr. Ubhi should have never worked on the JEDI Cloud procurement, his involvement did not impact it. We are left with the firm conviction that the agency was headed in the direction of a single award from the beginning, indeed probably before Mr. Ubhi was enlisted to participate in the JEDI Cloud project. The CO is fundamentally correct: if there was a high speed train headed toward a single award decision, Mr. Ubhi was merely a passenger on that train, and certainly not the conductor. Moreover, he exited DoD prior to the substance of the evaluation factors being crafted. Although the CO correctly found the assurances in his affidavit to be untrustworthy, we ultimately agree with the substance of her conclusion that his self-promoting, fabulist and often profanity-laced descriptions of his own role were merely that.

2. Alleged Organizational Conflict of Interest

Finally, Oracle turns to the CO's assessment of AWS. Oracle argues that the CO's determination that AWS did not violate procurement integrity law and does not have an unfair advantage lacks a rational basis. While Oracle's argument focuses on Mr. Gavin's and Mr. Ubhi's relationship with AWS, even though the CO properly considered both Mr. Bouier's and Dr. Sutherland's relationship with the company as well.

FAR Subpart 9 prescribes rules and responsibilities regarding organizational conflicts of interest. "An organizational conflict of interest may result when factors create an actual or potential conflict of interest on an instant contract, or when the nature of the work to be performed on the instant contract creates an actual or potential conflict of interest on a future acquisition." FAR 9.502(c) (2018). It is the CO's responsibility to "[i]dentify and evaluate potential organizational conflicts of interest as early in the acquisition process as possible" and to "[a]void, neutralize, or mitigate significant potential conflicts before contract award." FAR 9.504(a). The CO "should avoid creating unnecessary delays, burdensome information requirements, and excessive documentation. The [CO's] judgment need be formally documented only when a substantive issue concerning potential organizational conflict of interest exists." FAR 9.504(d).

The CO should examine "[e]ach individual contracting situation . . . on the basis of its particular facts and the nature of the proposed contract." FAR 9.505. "The exercise of common sense, good judgment, and sound discretion is required in both the decision on whether a significant potential conflict exists and, if it does, the development of an appropriate means for resolving it." *Id.* Relevant here, the CO should seek to prevent "unfair competitive advantage." *Id.* Such unfair advantage "exists where a contractor competing for award of any Federal contract possesses—(1) Proprietary information that was obtained from a Government official without proper authorization; or (2) Source selection information . . . that is relevant to the contract but is not available to all competitors, and such information would assist that contractor in obtaining the contract." *Id.*

Oracle argues that there can be no question that AWS had a significant, actual conflict and that only extreme measures would eliminate the conflict at this stage. It contends that the CO irrationally determined that AWS could not derive an unfair competitive advantage from the information Mr. Ubhi or Mr. Gavin brought with them to AWS. The government responds that the CO properly determined that a significant potential conflict did not exist, because there is no evidence—in the CO's determination or that

she missed—that indicates AWS possesses proprietary information or source selection information not available to all competitors.

The CO's conclusion that a conflict of interest did not exist was sufficiently supported based on the facts presented to her. She specifically considered whether the DoD employees who accepted jobs at AWS could have, and did, communicate information to AWS that would give AWS an unfair competitive advantage. She concluded that the information the three individuals had could not offer an unfair competitive advantage and that, in any event, there is no evidence that protected information was communicated to AWS.

Her assessment began with whether AWS obtained source selection information that is relevant, not available to all competitors, and would assist AWS in winning the JEDI Cloud contract. The pertinent facts she considered are that Mr. Ubhi participated in many JEDI Cloud meetings and assisted in drafting several pre-RFP documents; he had access to the contents of the Google Drive; Mr. Gavin participated in two meetings and viewed a limited set of documents; and Dr. Sutherland apparently had access to some documents through her work with the Joint Requirements Oversight Council. The substance of the documents to which they had access, however, along with the meeting notes, concerns DoD's need to adopt cloud computing, the disadvantages of not being able to access an enterprise cloud, the list the cloud services DoD would need, and the processes for how to get to closure in the procurement.

AWS could have contemporaneously gathered such information through the November 2017 JEDI Cloud summary, the RFI, meetings with the JEDI Cloud procurement team, and later through the draft RFP and the final solicitation package, not to mention DoD's 2017 meeting with AWS prior to the kickoff of the JEDI Cloud procurement process. DoD was not particularly secretive about its cloud services needs or its plan for the solicitation. In fact, DoD involved industry from the beginning of this procurement. At the time Mr. Ubhi and Mr. Gavin sought AWS employment, no bids or other source selection information existed. We find nothing irrational in the CO's conclusion that Mr. Gavin and Mr. Ubhi did not offer AWS an unfair competitive advantage based on their knowledge of nonpublic information relating to the procurement.

Oracle also argues that Mr. Ubhi had nonpublic information regarding AWS's potential competitors, implying that he had imparted to AWS "[p]roprietary information that was obtained from a Government official

without proper authorization." FAR 9.505(b)(1). There is no real support for this supposition. The CO considered this issue and concluded that the information Mr. Ubhi had access to could be accessed publicly. She also concluded that Mr. Ubhi's knowledge of Microsoft's proprietary information, submitted to DoD during its one-on-one meeting with the JEDI Cloud team, could be accessed publicly. Moreover, none of the information Oracle points out appears to be sensitive to Microsoft's future offer or approach to tackling the JEDI Cloud project. It is a reasonable conclusion that AWS had access to the information with or without Mr. Ubhi.

In this case, there was a significant amount of communication and negotiation between AWS and DoD employees. As in the case of the individual conflicts of interest, the individuals, the company, and the agency were slow to identify the potential this created for an organizational conflict, particularly as it might relate to a procurement of this magnitude, and less than aggressive in heading off potential harm. Nevertheless, our review is not de novo. The question is whether the procurement was tainted, so as to warrant a redo or possible exclusion of AWS, a question that lies, in the first instance, in the hands of the CO. The issue for the court is whether she properly exercised her discretion in concluding that AWS does not have an organizational conflict of interest based on the facts as presented. We believe she correctly focused on the significance of the potential conflict and whether it gave AWS any competitive advantage. Her conclusion that the errors and omissions were not significant and did not give AWS a competitive advantage was reasonable and well supported.

CONCLUSION

Because the court finds that Gate Criteria 1.2 is enforceable, and because Oracle concedes that it could not meet that criteria at the time of proposal submission, we conclude that it cannot demonstrate prejudice as a result of any other possible errors. Plaintiff's motion for judgment on the administrative record is therefore denied. Defendant's and intervenor's respective cross-motions for judgment on the administrative record are granted. The Clerk is directed to enter judgment for defendant. No costs.

s/Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge