IN THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST

ORACLE AMERICA, INC., Plaintiff, v. THE UNITED STATES, Defendant, and AMAZON WEB SERVICES, INC., Defendant-Intervenor.	REDACTED COPY Case No. 18-1880C Senior Judge Eric G. Bruggink [redacted]

SUPPLEMENTAL BID PROTEST COMPLAINT

Pursuant to the United States Court of Federal Claims April 15, 2019 Scheduling Order, Plaintiff Oracle America, Inc. ("Oracle"), by its undersigned counsel, timely files this Supplemental Bid Protest Complaint. Oracle challenges several terms of Department of Defense ("the Agency" or "DoD") Solicitation No. HQ0034-18-R-0077 (the "RFP"), commonly referred to as the Joint Enterprise Defense Infrastructure Cloud procurement ("JEDI"). JEDI solicits a single awardee to provide infrastructure as a service ("IaaS") and platform as a service ("PaaS") cloud services across the entire DoD enterprise, under a ten-year, ten billion dollar, Indefinite Delivery Indefinite Quantity ("IDIQ") contract. In addition, Oracle challenges the Agency's decision to exclude Oracle from the competitive range based on unduly restrictive and arbitrary gate criteria, the conflicts of interest created by multiple government employees participating on JEDI despite relationships with Amazon Web Services, Inc. ("AWS"), and the unfair competitive advantage created by AWS hiring several JEDI officials during the procurement.

[redacted]

I. SUMMARY OF THE CASE

1. Forced by Congressionally-requested Inspector General ("IG") and Federal Bureau of Investigation ("FBI") reviews, public concern, cloud community criticism, and Oracle's protest, DoD (in or about December 2018) began questioning AWS and the former JEDI officials on AWS' payroll only to uncover a web of lies, ethics violations, and misconduct. DoD now concedes that the business dealings of at least two DoD JEDI officials with AWS "violated FAR § 3.101-1 and possibly violated 18 U.S.C. § 208 and its implementing regulations."[1] (Ubhi Mem. at 28 (¶ 99); [redacted] Mem. at 4.)[2]

2. Hidden job offers and bonus payments by a federal contractor (AWS) to federal procurement officials during a multi-billion dollar procurement; downloading and removal of JEDI procurement materials by a JEDI official with an AWS job offer in hand; "highly technical" meetings with AWS cloud competitors orchestrated and conducted by this same official (after committing to return to AWS); strenuous advocacy for gate criteria limiting competition, massive technical requirements favoring AWS, and a single source award all advocated by a DoD official with an undisclosed agreement to return to AWS; AWS officials leveraging a DoD JEDI official with whom AWS had a hidden job agreement in JEDI-related meetings; AWS failing to timely disclose material misstatements made to DoD in connection with a federal procurement; and more, now exist in this procurement record. And the DoD IG and FBI investigations continue. For most contractors, competition exclusion would be the least of the worries. For AWS, there are no consequences. The DoD Defense Digital Service ("DDS") personnel involved in this procurement have demonstrated now twice that they have no

[1] All emphasis of quoted material in this submission is added unless otherwise expressly noted.
[2] Because Oracle expects that DoD will include the documents provided to Oracle counsel on April 10, 2019 in the Supplemental Administrative Record, Oracle has not attached those protected documents to this filing. Oracle can provide the documents on the Court's request.

[redacted]

intention of holding AWS accountable or remedying the conflicts undermining the public trust, no matter how severe the improprieties. Fortunately for the procurement system, taxpayers, contractors, and the United States, the law compels a different outcome.

3. The cloud computing community, trade groups, the press, and Congress have questioned JEDI's design since its inception. The disregard of statutory requirements, the breaks with industry best practices, and the telltale indicia of a procurement crafted around a particular offeror's service all have contributed to the widespread criticism of JEDI. Indeed, every eligible IaaS provider of size (except AWS)[3] has complained about the procurement's structure:

- Google declined to bid for the JEDI contract, noting: "we determined that there were portions of the contract that were out of scope with our current government certifications." Google also stated: "Had the JEDI contract been open to multiple vendors, we would have submitted a compelling solution for portions of it.... At a time when new technology is constantly becoming available, customers should have the ability to take advantage of that innovation."[4]

- IBM protested the JEDI Cloud RFP noting in a public statement that: "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."[5]

- Oracle has challenged the JEDI Cloud RFP and its unduly restrictive criteria.

---

[3] Gartner, a leading information technology marketplace analyst relied on by DoD as part of JEDI, identifies six leading IaaS providers. *See Magic Quadrant for Cloud Infrastructure as a Service, Worldwide*, Gartner (May 23, 2018), https://www.gartner.com/doc/reprints?id=1-50WJ5CK&ct=180525&st=sb (last visited 4/26/19). Alibaba Cloud is a Chinese cloud computing company ineligible to compete in this procurement.

[4] Aaron Gregg, *Google bows out of Pentagon's $10 billion cloud-computing race*, The Washington Post (Oct. 9, 2018), https://www.washingtonpost.com/business/2018/10/09/google-bows-out-out-pentagons-billion-cloud-computing-race/?utm_term=.a52ce34abd46 (last visited 4/26/19).

[5] Sam Gordy, *JEDI: Why We're Protesting*, IBM (Oct. 10, 2018), https://www.ibm.com/blogs/policy/jedi-protest/ (last visited 4/26/19).

[redacted]

- Microsoft severely criticized the JEDI Cloud procurement, questioning its structure and fairness.[6]

4. Ethics watchdogs have challenged the substantial connections between AWS and involved DoD personnel. Legal scholars and commentators have derided DoD's incongruous determination that DoD may use a single source IDIQ procurement to purchase $10 billion of ever-evolving cloud computing services, across ten years, without task order competition, in direct violation of Congress' multi-award mandate.[7] And Congress itself has required reports from the Secretary of Defense, acted to block DoD's use of a single award approach (which direction DoD effectively has ignored), and requested that the DoD IG scrutinize the ties between competitor AWS and the DoD JEDI contracting personnel.

5. As it now turns out, the old adage is true: where there is smoke, there is indeed fire. JEDI is riddled with improprieties, including FAR Part 3 violations, Title 18 transgressions, and 5 C.F.R. deviance—all tied to a single offeror, AWS. Indeed, after repeatedly attacking Oracle for identifying patent gaps and incongruities in the earlier Contracting Officer ("CO") integrity investigation, DoD's belatedly reopened investigation has uncovered an even more troubling web of misconduct. The latest investigation reveals that AWS made undisclosed employment and bonus offers to at least two DoD JEDI officials (Deap Ubhi and [redacted])

---

[6] Billy Mitchell, *DOD defends its decision to move to commercial cloud with a single award*, FedScoop (Mar. 8, 2018), https://www.fedscoop.com/dod-pentagon-jedi-cloud-contract-single-award/ (last visited 4/26/19).

[7] Steven L. Schooner, *Indefinite-Delivery/Indefinite-Quantity Contracts: Time to Correlate Practice and Policy?*, 32 Nash & Cibinic Rep. ¶ 44 (Sept. 2018) ("In a compelling recent example, in one of its highest profile ongoing solicitations [JEDI], the DOD reminds us that the multiple award preference, in practice, is the exception, not the rule.... Lord's D&F appears entirely consistent with her stated emphasis on speed, rather than bureaucracy, control, or regulation."); Chris Pemberton, *Hidden Cloud Opportunities for Technology Service Providers*, Gartner (June 20, 2018), https://www.gartner.com/smarterwithgartner/7-hidden-cloud-growth-opportunities-for-technology-service-providers/ (last visited 4/26/19) ("How can the Pentagon request firm fixed prices on services that don't yet exist?")

[redacted]

during JEDI.[8] Neither official timely disclosed his employment dealings with AWS to DoD or timely recused himself from JEDI. Instead, both Ubhi and [redacted] participated in JEDI, accessing sensitive procurement information even after accepting job offers from AWS. For his part, Ubhi (while gathering and removing extensive sensitive information from DoD) fabricated an elaborate "Tablehero" lie to hide his misconduct. DoD now admits that both Ubhi and [redacted] have violated FAR 3.101-1, potentially 18 U.S.C. § 208, and other regulations. DoD has referred both to the DoD IG for further investigation, presumably as part of the existing Congressionally-requested JEDI investigation. Still, another former AWS consultant (Anthony DeMartino) violated specific DoD Standards of Conduct Office ("SOCO") direction and participated in JEDI despite his covered relationship with AWS.

6. As related to AWS' part in this procurement misconduct, AWS knowingly made job offers to federal procurement officials during a multi-billion dollar procurement.[9] AWS did not disclose the job offers to DoD. AWS did not request DoD ethics letters from Ubhi or apparently [redacted] regarding what work the officials had performed for DoD or could perform for AWS. AWS did not timely or properly set up ethical walls to protect against improper use of information possessed by the former DoD officials. And, AWS did not see fit to correct the errant record before DoD, the U.S. Government Accountability Office ("GAO"), or this Court (despite necessary awareness of Ubhi's "Tablehero" lies) until February 2019. AWS and Ubhi even participated together in a DoD JEDI-related meeting, with Ubhi pretending to act as an unbiased DoD official—neither disclosed their employment agreement to DoD. And

[8] For instance, despite AWS necessarily knowing Ubhi had lied to DoD, AWS just months ago told this Court that "Ubhi acted specifically to avoid any potential conflict by voluntarily recusing himself from any JEDI activities before he eventually returned to AWS." (Dkt. 41 at 31.)

[9] Ubhi also apparently received a substantial bonus.

[redacted]

significantly, this is without anything but a perfunctory review of what happened to the information improperly downloaded, removed, accessed, etc.

7. To be certain, the procurement integrity issues which have derailed the procurement and stayed this protest merit significant Court scrutiny (and AWS exclusion). But other significant violations of law also exist. Specifically, Oracle's protest focuses principally and narrowly on targeted statutory procurement flaws associated with the single source decision and three flawed gate criteria—flaws that remain irrespective of the procurement misconduct findings. Oracle believes and asserts that these conflicts impacted each allegation of this protest, but whether the challenged criteria resulted from procurement misconduct or legal error ultimately does not matter as the criteria also violate the United States Code and FAR.

8. By Count I, Oracle alleges that DoD has violated 10 U.S.C. § 2304a(d)(3) in soliciting this $10 billion IDIQ contract, with near constant technology refresh requirements, as a single award. In 2008, Congress, confronted with numerous examples of DoD's runaway, single source IDIQ contracts, prohibited use of such contracts absent a head-of-agency determination that one of four narrow exceptions existed. As relevant here (based on the exception DoD selected), section 2304a(d)(3) permits the award of an IDIQ contract valued over $112 million to a single source 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); 48 C.F.R. § 16.504(c)(1)(ii)(D). DoD, by the challenged determination and finding ("D&F"), asserts that the awardee's cloud catalogs proposed for JEDI and incorporated into the contract will cover all services delivered across the potential ten years of performance and include a "single, fixed unit price for delivery of that particular cloud service." (AR Tab 16 at 319.) The RFP and record demonstrate that this is not so.

[redacted]

9. DoD designed JEDI to help DoD keep pace with the rapidly-evolving commercial cloud arena by having the awardee regularly add new commercial cloud services onto the JEDI contract. In this respect, JEDI is a classic IDIQ technology contract of the very type that led Congress to enact provisions favoring task order competition. The Office of Management and Budget ("OMB") has described the backdrop for the earliest single IDIQ contract restrictions:

> Use of multiple award contracts may be especially effective for maintaining better prices and quality in the IT market. Before FASA, many agencies relied on long-term ID/IQ and umbrella contracts with technology refreshment and price reduction clauses to take advantage of falling prices and new technology. Even with these clauses, the government had to negotiate in a sole-source environment and was often unable to realize the economies and efficiencies afforded by vigorous competition among vendors in the marketplace.

(AR Tab 77 at 5310.)

10. Record documents not shared with GAO confirm that DoD knew the solicited "Iaas/PaaS offerings are not static and will be updated overtime [sic] both in terms of available services and applicable pricing." (AR Tab 130 at 8721.) Indeed, DoD crafted a special technology refreshment clause under which the awardee will continually add new services to the contract—the prices of which the awardee and DoD will set when incorporating the future service onto the contract. (AR Tab 35 at 740-41.) Gartner estimates that major cloud providers release 40 to 50 new cloud services in any given month.[10]

11. By Count II, the CO separately violated statutory and regulatory directives (applicable to all IDIQ contract competitions, regardless of size) to favor a multiple award IDIQ acquisition strategy to the "maximum extent practicable." *See* 10 U.S.C. § 2304a(d)(4); 48 C.F.R. § 16.504(c)(1)(i); *WinStar Commc'ns, Inc. v. United States*, 41 Fed. Cl. 748, 759 (1998)

[10] Chris Pemberton, *Hidden Cloud Opportunities for Technology Service Providers*, Gartner (June 20, 2018), https://www.gartner.com/smarterwithgartner/7-hidden-cloud-growth-opportunities-for-technology-service-providers/ (last visited 4/26/19).

[redacted]

(holding agency failed to comply with "maximum extent practicable" requirement). Congress' "maximum extent practicable" direction is not an empty decree. *Cf. Palantir USG, Inc. v. United States*, 904 F.3d 980, 992-93 (Fed. Cir. 2018) (affirming Army undermined different "maximum extent practicable" commercial item preference).

12. Here, accepting the CO's one-sided "maximum extent practicable" analysis requires a suspension of disbelief. With respect to the purported negatives of competition, a concoction of *ipse dixit* assertions and unsupported inputs yields implausible conclusions such as multiple awards will "result[] in 282,240 days (or 770 years worth of time collectively) of delaying warfighters from getting access to foundational cloud computing and storage resources." (AR Tab 24 at 460.) The analysis also relies on an inflated assertion that task order competition will add $505 million in administrative costs, apparently hoping that the eye-popping output will dissuade a discriminating review of the unsourced inputs. (*Id.*)

13. But, even with the CO's inflated numbers, the scales would have tipped in favor of competition had the CO considered the benefits of multiple awards as FAR 16.504(c) requires: "Each of these [FAR 16.504(c)(1)] criteria plainly requires consideration of the benefits of multiple awards." *WinStar*, 41 Fed. Cl. at 758 (overturning each of three invoked single award reasons). Indeed, OMB has observed that multiple award IDIQ technology contracting can both reduce costs (by 16% for one agency, $1.6 billion here) **and** improve quality. (AR Tab 77 at 5309-12.) DoD Guidelines, likewise, identify seven different benefits of competition. (*Id.* at 5361-62.) Yet, the CO here neither quantifies nor weighs any benefits of task order competition. Moreover, the consistent, continuing use by the military branches and

[redacted]

the intelligence community of multi-cloud approaches belie the CO's claims. In fact, even the Central Intelligence Agency (cited by DoD) has announced its intent to go multi-cloud.[11]

14. By Count III, Oracle challenges the arbitrary Subfactor 1.1, Elastic Usage, as applied by DoD to achieve its stated goal of reducing competition. This subfactor requires each offeror to demonstrate that the DoD-provided, estimated JEDI usage metrics (network, compute, and storage) in the RFP are less than 50% of the offeror's Commercial Cloud Offering usage for the months of January-February 2018, i.e., nine months before the proposal deadline and seventeen months before the anticipated award date. (AR Tab 35 at 791.) The metrics DoD selected are massive. Indeed, these January-February 2018 metrics are so large that DoD asserts that Oracle (one of the largest cloud providers in the world) fails against them. But the measurement period selected for these outsized metrics (well prior to even proposal submission) is not related to any legitimate need and unduly restricts competition. DoD has conceded that the capacity needs measured by the Subfactor 1.1 metrics will not arise until after contract award. (AR Tab 42 at 5749:5-9.) Had DoD measured the commercial cloud network, compute, and storage metrics at the time of proposal submission (October 2018) or actual need (no earlier than mid-2019), Oracle would have amply exceeded the arbitrary criteria.

15. The U.S. Code and FAR severely restrict an agency's use of qualification requirements. Indeed, 10 U.S.C. § 2319 requires DoD to take numerous steps prior to using such a qualification requirement—none of which DoD has undertaken here. *W.G. Yates & Sons Constr. Co. Inc. v. Caldera*, 192 F.3d 987 (Fed. Cir. 1999) (declaring qualification requirement that bidder have "manufactured ten door systems which were operating satisfactorily for at least

[11] Jason Miller, *Is the CIA's new cloud procurement a signal to DoD to update JEDI?*, Federal News Network (Apr. 8, 2019), https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/04/is-the-cias-new-cloud-procurement-a-signal-to-dod-to-update-jedi/ (last visited 4/26/19).

[redacted]

five years prior to the date of award" invalid where agency failed to comply with the statutory requirements for such a provision).

16. To the extent that the United States contends this gate criterion is a procurement specification (not a qualification requirement), it remains unlawful because a performance specification by statutory definition may not exceed the agency's minimum needs. Subfactor 1.1 does not measure which offerors can meet DoD's needs during performance. It measures historic usage at least seventeen months before DoD will even issue its first JEDI task order and nine months before proposal submission. *Am. Safety Council, Inc. v. United States*, 122 Fed. Cl. 426, 435 (2015) (finding solicitation clauses unduly restrictive and unrelated to a legitimate need); *USA Jet Airlines, Inc., Active Aero Grp., Inc.*, B-404666, Apr. 1, 2011, 2011 CPD ¶ 91 (agency may not require an offeror to demonstrate the ability to meet a requirement earlier than agency needs).

17. Although Oracle's Count III challenge does not depend on Ubhi's involvement or DoD's intent in setting these metrics, the record makes both clear:

> Let me put the metrics [we select] 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 solve the problem.

(AR Tab 47c at 3123 (Woods and Ubhi discussing JEDI metrics).) DoD published its draft RFP containing each of the gate criteria in March 2018 and devised the metrics in late 2017 with Ubhi's (heavily conflicted) involvement.

18. By Count IV, and to the extent that the Court does not strike Subfactor 1.1 as improper, Oracle challenges its exclusion from the competitive range based solely on an unacceptable Subfactor 1.1 rating. [redacted]. Moreover, Oracle's Subfactor 1.1 submission purportedly confused DoD, and Oracle

[redacted]

thus would have benefited from discussions and an opportunity to revise its proposal such as the two [redacted] competitive range offerors will now receive. The Agency has provided no reasoned basis for excluding Oracle relative to the two [redacted] offerors included in the competitive range.

19. By Count V, Oracle challenges, as unduly restrictive of competition, Subfactor 1.2 and its mandate that each offeror have, at the time of proposal submission, three existing, physical data centers separated by at least 150 miles, each supporting Federal Risk and Authorization Management Program ("FedRAMP") Moderate Authorized offerings.[12] DoD admits that the JEDI contract does not require FedRAMP authorization at all—much less at the time of proposal submission: "[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...." (AR Tab 78 at 5495:5-14.) The offeror need not even propose the data centers and offerings used to clear the gate. (AR Tab 40 at 853 (Q233).) Instead, DoD structured this gate to limit the competitive field. As noted in Count III, Congress has strict rules limiting the use of such qualification requirements. 10 U.S.C. § 2319; *W.G. Yates*, 192 F.3d at 992-93 (declaring qualification requirement invalid). DoD, however, did not even attempt to follow these basic statutory requirements. Equally problematic, DoD's demand that the offerors meet this requirement at the time of proposal submission both exceeds DoD's minimum needs (it is not using FedRAMP for performance at all) and violates FedRAMP policy: "Federal agencies cannot require [Cloud Service Providers ("CSPs")] 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."

[12] DoD declared IBM, another substantial commercial and government cloud provider, ineligible against this gate. DoD did not evaluate Oracle against this gate.

[redacted]

FedRAMP Tips & Cues Compilation 2015-2017 (Jan. 2018) at 7, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Tips_and_Cues.pdf.

20. Still further, DoD necessarily knew or should have known that only two offerors could satisfy this requirement at the time of proposal submission. Yet, DoD took no steps to comply with 10 § U.S.C. 2304(c)(1) and FAR 6.302-1 which apply where DoD asserts only a limited number of qualified sources can meet DoD's needs.

21. By Count VI, Oracle challenges Subfactor 1.6 as improper. Subfactor 1.6 requires each offeror to demonstrate an online marketplace of third-party platform and software offerings, which JEDI Cloud users can purchase and quickly provision. But DoD lacks authority to procure such a marketplace. Congress only recently gave the General Services Administration ("GSA") permission to test such an approach and required inclusion of multiple contractors. Just months ago, this Court declared a similar vendor-overseen marketplace sought by the Department of Veterans Affairs a violation of the Competition In Contracting Act ("CICA"). *Electra-Med Corp. v. United States*, 140 Fed. Cl. 94, 104 (2018).

22. By Count VII, Oracle challenges the DoD-Ubhi-AWS created conflicts that have severely tainted JEDI.[13] Despite conflict-of-interest laws and DoD requirements, DoD never screened Ubhi (certainly not properly) and never obtained a signed non-disclosure agreement from Ubhi prior to involving him in JEDI.[14] Although the record still remains incomplete, the Agency's reopened investigation caused a string of AWS and Ubhi admissions, which establish that DoD never should have involved Ubhi in JEDI.

[13] Oracle separately treats the unfair competitive advantage that arose when AWS subsequently employed Ubhi and the other former DoD officials.
[14] DoD suggests that it orally screened Ubhi and he lied about his ongoing relations with AWS.

[redacted]

23. Ubhi worked at AWS before joining DDS in summer 2016, and he returned to AWS as a General Manager in November 2017. (AR Tab 77 at 5254-55; AR Tab 33 at 686.) Moreover, the record is now clear that across much of his time at DDS Ubhi engaged in active, undisclosed re-employment discussions with AWS. Indeed, during JEDI, AWS made significant, undisclosed job and bonus offers to Ubhi.

24. While at DDS, Ubhi served as "lead [Product Manager] on the [JEDI] effort," (AR Tab 47a at 2793) one of four people within DDS "leading the cloud acquisition for DoD." (*Id.* at 2813.) No dispute exists that Ubhi participated personally and substantially in JEDI while successfully securing re-employment with AWS. Indeed, Ubhi worked on JEDI for weeks after accepting AWS' verbal employment offer. Ubhi then created an elaborate lie about a recent Amazon offer for Tablehero when he belatedly recused himself, seemingly to avoid scrutiny by DoD into Ubhi's employment discussions with AWS and Ubhi's actions on JEDI.

25. Procuring agencies must "avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-contractor relationships." 48 C.F.R. § 3.101-1. The record, however, evidences a systemic DoD failure. Indeed, DoD acknowledges that Ubhi violated FAR 3.101-1 and may have violated 18 U.S.C. § 208 and other regulations, but still contends Ubhi did not impact the procurement despite a disturbing record that evidences Ubhi, after verbally accepting an AWS employment offer: (i) zealously advocated a single source JEDI award approach favored by no competitor but AWS; (ii) downloaded the entire JEDI Google drive to his laptop; (iii) participated in the DDS effort to set the gate metrics at levels so high that DoD would "get to one"; (iv) met with DoD cloud users regarding their needs; (v) denigrated DoD and industry personnel who favored multiple awards or non-AWS

[redacted]

approaches; and (vi) set up and conducted "highly technical" discussions with potential JEDI competitors regarding their JEDI capabilities.

26. Faced with this record, the CO underpins much of her no-impact finding with the proposition that: "Ubhi did not have the technical expertise to substantially influence the JEDI Cloud requirements" and also could not understand the technical information he accessed. (*Id.* at 24 (¶ 90).) Both the CO and a DDS Deputy Director, however, testified repeatedly to Ubhi's technical expertise before GAO in this very matter: "Right, again, Deap is a technical expert. That's why he was hired on to the DDS team." (AR Tab 78 at 5445:6-8.) The CO herself testified that: "[T]he technical expert that was pegged to support this -- support aspects of this was Deap Ubhi." (*Id.* at 5571:18-20.) Such contradictions in DDS' position betray the goal of the no-impact analysis.

27. Similarly, DDS seemingly spends more time trying to disprove the proprietary nature of the offeror-provided and marked "Proprietary and Confidential" JEDI information that Ubhi accessed and downloaded than DDS does trying to figure out what Ubhi did with all of the proprietary information he took. For instance, DDS challenges whether Microsoft properly marked information submitted and accessed by Ubhi: "While the [Microsoft] information is marked proprietary, in my opinion that is because it has Microsoft product names on it...." (Ubhi Mem., Appx. 3 at 7 (¶ 3.A).) Presumably, if DoD sought a correct answer about the proprietary nature of the marked Microsoft JEDI White Paper, then DoD would have asked Microsoft (and the other companies whose marked JEDI information Ubhi accessed). DoD did not, preferring to offer opinions such as the "architecture diagrams" provided by Microsoft "are at a high enough level that it could be easily argued that this is the model that any cloud provider would use...." (*Id.*)

[redacted]

28. By Count VIII, Oracle challenges the conflict of interest associated with DoD permitting the JEDI participation of [redacted] a former [redacted] of the Navy involved with JEDI and hired by AWS. What limited information DoD has provided about this further impropriety is incomplete and inaccurate in some respects. Even the facts offered by AWS and relied on by the CO establish that AWS and [redacted] began employment discussions in the late summer of 2017 and continued the discussions throughout JEDI. Like Ubhi, [redacted] continued participating on JEDI even after accepting an employment offer from AWS. For instance, in [redacted] final JEDI meeting, held three days after [redacted] accepted an offer to serve as a principal in AWS' [redacted] division, [redacted] participated in and received access to the DoD source selection sensitive draft Acquisition Strategy.

29. Like Ubhi, [redacted] declaration submitted to DoD contains misstatements. And, as with Ubhi, AWS did not timely set up an ethical wall or notify DoD when AWS purportedly set up the firewall for monitoring purposes. DoD concedes that [redacted] "violated FAR 3.101-1, and possibly 18 U.S.C. § 208 and its implementing regulations." ([redacted] Mem. at 4.) DoD also concedes that [redacted] had access to JEDI source selection information. (*Id.*) DoD, however, asserts no harm came of [redacted] misconduct due to AWS' untimely email firewalls and self-serving affidavits. Both this Court and GAO, however, have rejected untimely firewalls, self-monitoring and offeror affidavits as a resolution to such issues. *See NetStar-1 Gov't Consulting, Inc. v. United States*, 101 Fed. Cl. 511, 528 (2011) (recognizing after-the-fact mitigation efforts are ineffective and inadequate where they allocate to the contractor the task of policing and mitigating its own potential conflicts); *L-3 Servs., Inc.*, B-400134.11, B-400134.12, Sept. 3, 2009, 2009 CPD ¶ 171 (agency unreasonably relied on after-the-fact mitigation).

[redacted]

30. By Count IX, Oracle challenges the CO's perfunctory review of Anthony DeMartino's JEDI involvement. Despite awareness of the severe flaws in the CO's prior determination, the CO took no further review steps regarding DeMartino during the stay period. The Agency, accordingly and inexplicably, rests on its earlier less than one page, error ridden analysis. (AR Tab 33 at 685.) At relevant times, DeMartino, a high-level political appointee, served as the chief of staff for the Deputy Secretary of Defense ("DSD")—the Pentagon official who initiated and led JEDI.[15] Given that DeMartino's work prior to entering the government involved consulting for AWS, DoD SOCO specifically directed DeMartino in April 2017 not to participate in any matters related to AWS without prior approval and, later in April 2018, directed DeMartino's immediate recusal from JEDI when SOCO untimely learned that DeMartino disregarded the earlier guidance. DoD's attempt to reclassify the DSD's Chief of Staff as a mere "note taker" lacks record support; the record demonstrates that DeMartino oversaw and impacted JEDI from the policy level to specific details.

31. The CO did not reasonably investigate and resolve the DeMartino conflict allegations. The CO did not consider (or know about) SOCO's pre-JEDI guidance to DeMartino. (AR Tab 78 at 5669:13-5670:13.) The CO did not interview DeMartino, review his documents, or even attend many of the JEDI meetings DeMartino held. (*Id.* at 5686:11-14, 5695:2-9; AR Tab 75 at 5239 (¶ 33).)

32. By Count X, Oracle challenges the CO's determination that AWS has adequately mitigated the unfair competitive advantage associated with AWS' knowing decision to hire (at least) two DoD JEDI personnel. "[W]here a firm may have gained an unfair competitive advantage through its hiring of a former government official, the firm can be disqualified from a

[15] DoD admits that DSD Shanahan (whose authority DeMartino implemented) had "personal and substantial" involvement in the procurement. (AR Tab 64 at 4862.)

[redacted]

competition based upon the appearance of impropriety which is created by this situation, even if no actual impropriety can be shown...." *Int'l Res. Grp.,* B-409346.2 *et al.*, Dec. 11, 2014, 2014 CPD ¶ 369 (sustaining protest involving "former [agency] director); *see also NFK Eng'g, Inc. v. United States*, 805 F.2d 372, 377 (Fed. Cir. 1986) (commending agency for disqualifying a bidder that hired a former government employee). Indeed, the law provides that such conflicts entitle the other offerors to a presumption that the hiring entity has misused the information known to the former procurement official. *See, e.g.*, *NetStar-1*, 101 Fed. Cl. at 528; *Int'l Res. Grp.,* B-409346.2 *et al.*, Dec. 11, 2014, 2014 CPD ¶ 369.

33. Far from presuming that the various AWS hirings have harmed the competition, the CO accepts that Ubhi (who violated FAR 3.101-1 and made numerous misstatements to DoD according the CO's own findings and apparently remains under investigation) informally firewalled himself, that AWS nearly six months later formalized the firewall with others at AWS by email. The CO also accepts that Ubhi (now caught in numerous mistruths regarding JEDI) did not share any "non-public" JEDI information with the JEDI proposal team, relying on post-hoc AWS declarations. To borrow from the late Judge Allegra:

> Can it be that the drafters of the FAR dedicated a whole subpart's worth of guidance to how and when to identify such conflicts, as well as how and when to mitigate the conflicts so identified, yet subscribed to the notion that the failure to follow these procedures could be cured by having the awardee swear up and down it did nothing improper? Of course not.

NetStar-1, 101 Fed. Cl. at 529.

34. The CO likewise treats AWS as somehow blame-free despite its heavy hand in the misconduct. For instance, AWS necessarily knew both that AWS had entered employment discussions with Ubhi and that Ubhi was serving as the JEDI lead product manager. Yet, AWS did not advise DoD of the employment discussions or even require Ubhi to provide an ethics

[redacted]

letter to support Ubhi's simultaneous participation in employment discussions with AWS while serving as the JEDI lead product manager. Instead, AWS purportedly relied on Ubhi's statement that he had no restrictions on his conduct notwithstanding that AWS necessarily knew that to be false. 48 C.F.R. § 3.104-8(b) ("An offeror who engages in employment discussion with an official subject to the restrictions of 3.104-3, knowing that the official has not complied with 3.1403(c)(1) is subject to the criminal, civil, or administrative penalties set forth in 41 U.S.C. 2105.")

35. Equally problematic are AWS' informal, contradictory ethical wall assertions. On the one hand, AWS asserts that Ubhi advised AWS (as part of the hiring process) that Ubhi had no ethical restrictions per DoD. Yet, AWS asserts that when Ubhi arrived, Ubhi set up an informal, undocumented ethical wall (an ethical wall that even Ubhi's AWS manager cannot recall). Thus, AWS purportedly believed that Ubhi faced no restrictions relative to his JEDI work, but AWS nonetheless enforced the restrictions of which AWS purportedly did not know. AWS' conduct (like Ubhi's) merits rebuke, not reward.

II. PARTIES

36. Oracle, a leading technology provider, delivers enterprise cloud computing services globally. http://www.oracle.com/us/corporate/oracle-fact-sheet-079219.pdf (last visited 4/26/19). More than 500 government organizations use the leading edge technology, flexibility, and cost savings provided by the Oracle Cloud. https://www.oracle.com/industries/public-sector/index.html (last visited 4/26/19).

37. The DoD Washington Headquarters Services provides administrative support services to the Secretary of Defense and various DoD agencies. http://www.whs.mil/our-organization (last visited 4/26/19).

[redacted]

38. AWS is a JEDI competitor that engaged in employment discussions and hired several former government personnel participating in JEDI during the procurement.

III. JURISDICTION AND VENUE

39. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1491(b).

40. Venue is proper in this Court pursuant to 28 U.S.C. § 1491(b).

IV. STANDING

41. Oracle is an interested party with standing to bring this protest. *See* 28 U.S.C. § 1491(b)(1). Oracle timely protested the matters set forth herein and submitted a responsive proposal. Oracle also expects to compete under any revised RFP the Agency issues.

42. Oracle has a direct economic interest because the alleged violations of law and arbitrary actions cause Oracle "non-trivial competitive injury," which the Court can redress. *Weeks Marine, Inc. v. United States*, 575 F.3d 1352, 1362-63 (Fed. Cir. 2009).

43. The single award decision, unduly restrictive RFP terms, exclusion of Oracle from the competitive range, and conflicts of interest all undermine Oracle's ability to compete fairly under the RFP, an injury this Court can remedy by declaring the challenged provisions and conduct improper and enjoining DoD from making award until the Agency amends the RFP and adequately investigates the conflicts and mitigates the harm to the procurement. *See Palantir Techs. Inc. v. United States*, 129 Fed. Cl. 21, 30-38 (2016) (protester had standing to raise pre-award protest).

V. TIMELINESS

44. Oracle timely filed its protest challenging the solicitation terms and conflicts of interest at GAO prior to the proposal submission deadline. *See Blue & Gold Fleet, L.P. v. United States*, 492 F.3d 1308, 1313 (Fed. Cir. 2007); 4 C.F.R. § 21.2(a)(1). The proposal submission

[redacted]

deadline lapsed during Oracle's pre-award protest at GAO, and Oracle submitted a timely proposal.

45. Oracle timely filed its protest at this Court following the GAO decision. *DGR Assocs., Inc. v. United States*, 94 Fed. Cl. 189, 202-03 (2010).

46. Oracle also timely files this supplemental complaint. (Dkt. 66.)

VI. FACTUAL ALLEGATIONS

A. The Genesis Of DoD's JEDI Cloud Initiative And Conflicted Participants

47. DoD's IT environment is "highly decentralized with thousands of networks and data centers and more than 500 cloud efforts." (AR Tab 25 at 471.) DoD "spends approximately $45 billion per year on IT." (*Id.*)

48. In August 2017, the Secretary of Defense and members of the Defense Innovation Board visited AWS' Seattle, Washington facility "to understand cloud market capability." (AR Tab 33 at 686.)

49. In September 2017, the Deputy Secretary of Defense established a Cloud Executive Steering Group ("CESG"), chaired by the Honorable Ellen Lord, to "devise and oversee the execution of a strategy to accelerate the adoption of cloud architectures and cloud services, focusing on commercial services." (AR Tab 91 at 5955.) Phase I of that initiative included a tailored acquisition process (JEDI) to acquire a modern enterprise cloud services solution that can support unclassified, secret, and top secret information. (*Id.* at 5956.)

50. Ubhi, a former AWS employee (who was actively seeking to return to AWS throughout his time at DDS), served on the four-person DDS team leading the JEDI effort as the "lead PM [Product Manager] for the effort." (AR Tab 47a at 2793.) To help structure the requirements, Ubhi led communications with industry and other DoD entities. (*See* AR Tab 34

[redacted]

at 708 (Ubhi was "running point on all [JEDI] industry touch points"); AR Tab 78 at 5436:11-5437:3; *id.* at 5463:12-5464:11.)

51. Ubhi met with numerous potential JEDI competitors regarding their capabilities and approaches—including Microsoft, Google, and others. (AR Tab 47a at 2787 (Microsoft thanking Ubhi for "our meeting a couple of weeks ago at the Pentagon"); *id.* at 2900 (regarding JEDI meeting and warning Google to "expect our conversation tomorrow to be highly technical").)

52. These one-on-one meetings with potential vendors were "highly technical." (AR Tab 78 at 5463:12-5464:11 (Ubhi "coordinat[ed] those conversations" which "were highly technical").) The meetings involved questions to each of the vendors about their capabilities, including:

> 1. What does your hardware architecture look like with regard to cloud services?
>
> 2. [*If they don't provide hardware solution*] How does your company interact with a deployed cloud solution? Where does it hook in and how?
>
> 3. Talk to us about your approach to information security, specifically with regard to minimizing attack vectors and then identifying, mitigating, and containing issues.
>
> 4. How does account provisioning or service initiation work with your solution? What parts of this are automated versus requiring administrator interaction? And what about service termination?
>
> 5. How would you handle an installation at the edge of connectivity, including service initiation and eventual syncing?
>
> 6. Talk to us about moving data and services across network boundaries, both as it applies to peering internally and across physical networks.
>
> 7. What are the general service level expectations of your solution? When there is an outage, what is the process for both communication and getting back up? What is the process for updating both software and hardware? We're interested in both software and hardware issues and solutions.
>
> 8. What is your biggest weakness, and how are you working to improve in that area?

(AR Tab 20 at 388-89.)

[redacted]

53. Ubhi also held source selection sensitive meetings with various DoD stakeholders to learn about their cloud-related needs, such as the Air Force (AR Tab 47a at 2806) and the Navy (*see id.* at 2829), including SPAWAR (*see* AR Tab 47b at 3065-75; AR Tab 47c at 3172-73 (regarding an internal meeting with SPAWAR), and the Marine Corps. (AR Tab 47c at 3114-15; AR Tab 78 at 5436:11-5437:3 (noting that CESG "collect[ed] information [on] the Department's current usage of cloud services.... Deap was having those conversations").)

54. Based on these meetings, in the fall of 2017, DDS (with input from Ubhi) submitted a "cloud brief" to the Joint Requirements Oversight Council ("JROC") which specified DoD's cloud needs and provided guidance on the cloud transition. (AR Tab 17 at 321, 323-24; AR Tab 51 at 4369.)

55. On or about October 30, 2017, DDS (with input from Ubhi) issued a Request for Information ("RFI") to industry seeking input on the JEDI Cloud acquisition. (AR Tab 20 at 368; 391-94.) DDS received sixty-four discrete RFI responses. (AR Tab 23 at 437.)

56. In or about March 2018, DoD prepared a report summarizing findings based on the RFI responses received. (AR Tab 20.) According to the report, "multiple sources are capable of satisfying DoD's requirements for JEDI Cloud." (*Id.* at 366.)

57. Many respondents noted, however, that the FedRAMP accreditation process "extremely limited" the commercial offerings available to DoD. (*Id.* at 373-74.)

58. Additionally, "the majority of industry recommend[ed] multiple awards in order to prevent cost prohibitive vendor lock-in (i.e. it becomes too costly to move data out of the single award contractor cloud), and enables DoD to use different providers to meet specific requirements." (*Id.* at 386.)

[redacted]

B. From The Outset, DoD Pursued A Single Award.

59. On September 14, 2017, the day after the DSD initiated JEDI, the CESG expressed its commitment to a single award approach and an intention to withhold that decision from the public to delay scrutiny. (*See* AR Tab 86 at 5928 (CESG meeting minutes withheld from GAO showing CESG sought to "[a]void specifying that there is a single vendor," because doing so "will create perception issues with vendors already in use.").)[16]

60. The CESG's October 5, 2017 meeting minutes reiterate the single award approach: "Single cloud solution necessary for this enterprise initiative to be successful and allow DoD to achieve its mission objectives with cloud adoption." (AR Tab 88 at 5934; *see also* AR Tab 51 at 4325 (October 27, 2017 update to DSD: "the CESG acquisition strategy is focusing on a single award.").)

61. On November 6, 2017, DoD confirmed publicly the chosen "Acquisition Strategy" of a "Single-award [IDIQ] contract...." (AR Tab 92 at 5957.)

62. On July 17, 2018, nearly ten months after the first CESG meeting adopting the single award approach, the CO signed a memorandum setting forth three purported justifications for adopting this acquisition strategy. (AR Tab 24.)

63. The CO's one-sided analysis reflects the singular purpose: to support DoD's foregone single award conclusion. The CO ignored the benefits of task order competition and failed to give the maximum practicable preference to multiple awards. Each finding is inaccurate, unsubstantiated, or both. For instance, relying on a flawed calculation, the CO concludes that a single award approach will save the government half a billion dollars in

[16] DoD withheld much of the record from GAO, including the documents at AR Tabs 86-186.

[redacted]

administrative costs and prevent "770 years worth of time ... of delaying warfighters." (*Id.* at 460.)

64. Two days later, on July 19, 2018, the Under Secretary of Defense for Acquisition and Sustainment signed a D&F declaring JEDI exempt from the statutory prohibition against large, single-award IDIQ contracts. (AR Tab 16.) The D&F rests on a single conclusion, i.e., the JEDI contract will provide 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." (*Id.* at 318.)

C. The Solicitation

65. DoD issued the original RFP on July 26, 2018, and amended it on four occasions during the pendency of Oracle's pre-award GAO protest. (*See* AR Tabs 1, 26, 35, 48, 52.)

66. The RFP indicates DOD's intent to conduct the procurement under the streamlined commercial item provisions of FAR 12.6. (*Id.* at 718.)

67. The RFP provides for DoD to award the JEDI Cloud IDIQ contract, with a potential ten year performance period, to a single, best value offeror (*id.* at 782, 805), and sets the maximum contract limit at $10 billion and the minimum order guarantee at $1 million. (*Id.* at 730.)

68. The RFP utilizes a two-phase evaluation. (AR Tab 35 at 805.) In Phase One, the RFP directs DoD to evaluate offerors against several "Acceptable/Unacceptable" Gate Criteria, discussed in detail below. (*See id.*) In Phase Two, the RFP requires DoD to evaluate each offeror's proposed technical solutions. (*Id.* at 805-06.)

69. The RFP lists the non-price evaluation factors in descending order of importance:

Factor 2 – Logical Isolation and Secure Data Transfer
Factor 3 – Tactical Edge

[redacted]

Factor 4 – Information Security and Access Controls
Factor 5 – Applications and Data Hosting and Portability
Factor 8 – Demonstration
Factor 6 – Management and TO 001
Factor 7 – Small Business Approach

(*Id.* at 805.) These factors, when combined, are more important than Factor 9—Price. (*Id.*)

70. In Phase Two, step 1, the RFP contemplates DoD establishing a competitive range of not more than four offerors. (*Id.* at 782, 805.)

1. The RFP Scope of Work and Pricing Provisions

71. The Statement of Objectives ("SOO") evidences an expansive scope for the JEDI Cloud contract. The contractor will provide IaaS and PaaS offerings, in both unclassified and classified environments, to support DoD business and mission operations from the homeland to the tactical edge, including disconnect and austere environments, and closed loop networks. (AR Tab 27 at 608.) The RFP defines the tactical edge to include "[e]nvironments covering the full range of military operations...." (AR Tab 29 at 652.)

72. Users will include DoD entities and others performing "DoD business and mission operations," including the U.S. Coast Guard, the Intelligence Community, allies, and Federal contractors. (AR Tab 27 at 608.)

73. As related to cyber security, the CSP must meet: (i) the Cyber Security Plan security requirements for the unclassified services within 30 days of contract award; (ii) the Secret-level security requirements within 180 days of contract award; and (iii) the security requirements for all other classified services including Top Secret, SCI, and SAP within 270 days of contract award. (*Id.* at 610; AR Tab 115 at 6789 (RFP Cover Letter stating: "[t]here is no requirement for offerors to have accredited classified environments at the time of proposal.").)

[redacted]

74. Contrary to what one might assume based on the Gate Criteria, the Cyber Security Plan does not require the awardee to have data centers or offerings authorized through FedRAMP. (AR Tab 78 at 5495:5-14 ("[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"); *id.* at 5496:3-6 ("Q: So if I understand correctly, your cybersecurity plan does not require FedRAMP authorization. A: Correct.").

75. Instead, DoD will assess the awardee's Cloud offering against the JEDI Cloud security requirements by a review and assessment of CDRL 11, the Security Authorization Package. (AR Tab 78 at 5496:7-5498:15; *see also* AR Tab 5 at 159.) The RFP does not require the awardee to submit its CDRL 11Security Authorization Package to DoD until 30 days after contract award, and DoD does not commit to a timeframe for the assessment. (AR Tab 5 at 159; AR Tab 78 at 5497:2-5498:15.)

76. The RFP anticipates that the contractor continually will add new or improved IaaS, PaaS, or Cloud Support services to the contract by (i) advising the CO of new services that the vendor has made publicly available in the vendor's CONUS commercial cloud, or (ii) notifying the CO of potential new services in advance of availability in the vendor's CONUS commercial cloud. (AR Tab 35 at 740.) Pursuant to RFP Section H2, the price of any new unclassified services shall not be higher than the price that is publicly available in the commercial cloud plus any applicable discounts, premiums, or fees the CSP proposed in RFP Attachment J-3. (*Id.*) If offered in advance of availability into the commercial marketplace, the CO will make a commerciality determination about the new service and may require cost and pricing data or other than cost and pricing data as required by FAR 15.4. (*Id.*)

[redacted]

77. The pre-submission offeror questions to DoD contemplate "multiple catalog [change] submissions on a daily or weekly basis as new services are released" post award. (*See, e.g.*, AR Tab 32 at 660 (Q17).) In fact, the offeror questions anticipate changes to the proposed services and prices even during the evaluation period. (*Id.* at 668 (Q86 and Q87).) Gartner notes that major cloud providers may release 40 to 50 new features in any given month.[17]

78. For new classified services, RFP Section H2 provides that the "price incorporated into the JEDI Cloud catalog ... may include a price premium compared to the unclassified services because of the additional security requirements." (AR Tab 35 at 740-41.) That premium, per Section H2, will be the lesser of the premium applicable to the most comparable classified service at the time of contract award, the classified price premium offered by the CSP in its proposal for Section H2, or the premium proposed by the CSP at the time it offers the new service to DoD. (*Id.* at 741.)

79. Each offeror must submit four catalogs, one each for: CLIN x001 Unclassified IaaS and PaaS Offerings; CLIN x002 Classified IaaS and PaaS Offerings; CLIN x003 Unclassified Cloud Support Package; and CLIN x004 Classified Cloud Support Package. (*Id.* at 801.) Each catalog may contain "hundreds if not thousands of items." (AR Tab 70 at 5002 (¶ 51).) DoD will not, however, evaluate the price catalogs except to confirm the accuracy of any prices used in the Price Scenario build-ups. (AR Tab 35 at 811-12.)

2. DoD Structured The Challenged Gate Criteria To Restrict Competition.

80. DoD structured the RFP to restrict competition:

The JEDI program schedule could be negatively impacted if source selection

[17] Chris Pemberton, *Hidden Cloud Opportunities for Technology Service Providers*, Gartner (June 20, 2018), https://www.gartner.com/smarterwithgartner/7-hidden-cloud-growth-opportunities-for-technology-service-providers/ (last visited 4/26/19).

[redacted]

> 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.

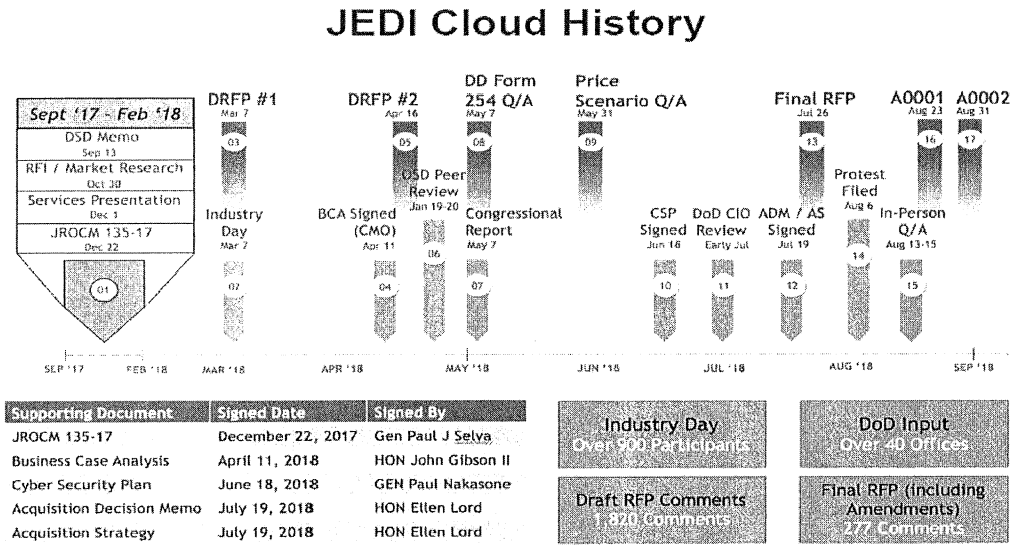
(AR Tab 21 at 422; AR Tab 25 at 504; AR Tab 78 5473:2-11; AR Tab 35 at 805.)

81. The DDS team leading the acquisition, including Ubhi, set the metrics and capabilities required by the gate criteria to "get to one" contractor. (*See* AR Tab 47c at 3123 ("So if multiple cloud providers can meet the metrics, then we won't get to one.").)

82. Consequently, if an offeror receives an Unacceptable rating under any gate, the RFP provides that "the remainder of the proposal will not be evaluated and will not be considered for award." (AR Tab 35 at 805.)

83. The gate criteria served their improper purpose. DoD's market research noted the existence of a robust commercial cloud services market. (AR Tab 20 at 366.)

84. When first announced, JEDI sparked intense interest in the contracting community: hundreds of companies attended the industry day, and more than sixty companies submitted detailed RFI responses identifying extensive, sometimes unique capabilities:



[redacted]

(AR Tab 70 at 4986-87, 5022.) But following the issuance of the final RFP and its restrictive gate criteria, only four companies attended DoD's in-person question and answer ("Q&A") sessions and ultimately submitted proposals. (*See* AR Tabs 120-123.)

85. Three of the four offerors expressed concerns during the Q&A session regarding the restrictive nature of the gate criteria and the considerable effort and resources necessary to pass the gates and compete. (*See id.*)

86. Two of the four offerors (Oracle and IBM) ultimately filed protests challenging the restrictive specifications,[18] and a third offeror (Microsoft) publicly criticized the restrictive gates.[19] Other major CSPs, e.g., Google, chose not to compete based, in part, on the RFP's restrictive terms: "We determined that there were portions of the contract that were out of scope with our current government certifications."[20]

87. Of the seven gates, three are relevant to Oracle's protest challenge.

88. First, Subfactor 1.1 requires the offeror to demonstrate that the estimated JEDI Cloud metrics for Network, Compute, and Storage are less than 50% of the Commercial Cloud Offerings usage during the months of January-February 2018. (AR Tab 35 at 791.)

89. DDS claims these metrics ensure the JEDI contractor will have surge capacity for unexpected future events and continue to invest in innovation during contract performance. (AR Tab 42 at 944-46.) But Subfactor 1.1, as written, measures the offeror's historic usage (as of

---

[18] Sam Gordy, *JEDI: Why We're Protesting*, IBM (Oct. 10, 2018), https://www.ibm.com/blogs/policy/jedi-protest/ (explaining that "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.") (last visited 4/26/19).

[19] Billy Mitchell, *DOD defends its decision to move to commercial cloud with a single award*, FedScoop (Mar. 8, 2018), https://www.fedscoop.com/dod-pentagon-jedi-cloud-contract-single-award/ (last visited 4/26/19).

[20] Naomi Nix, *Google Drops Out of Pentagon's $10 Billion Cloud Competition*, Bloomberg (Oct. 8, 2018), https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition (last visited 4/26/19).

[redacted]

January and February 2018) long before proposal submission and nearly seventeen months before DoD will award the contract let alone issue a task order. (AR Tab 35 at 791.)

90. Second, Subfactor 1.2 mandates that each offeror have, at the time of proposal submission, no fewer than (i) three physically existing data centers, (ii) within the customs territory of the United States, (iii) that are 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 that are FedRAMP Moderate 'Authorized' by the Joint Authorization Board (JAB) or a Federal agency as demonstrated by official FedRAMP documentation." (AR Tab 35 at 792; AR Tab 32 at 661 (responses to Q26 and Q27); AR Tab 42 at 946-47; AR Tab 78 at 5488:22-5489:21.)

91. DoD first required FedRAMP authorized services in all three data centers in the July 26, 2018 final RFP. (*Compare* AR Tab 105 at 6241 (requiring "FedRAMP Moderate compliant") *with* AR Tab 35 at 792.) DoD thus gave interested providers less than two months to obtain FedRAMP authorization, a process that takes at least six months to complete.[21]

92. "FedRAMP Authorized" is a designation that the CSP's systems have completed the FedRAMP authorization process.[22] Two acceptable paths of authorization exist: a JAB provisional authorization or an initial agency authorization.[23]

93. FedRAMP prohibits federal agencies from requiring authorization as a prerequisite for bidding on a federal cloud services solicitation. (AR Tab 77 at 5292.)

---

[21] *Compare* AR Tab 1 at 67 (requiring proposals by September 17, 2018) *with FedRAMP Accelerated A Case Study for Change Within Government*, at https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf (noting FedRAMP efforts to reduce authorization timeline to six months) (last visited 4/26/19).
[22] https://www.fedramp.gov/faqs/ (last visited 4/26/19).
[23] https://www.fedramp.gov/agency-authorization/ (last visited 4/26/19).

[redacted]

94. The security requirements in the RFP's Cyber Security Plan, i.e., the contract requirements, do not require FedRAMP authorization. (AR Tab 78 at 5495:1-8.)

95. Third, Subfactor 1.6 requires demonstration at the time of proposal submission that the offeror has an online marketplace of third-party platform and software offerings that JEDI Cloud users can access to purchase and provision software. (*Id.* at 793-94.) DoD has yet to (and cannot) identify any legal authority permitting it to set up this online marketplace.

D. DoD Neither Implemented Procedures To Promote The Public Trust In JEDI Nor Properly Investigated And Resolved Conflicts.

96. DoD deviated from its procurement policy and did not require personnel participating in JEDI to complete a conflict-of-interest form. DoD Source Selection Procedures at 11, 36 (effective May 1, 2016) (citing FAR 3.104 and 5 C.F.R. § 2635) ("To confirm statutory and regulatory compliance, ensure all persons receiving source selection information sign a Non-Disclosure Agreement 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.").[24]

97. Consequently, DoD failed to screen the JEDI officials for potential conflicts of interest prior to JEDI involvement, and wrongly permitted individuals with AWS ties to participate personally and substantially in the acquisition contrary to law.

98. On July 23, 2018, three days before posting the final RFP, the CO issued a memorandum for the record indicating that "there were four instances where individuals with potential financial conflicts of interest under 18 U.S.C. § 208 or impartiality restrictions under 5

[24] https://www.dau.mil/guidebooks/Shared%20Documents/Source%20Selection%20Guide.pdf. DoD has cited a short Slack exchange for the proposition that DOD properly vetted Ubhi. (Dkt. 40 at 30.) But that exchange is not a screening at all and fails to explore numerous topics the law requires of a proper screening. 5 C.F.R. §§ 2635.402, 403, 502, 503, 604, 606.

[redacted]

C.F.R. § 2635.502 were provided with access to procurement sensitive information." (AR Tab 33 at 683.) The CO observed that each "individual had either a financial interest in or a covered relationship with Amazon, Inc./Amazon Web Services (AWS)…." (*Id.*)

1. Deap Ubhi

99. Ubhi temporarily left AWS to serve as a "Product Director" at DDS in August 2016. (AR Tab 77 at 5254; AR Tab 33 at 686.) DDS hand-picked Ubhi to the four person team leading the JEDI acquisition. (AR Tab 47a at 2813.) Absent from the record is a conflict-of-interest questionnaire or any signed non-disclosure agreement for Ubhi.

100. DoD's only purported vetting is a Slack exchange on September 25, 2017, in which DoD counsel informs Ubhi that industry will "want to give 'capabilities briefings' to DDS about cloud," and asks who should serve as the point of contact. (AR Tab 47b at 3049.) Ubhi responds "[m]ake it me please," and follows-up with "[u]nless you think my past in AWS biases me." (*Id.*) Counsel responds back—without asking any questions about whether he still has ties to or financial interests in AWS—"No. You have no conflict anymore." (*Id.*)

101. DoD has acknowledged that Ubhi participated personally and substantially in JEDI. (*Compare* AR Tab 33 at 686-87 *with* AR Tab 64 at 4860, 4862.)

102. Ubhi also managed untold amounts of nonpublic and acquisition sensitive JEDI-related information based on his access to the acquisition's Google drive, which housed all acquisition-related documents. (AR Tab 78 at 5533:8-16.) Ubhi had "administrative privileges" to manage the drive and others access to the information on it. (*Id.*; *see also*, *e.g.*, AR Tab 47a at 2910; AR Tab 47b at 2984 (describing an "INTERNAL DDS folder for things on this [DoD Cloud] topic we don't want to share … [with a less exclusive group]."); *id.* at 3015-17, 3025.)

[redacted]

103. Ubhi's access to the Google drive also provided him access to JEDI Cloud information shared with the CESG by the offices of the DoD Chief Information Officer ("CIO") and the Under Secretary, which "agreed to data dump everything into Google Folder and use Slack." (*See* AR Tab 47b at 2986.)

104. The CO's July 23, 2018 no-impact determination dedicated less than one page to the Ubhi conflicts. (AR Tab 33 at 686-87.)

105. Had the CO performed a reasonable investigation in July 2018, the CO would have learned prior to the RFP's release that Ubhi lied extensively about his relationship with AWS and that AWS had engaged in undisclosed employment discussions with Ubhi throughout Ubhi's JEDI involvement.

106. On or about October 12, 2018, the CO received AWS' proposal, including its conflict of interest response, which contained an October 8, 2018 affidavit signed by Ubhi.

107. On December 7, 2018, the CO apparently sent an email to AWS asking the following five "yes" or "no" questions of Ubhi:

- Do you recall being asked to sign a JEDI Cloud specific non-disclosure agreement (NDA)?
- Do you believe you signed a JEDI Cloud specific NDA?
- If you believe you signed a JEDI Cloud specific NDA, do you consider these terms still binding?
- At any point during your employment negotiations with AWS were you asked to provide nonpublic information and/or documentation about the JEDI Cloud or DoD's cloud service needs?
- Prior to your employment with AWS, excluding the market research you conducted on behalf of the DoD, did anyone from AWS ask you for nonpublic information and/or documentation about the JEDI Cloud requirement?

(AWS OCI Mem. at 2-3 (¶ 7.B).)

[redacted]

108. AWS submitted an affidavit from Ubhi to the CO in response to the CO's questions on December 14, 2018. (*Id.* at 3 (¶ 7.B).) Ubhi apparently "stipulate[d] that he participated in the planning phase that preceded the JEDI Cloud acquisition," rather than acknowledging that he was a member of the four person DDS team leading the acquisition efforts. (*Id.*) Ubhi also stated that he did not remember signing an NDA, yet purportedly understood that he "was (and remain[s]) prohibited from disclosing non-public information relating to JEDI Cloud gained while employed by DDS." (*Id.*)

109. The public GAO decision, issued in November 2018, put AWS on notice that Ubhi's recusal notice to DoD falsely claimed that AWS had expressed an interest in purchasing his start-up in late October 2017 and that the CO found Ubhi's recusal "prompt" based on the statements therein. *Oracle Am. Inc.*, B-416657, *et al.*, Nov. 14, 2018, 2018 CPD ¶ 391.

110. Oracle filed the redacted version of its original Court of Federal Claims bid protest complaint on December 10, 2018, further detailing the CO's conclusion regarding Ubhi's conflict from the Amazon-Ubhi Tablehero discussions. (Dkt. 13 at 42-44, 83-91, n.21.)

111. But AWS did not alert the CO to the fact that Ubhi's recusal letter was inaccurate in its December 14, 2018 response to the CO's questions.

112. Instead, AWS intervened in this action and submitted filings asserting that Ubhi had "acted specifically to avoid any potential conflict by voluntarily recusing himself" and that DoD had "immediately revoked" Ubhi's JEDI access (Dkt. 41 at 31), despite that AWS knew such assertions to be false.

113. AWS then waited until February 12, 2019, to "clarify one point with respect to Mr. Ubhi's recusal," specifically that Ubhi's purported basis for recusal was false, yet claimed

[redacted]

that this "clarification does not alter, and indeed provides additional support for, [the CO's] conclusion that there is no conflict." (Dkt. 60-1 at 5.)

114. The belated AWS letter revealed to the CO that Ubhi lied about his dealings with AWS to DDS. In the February 12, 2019 letter, AWS advised that Ubhi and Amazon Restaurants and Amazon.com, Inc. ended discussions about partnering with Ubhi's start-up company Tablehero in December 2016, and claimed that AWS did not know why Ubhi's October 2017 recusal letter stated otherwise. (*Id.* at 5-6.)

115. In the February 2019 letter, AWS also advised the CO for the first time that Ubhi (i) had discussions with his former AWS supervisor about returning to AWS in September 2017, (ii) formally applied for an open position on October 17, 2017 and indicated to AWS in that application that he conferred with his governmental ethics officer and was permitted to engage with employment discussions with AWS. (*Id.* at 6.) AWS does not explain how it could have reasonably believed that Ubhi was permitted to engage in employment discussions with AWS when AWS also knew that Ubhi was participating personally and substantially on JEDI. Notably, the CO did not notice or resolve this glaring inconsistency.

116. Also notable is what is absent from the AWS February 2019 letter. AWS failed to disclose to the CO at this time that Ubhi had in fact been engaged in employment discussions with AWS since February 2017. (Ubhi Mem. at 15-16 (¶ 65); *id.* at 10-11 (¶¶ 39-42).) AWS also did not disclose that on August 23, 2017, Ubhi emailed [redacted] (Ubhi's [redacted] at AWS) indicating that Ubhi would consider the offer to "craft my own role" to rejoin AWS. (*Id.* at 11 (¶ 42).) Neither Ubhi nor AWS contemporarily raised these employment discussions with DDS.

[redacted]

117. Instead, on September 22, 2017, while Ubhi was serving as the lead PM for JEDI, [redacted] and Ubhi discussed by phone Ubhi rejoining AWS. (*Id.* at 15 (¶ 65.ii.b).) [redacted] followed up by email on September 29, 2017. (*Id.* (¶ 65.ii.d).) On October 4, 2017, Ubhi verbally committed to return to AWS. (*Id.*)

118. AWS' February 12, 2019 letter instead advised the CO that AWS made a formal employment offer to Ubhi on October 25, 2017, Ubhi accepted the offer on October 27, 2017, and on November 27, 2017 Ubhi rejoined AWS as a Senior Manager, Startup Program Management, AWS Business Development. (Dkt. 60-1 at 6.)

119. Based on AWS' February 12, 2019 letter, the CO re-opened her investigation to reconsider her no-impact determination with regard to Ubhi. (*Id.* at 2.)

120. The CO reassessed the no-impact determination and issued a new no-impact determination on or about April 9, 2019. (Ubhi Mem. at *passim*.)

121. The April 9, 2019 determination reveals that the CO conducted in-person or phone interviews with seven DDS personnel and the DoD SOCO counsel to (1) ascertain whether anyone at DDS knew the information in the CO's prior July 2018 memorandum was inaccurate, (2) "determine if the new information concerning Mr. Ubhi's AWS employment would lead anyone to adjust their opinion about whether Mr. Ubhi attempted to influence critical decisions," and (3) obtain other previously unknown information. (Ubhi Mem. at 11 (¶ 45).)

122. The CO did not interview Ubhi or anyone from AWS.

123. Instead, the CO requested and received the following from AWS (i) a copy of Ubhi's Oct. 17, 2017 application, (ii) Ubhi's job offer, (iii) Ubhi's signing bonus, (iv) confirmation that, in September and October 2017, Ubhi did not have ongoing bonus or options

[redacted]

from his previous AWS employment; and (v) a Government Entity Questions Form that Ubhi apparently completed with his application. (*Id.* at 9-10 (¶¶ 34, 35).)

124. In the Government Entity Questions Form, Ubhi falsely represented that (i) he had "consult[ed] with [his] employer's ethics officer that he was permitted to have to employment discussions with AWS," and (ii) to the best of his knowledge he did not have any employment restrictions "from handling any specific types of matters if employed by Amazon or its subsidiaries." (*Compare id.* at 10 (¶ 35) *with id.* at 12 (¶ 49) (Ubhi did not speak with DDS or DoD SOCO counsel prior to engaging in employment discussions with AWS).)

125. The CO also relies on an affidavit from the AWS [redacted] Recruiter, who averred that during an October 24, 2017 call with Ubhi, Ubhi purportedly contradicted his Government Entity Questions Form submitted a week earlier and advised the recruiter that he had to recuse himself from working on a DoD program and could not work with the AWS public sector team. (*Id.* at 16 (¶ 65.ii.h).) Although Ubhi allegedly told the recruiter he could not perform work related to the "program" he worked on at DoD, the recruiter averred that she never "asked for any detail, about the program that he was working on for DoD." (AWS OCI Mem. at 4.) Despite that FAR 3.104-8(b) required AWS to follow up with DoD, the CO never asked AWS to explain the discrepancy between Ubhi's no-restriction averment on the employment questionnaire and the recruiter's affidavit, including why AWS would proceed to hire someone that had made false statements on his Government Entity Question Form, or why AWS failed to follow up with DoD given Ubhi's conflicting statements.

126. The CO also did not ask what the recruiter did (if anything) to implement the restrictions Ubhi purportedly raised in late October 2017. Instead, the CO found that the "[b]est business practice would have been for [redacted] [the recruiter] to forward the information

[redacted]

about Mr. Ubhi's preclusion to attorneys working with the AWS WWPS [AWS Public Sector group] to ensure this preclusion was known to both AWS's Commercial organization and AWS WWPS." (AWS OCI Mem. at 3-4.) Although AWS did not follow this best practice or notify DoD, the CO nevertheless deemed AWS' procedures "effective to maintain the integrity of the procurement process." (*Id.*) The CO does not explain the rationale for such a conclusion.

127. The CO also relies on an affidavit from the AWS JEDI [redacted], who averred that, on May 11, 2018 (more than five months after Ubhi arrived), AWS instituted an email firewall between Ubhi and the JEDI proposal team. The CO did not investigate what precipitated the email or why it took months to institute a firewall. Instead, the CO mischaracterized AWS as "proactive[]." (Ubhi Mem. at 6 (¶ 27).)

128. The CO did not investigate or seek confirmation from each member of the JEDI proposal team, nor confirm that the proposal team had not indirectly received nonpublic information from Ubhi. Instead, the CO relies on Ubhi's statement that he did not share any JEDI information with anyone at AWS. (*Id.*) Such reliance is inconsistent with the CO's other statements that, "[i]n light of Mr. Ubhi's other misrepresentations," the CO did not give much "weight or credibility to the statements Mr. Ubhi provided in his declarations." (AWS OCI Mem. at 2.)

129. In another glaring inconsistency, although Ubhi's manager averred that he never had any conversations with Ubhi about his work at DoD, the CO credited Ubhi's affidavit statements that Ubhi "informally firewalled himself by duly notifying his manager that he should not be involved in JEDI Cloud activities because of potential conflict issues." (*Compare* AWS OCI Mem. at 3 *with* Ubhi Mem. at 7 (¶ 29).)

[redacted]

130. Despite the flawed affidavits and belated and untimely firewall efforts, the CO determined that Ubhi's employment with AWS does not create an OCI. The CO stated:

> I assessed the information firewall plan and procedure in place for Mr. Ubhi, as documented in OCI Mitigation Plan, to be reasonable and effective to maintain the integrity of the procurement process. I assessed the information about the informal firewall for Mr. Ubhi, as documented in the supplemental materials from AWS, to be effective to maintain the integrity of the procurement process.
>
> Based on the OCI Mitigation Plan, two Mr. Ubhi Affidavits, AWS responses [to the CO's specific leading questions], [redacted] Affidavit, [redacted] affidavit, and [redacted] affidavit; I find that AWS did not receive any nonpublic information or documentation JEDI Cloud-related, including potential competitors, from Mr. Ubhi.

(AWS OCI Mem. at 4-5 (¶¶ 7.C-8.)

131. With regard to Ubhi's personal conflicts of interest, the CO determined that Ubhi violated FAR 3.101-1 by (i) "seeking employment with a potential offeror while being personally and substantially involved in the JEDI Cloud effort" and (ii) "actions to conceal seeking employment and accepting a position...." (Ubhi Mem. at 14 (¶ 62).) The CO stated:

> Mr. Ubhi should not have continued participation in JEDI Cloud activities, including attending any market research meetings, after he began employment discussions with AWS.
>
> I am very disappointed by Mr. Ubhi's deception and delay in disqualifying himself from the JEDI Cloud activities. Given the critical importance of the JEDI Cloud to the warfighter, Mr. Ubhi's knowledge of his ethical obligations, and the importance of maintaining the integrity of this already complex acquisition, it is likewise disconcerting for me to know that Mr. Ubhi's misrepresentation of the facts and the need for me to reopen my investigation has caused others to question the quality and integrity of the JEDI Cloud acquisition, in general.

(*Id.* (¶¶ 60-61).)

132. The CO, finding that the facts warrant further investigation concerning whether Ubhi violated 18 U.S.C. § 208, and the implementing regulations including 5 C.F.R. §§ 2635.402, 2635.604, has referred the matter to the DoD IG. (*Id.* at 14 (¶ 63).) The CO

[redacted]

nevertheless determined that Ubhi's "unethical behavior has no impact on the pending award or selection of a contractor in the JEDI procurement." (*Id.*)

2. Anthony DeMartino

133. DeMartino served as a consultant for AWS through January 2017, when he became Deputy Chief of Staff for the Office of the Secretary of Defense. (AR Tab 75 at 5231-32 (¶ 9).) In March 2017, DeMartino transitioned to serve as the DSD's Chief of Staff. (*Id.*) DeMartino reportedly declared income from AWS through August 2017—the same month in which Secretary Mattis visited AWS to learn about AWS' cloud service capabilities

134. Due to his financial ties with AWS, DeMartino received an ethics letter from DoD's SOCO in April 2017 warning DeMartino not to work on matters involving AWS. (AR Tab 51 at 4345.)

135. DeMartino ignored SOCO's written direction, electing to participate in JEDI from its inception. (AR Tab 75 at 5233 (¶ 13).)

136. As the Chief of Staff for the organization driving DoD's cloud strategy, DeMartino participated in JEDI from a policy level all the way down to specific details regarding the acquisition. DeMartino obtained and edited JEDI briefings on behalf of the Secretary of Defense and DSD, directed JEDI activities, and participated in JEDI strategy meetings that discussed the Acquisition Strategy, Security Strategy, Business Case, and the propriety of a single versus multiple award approach. (AR Tab 51 at 4351-53, 4366-68, 4390; AR Tab 47a at 2926; AR Tab 78 at 5676:21-5677:18; *id.* at 5541:3-20; AR Tab 47e at 3310, 3315-16.)

137. DeMartino also directed efforts and strategized as to the most likely way to garner approval for the single source approach. (AR Tab 51 at 4366-67.)

[redacted]

138. Additionally, DeMartino provided input regarding the JEDI industry day briefing and coordinated and provided input into the JEDI press strategy. (*Id.* at 4402, 4404; AR Tab 47f at 3831, 3880; AR Tab 47e at 3319.)

139. In April 2018, after DoD received press Freedom of Information Act ("FOIA") requests raising concerns about his involvement, DeMartino apparently asked SOCO about his JEDI involvement, and SOCO instructed DeMartino to recuse himself immediately. (*Id.*)

140. In late July 2018, based on an analysis that spans less than one page, the CO concluded that "DeMartino's involvement did not negatively impact the integrity of the JEDI Cloud acquisition" based on the assumption that his role was "ministerial," and that "he did not participate personally and substantially in the procurement":

> Facts:
>
> 1. It was brought to the Contracting Officer's attention that Mr. DeMartino previously provided consulting services to AWS while employed with SDB Advisors. Mr. DeMartino ended his SDB Advisors employment in January 2017.
>
> 2. Mr. DeMartino worked as a Chief of Staff/Deputy Chief of Staff for the Deputy Secretary and Secretary, respectively. In this capacity, he scheduled and attended meetings relative to the JEDI Cloud procurement, which did include access to pre-decisional documents concerning JEDI Cloud procurement acquisition strategy and other matters during the Fall and Winter of 2017. Mr. DeMartino recorded meeting minutes and had no 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.
>
> 3. Mr. DeMartino worked with SOCO throughout his DoD employment to ensure compliance with all applicable ethics rules.
>
> Conclusion: Mr. DeMartino's involvement was ministerial and perfunctory in nature and he provided no input into the JEDI Cloud acquisition documents and 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.

[redacted]

(AR Tab 33 at 685.) The CO's findings related to DeMartino are directly contrary to her recent conclusion that another government official's attendance at an April 2018 meeting concerning the draft Acquisition Strategy "may have constituted personal and substantial participation." ([redacted] Mem. at 4 (¶ 22).)

141. The CO did not interview DeMartino, review his emails, or assess his work product. (AR Tab 78 at 5686:11-14; AR Tab 75 at 5239 (¶ 33 ("there are relatively few documents that I considered in my investigation").) Instead, the CO "largely relied on conversations that [she] had with the DDS legal counsel who provided advice in concert with SOCO." (AR Tab 78 at 5695:2-9.) At GAO, the CO testified that she could not remember when, or exactly how, DeMartino's conflict came to her attention. (*Id.* at 5668:16-5669:5.)

142. The CO had not even seen SOCO's prior ethics warning to DeMartino prior to completing her determination. (*Id.* at 5669:11-5670:13.) The CO did not confer with SOCO (*id.* at 5675:4-8) or even consider the materials that SOCO reviewed (if any) when SOCO directed DeMartino in April 2018 to immediately recuse himself (*id.* at 5674:1-5675:3).

143. The CO did not revisit and supplement the perfunctory July 2018 review when the CO reopened her integrity investigation in February 2019.

3. [redacted]

144. Upon receipt of AWS' proposal, the CO learned of another AWS conflict of interest issue involving [redacted] the former [redacted] of the Navy for [redacted] [redacted]. (AWS OCI Mem. at 5 (¶ 9).) In this role, [redacted] served as the principal Navy advisor for the acquisition of [redacted]

[redacted]

[redacted].[25] In that capacity, [redacted] participated in JEDI.

145. The CO did not interview [redacted] review any conflict-of-interest disclosures he made to AWS, or determine the scope of his DoD activities. Rather, the CO based her no-impact determination on AWS' OCI Mitigation plan and affidavits by AWS employees [redacted], [redacted] [redacted], and [redacted]. ([redacted] Mem. at *passim*.)

146. In the summer of 2017, [redacted] apparently consulted with Navy ethics counsel about retirement and engaging with defense contractors about future employment. ([redacted] Mem. at 3 (¶ 11).) The substance of those conversations is unknown because the CO did not consult with [redacted] or the Navy ethics counsel, or review any documentation related thereto.

147. According to AWS, from August 2017 to early 2018, [redacted] engaged with an AWS recruiter, [redacted], and [redacted] about his retirement and post-government plans. (*Id.* (¶ 12).) The CO's determination does not detail the substance of these material communications either.

148. Based on an affidavit from [redacted] submitted with AWS' proposal, the CO found that [redacted] attended an October 5, 2017 CESG to discuss the Navy's experience with cloud services. ([redacted] Mem. at 3 (¶ 10).)

149. The CO, based on personal knowledge, also knew that [redacted] attended a JEDI Cloud meeting held on April 5, 2018 to discuss, among other things, the draft Acquisition Strategy, because the CO also attended the meeting. (*Id.* (¶ 16).) The CO did not explore why

25 [redacted].

[redacted]

[redacted] failed to disclose this meeting in his affidavit or investigate whether [redacted] was involved in any other JEDI-related activities.

150. On January 11, 2018, months after his discussions with the recruiter and [redacted] and prior to attending the April JEDI Cloud meeting, [redacted] submitted a "Request for Disqualification from Duties" to the Navy. (*Id.* (¶ 13).) It is unclear whether the CO reviewed or obtained the disqualification request as part of her no-impact determination.

151. On January 15, 2018, [redacted] interviewed with AWS, he received a job offer from AWS on March 29, 2018, and accepted the offer on April 2, 2018. (*Id.* (¶ 14).) Thus, three days after accepting the AWS job, and despite his prior recusal, [redacted] attended the April 5, 2018 JEDI Cloud meeting to discuss the draft Acquisition Strategy. (*Id.* (¶ 16).) No one that the CO interviewed knew of [redacted] disqualification. (*Id.* (¶19).) It is unclear whom the CO interviewed in this regard, as her [redacted] determination does not identify any interview subjects.

152. [redacted] retired from the Navy on June 1, 2018 and joined AWS 17 days later as [redacted] (*Id.* (¶ 15).)

153. The CO's determination states "other than the October 2017 and April 2018 meetings, Mr. [redacted] <u>is not known by me</u> to be affiliated in any way with the JEDI Cloud acquisition." (*Id.* (¶ 20).) The determination contains no evidence that the CO reviewed all relevant information to make a reasoned conclusion about [redacted] involvement.

154. The CO concluded that [redacted] attendance at the October 2017 CESG meeting "did not constitute personal and substantial participation in the JEDI Cloud procurement," finding that his attendance was "for the purposes of providing information on the Navy's experience with cloud services," and stating that such activities are not "personal and substantial participation." (*Id.* (¶ 21).)

[redacted]

155. With regard to the April 5, 2018 meeting, the CO found that [redacted] attendance may have constituted personal and substantial participation and may have violated 18 U.S.C. § 208 because [redacted] had previously accepted a job with AWS. (*Id.* at 4 (¶ 22).) The CO nevertheless concluded that [redacted] participation does not "have any significance to the acquisition" "because his participation was in advance of the issuance of the RFP, final decisions made to key acquisition documents, and receipt of any proposals, nor was the multiple award approach advocated by Mr. [redacted] adopted." (*Id.* (¶¶ 22, 23).)

156. The CO acknowledged that the acquisition strategy discussed at the April 2018 meeting constituted source selection sensitive, nonpublic JEDI Cloud information with competitive value. (*Id.* (¶¶ 24-25).) But, based on AWS affidavits received on March 21, 2019 from [redacted], [redacted], and [redacted] and AWS' OCI's Mitigation Plan, the CO concluded that [redacted] did not provide any nonpublic information to AWS. (*Id.* (¶ 26.b); *see also* AWS OCI Mem. at 5-6 (¶ 9).)

4. [redacted]

157. Upon review of AWS' proposal, the CO learned that AWS hired another DDS official in September 2017 who has not been walled off from AWS' proposal efforts.

158. [redacted] served at DDS from April 2016 through September 1, 2017, prior to joining AWS as a [redacted] in late September 2017. Based on his LinkedIn profile, during his stint at DDS, [redacted] served as the [redacted] and [redacted]

[redacted]

[redacted][26]

159. On December 18, 2018, the CO sent an email to AWS requesting that [redacted] submit a signed affidavit addressing the following three questions: (i) what was [redacted] start date at AWS?; (ii) "[A]t any time during [redacted] employment negotiations with AWS," was [redacted] "asked to provide nonpublic information and/or documentation about the JEDI Cloud or DoD's cloud service needs?"; and (iii) "Prior to [redacted] employment with AWS, did anyone from AWS ask [redacted] for nonpublic information and/or documentation about the JEDI Cloud requirement?" (AWS OCI Mem. at 6-7 (¶10).)

160. Based on his affidavit, the CO found that "[redacted] did not have any nonpublic information or documentation related to the JEDI Cloud, and therefore it is reasonable that AWS did not firewall [redacted]." (*Id.* at 7 (¶ 10).)

161. The CO did not investigate the work [redacted] performed while at DDS and whether that work provided [redacted] competitively useful, nonpublic information relevant to JEDI (e.g., information about DoD's cloud service needs or about AWS' cloud competitors), nor did the CO investigate [redacted] work and activities at AWS.

5. [redacted]

162. On February 26, 2019, [redacted] of the Cybersecurity and Defense Branch, Cyberspace Division, Joint Chiefs of Staff ("JCS"), contacted the CO to advise that [redacted] also was negotiating employment with AWS. (AWS OCI Mem. at 7 (¶ 11).)

---

[26] [redacted].

[redacted]

163. For JEDI, [redacted] at the direction of the JCS Vice Chief, "led the development of the cloud characteristics/requirements for the JEDI Cloud based on the needs of the Combatant Commands, warfighter." (*Id.*)

164. [redacted] also supported the JROC approval process "by directly addressing cloud concerns from each of the JROC members and adjusting the JROCM [the JROC Memorandum] based on feedback from the JROC." (*Id.*)

165. After the JROC signed the memorandum on December 22, 2017, [redacted] provided bi-weekly updates to the VCJCS regarding the status of the JEDI Cloud and other cloud efforts until April 2018. (*Id.*)

166. [redacted] also participated in and provided recommendations to the Cloud Cybersecurity Working Group for shaping cybersecurity requirements along with providing the DoD Dictionary to baseline termination. (*Id.* at 8 (¶ 11).)

167. [redacted] applied for five different positions with AWS on July 4, 2018, one position on December 31, 2018, and one on January 23, 2019. (*Id.*)

168. AWS apparently first contacted [redacted] on January 9, 2019. (*Id.*)

169. As of February 26, 2019, [redacted] had been through four interviews with AWS with a final interview set for February 27, 2019. (*Id.* at 7 (¶ 11).) During the interviews, [redacted] apparently discussed "her level of understanding and creation of cloud requirements for her current customers, the warfighter." (*Id.*)

170. On March 11, 2019, AWS offered [redacted] an [redacted] position on AWS' [redacted] Team, which [redacted] accepted that same day. (*Id.* at 8 (¶ 11).)

171. The CO found that "other than drafts of the JROCM and knowledge about initial conversations at the Cloud Cybersecurity Working Group that [redacted] attended, [redacted]

[redacted]

[redacted] did not have access to any nonpublic information or documentation related to the JEDI Cloud." (*Id.*) This finding contradicts earlier statements in the CO's determination describing [redacted] role providing bi-weekly updates to the VCJCS regarding the status of the JEDI Cloud and other cloud efforts. (*Id.* at 7 (¶ 11).)

172. Based on affidavits provided by [redacted] and [redacted], the CO concluded that [redacted] prospective employment with AWS does not create an unfair competitive advantage.

E. Congressional Concern With The JEDI Cloud Procurement

173. Congress repeatedly has questioned DoD's JEDI Cloud strategy and requirements. In March 2018, after DoD expressed its intent to structure the RFP for a single IDIQ contract award at Industry Day, Congress directed DoD to submit two reports to the congressional defense committees, the first from the DSD on the JEDI RFP, and the second explaining the single award strategy, the parts of DoD that will use the contract, and the exit strategy. *See* Legislative Report accompanying Consolidated Appropriations Act of 2018, Pub. L. No. 115-141 (Mar. 23, 2018), https://docs.house.gov/billsthisweek/20180319/DIV%20C%20-%20DEFENSESOM%20FY18%20OMNI.OCR.pdf at 88-89 (last visited 4/26/19).

174. DoD submitted a Combined Report to Congress in May 2018 and published the report with the final RFP. (AR Tab 115 at 6773-87; *see also* AR Tab 109.)

175. The report observes that "DoD is best served by a robust, competitive and innovative technology base" (AR Tab 109 at 6497), but states that if DoD "pursued multiple-award contracts for the JEDI Cloud, each individual task order would be competed, thus being paced by DoD acquisition process…." (*Id.* at 6496-97.)

[redacted]

176. The report also states that the JEDI Cloud contract will be firm-fixed price and purportedly employ "pre-negotiated catalogs resulting from the full and open competition." (*Id.* at 6503.) DoD observed, however, that the "JEDI Cloud contract will require ongoing commercial parity of technical offerings so long as the evolving capabilities comply with Department security requirements." (*Id.* at 6504.) In other words, "the contract requires that the capabilities and prices delivered to DoD keep pace with commercial innovation." (*Id.*)

177. After receiving the Combined Report, Congress' concerns with JEDI did not dissipate. In the Department of Defense and Labor, Health and Human Services, and Education Appropriations Act, 2019 and Continuing Appropriations Act (the "Act"), passed in late September 2018, Congress imposed three additional obligations on DoD related to the JEDI Cloud contract: (i) DoD must have a detailed acquisition plan to sustain competition among CSPs under the JEDI Cloud contract; (ii) the Secretary of Defense must submit a report to Congress describing that acquisition strategy; and (iii) DoD must wait 90 days after submission of that report to obligate or spend any funds for migration of data to the JEDI Cloud contract. Pub. L. No. 115-245, § 8137 at 50-51 (Sept. 27, 2018).

178. Additionally, in late October 2018, two Congressmen wrote a letter to the DoD IG requesting an investigation into the RFP development and acquisition strategy, expressing concern about provisions that restrict competition, and questioning conflicts of interest by involved DoD personnel. *See* Congressional Letter to Acting Inspector General Fine, https://federalnewsnetwork.com/wp-content/uploads/2018/10/JEDI-IG-Letter-FINAL-10.22.18.pdf (last visited 4/26/19).

[redacted]

F. Oracle's Pre-Award Protest To GAO

179. Oracle filed its initial pre-award protest challenging the RFP on August 6, 2018, well before the RFP's original proposal submission deadline of September 17, 2018. (*See* AR Tab 54.) After multiple RFP amendments and a supplemental protest, Oracle filed a consolidated protest on September 6, 2018. (*See* AR Tab 67.)

180. Oracle's GAO protest timely raised several challenges to the RFP, including each of the RFP challenges addressed in this protest. (*See id.*; *see also* AR Tab 73.)

181. Following record production and briefing, GAO conducted a hearing on October 11, 2018 involving testimony from two DoD witnesses, the CO and DDS Deputy Director, that addressed only a subset of Oracle's protest grounds. (*See* AR Tab 74.)

182. GAO denied Oracle's protest in a decision made public on November 19, 2018. *See Oracle Am., Inc.*, B-416657 *et. al.*, Nov. 14, 2018, 2018 WL 6040648; (*see also* AR Tab 83). GAO did not address several of the arguments raised by Oracle, declared one argument premature, and erred as to the arguments it did address.

G. Oracle's Bid Protest Challenge In This Court And DOJ's Stay Request

183. On December 6, 2018, Oracle filed its initial Bid Protest Complaint (Dkt. 1), and on January 10, 2019, DOJ filed the Administrative Record with the Court. (Dkt. 39.)

184. On February 5, 2019, Oracle moved for Judgment on the Administrative Record. (Dkt. 56-1.)

185. On February 19, 2019, DOJ moved to stay the case while DoD reconsidered "whether possible conflicts of interest involving former DoD employee Deap Ubhi impacted the integrity of the procurement at issue, based upon new information provided [by AWS] to the contracting officer on February 12, 2019." (Dkt. 60 at 1.) DOJ noted that because the CO was

[redacted]

reconsidering her no-impact determination, it would be inefficient to continue briefing the other issues in the case because "Oracle's allegations of personal conflicts of interest by former DoD employees are related to its challenges to the terms of the solicitation." (*Id.* at 4.)

H. The CO's Conflict Reconsideration Decision And Competitive Range Determination

186. In early December 2018, the Technical Evaluation Board ("TEB") completed its evaluation of Oracle against Gate Criterion 1.1. Because the TEB found Oracle's proposal unacceptable under that subfactor, the TEB did not evaluate Oracle under any other criteria. (Oracle Factor 1 Consensus Document.)

187. In late February 2019, the Source Selection Authority ("SSA") issued a memorandum to the CO documenting the gate criteria evaluation for each of the four offerors. The evaluation results showed that Oracle and IBM each failed one of the challenged gate criteria and therefore the TEB did not evaluate their full proposals. (SSA Determination at 1.)

188. The TEB found AWS and Microsoft Acceptable under the gate criteria and evaluated their complete proposals. (*Id.*) [redacted] (SSA Concurrence Re: Competitive Range at 3.)

189. Despite that the TEB found [redacted], the CO recommended, on April 9, 2019, that the Agency proceed with a competitive range of only two offerors, AWS and Microsoft, and excluded Oracle and IBM from the competition. (CO Competitive Range Determination.) That same day, April 9, 2019, the SSA concurred with the CO's competitive range determination. (SSA Concurrence Re: Competitive Range.)

[redacted]

190. Apparently on the same day, April 9, 2019, the CO also completed her reassessment of the conflict of interests and determined that AWS had no conflicts requiring its exclusion and that the Ubhi and [redacted] misconduct did not impact the procurement.

I. Harm To Oracle, Public Interest, And Lack Of Harm To DoD

191. The balance of harms and public interest favor the injunctive relief Oracle seeks.

192. Absent injunctive relief, Oracle will suffer the irreparable harm of being deprived of the opportunity to compete fairly for a contract, *see, e.g., Palantir*, 129 Fed. Cl. at 291; *Magnum Opus Techs., Inv. v. United States*, 94 Fed. Cl. 512, 544 (2010), and Oracle will have to compete in a procurement that violates applicable laws and regulations. *Weeks Marine v. United States*, 575 F.3d 1352, 1361-62 (Fed. Cir. 2009); *WinStar*, 41 Fed. Cl. at 762-63 (holding protester prejudiced where agency improperly adopted a single-award approach).

193. The public interest also favors injunctive relief to remedy the procurement errors and violations of law identified herein and to restore public trust and confidence in the integrity of this procurement. *See e.g., Palantir*, 129 Fed. Cl. at 294-95 (citing BINL, Inc. v. U.S,, 106 Fed. Cl. 26, 49 (2012) ("With regard to the public interest, it is well-settled that there is a public interest in remedying violations of law.")); *see also e.g., Ian, Evan & Alexander Corp. v. United States*, 136 Fed. Cl. 390, 430 (2018) ("an injunction will promote the integrity of the procurement process by holding the government accountable when it takes actions that are contrary to law and may result in cost-savings for the government.")

194. The irreparable harm to Oracle and the public interest outweigh any harm DoD may claim as a result of delays to the procurement. Any alleged delay claimed by DoD is a self-inflicted injury based on the refusal to ensure that DoD conducted this significant procurement in accordance with the law, in a manner above approach, with complete impartiality, and with

[redacted]

preferential treatment for none. *See, e.g., Univ. Research Co., LLC v. United States*, 65 Fed. Cl. 500, 515 (2005) (granting preliminary injunction and recognizing that "the public's interest in the integrity of the procurement process outweighs the public's interest in the timely completion of the government procurement process").

COUNT I
The Agency's Single IDIQ Award Determination Violates The Law

195. Oracle incorporates paragraphs 1 through 194 of the Complaint by reference.

196. The Agency seeks to avoid Congress' prohibition on using a single source IDIQ award for this ten billion dollar, ten-year contract based on the Under Secretary's flawed determination that the JEDI Cloud contract will only involve "FFP task orders for services for which prices are established in the contract for the specific tasks to be performed." (AR Tab 16 at 319.) But the contract will require the awardee to regularly add new offerings to the contract at prices not yet determined and the RFP does not outline the specific tasks at all. DoD's attempt to circumvent Congress' plain prohibition necessarily fails as a matter of basic statutory interpretation.

197. This Court must set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" or "without observance of procedure required by law." 5 U.S.C. § 706(2)(A), (D).

198. This Court will grant relief for an offeror which demonstrates that the agency's procurement conduct violates applicable statutes or regulations. *See* 28 U.S.C. § 1491(b)(4); 5 U.S.C. § 706(2)(A), (D); *Banknote Corp. of Am., Inc. v. United States*, 365 F.3d 1345, 1351 (Fed. Cir. 2004); *Palantir*, 904 F.3d 980 (affirming Court decision sustaining protest for failure to follow U.S. Code commercial item provision).

[redacted]

199. For IDIQ contracts estimated to exceed $112 million, the law prohibits a single award unless the head of the contracting activity (or senior procurement executive for DoD procurements) determines in a written determination that one of four stated exceptions exists. *See* 10 U.S.C. § 2304a(d)(3); 48 C.F.R. § 16.504(c)(1)(ii)(D); 48 C.F.R. § 216.504(c)(1)(ii)(D). FAR 1.704, in turn, requires that "[e]ach D&F shall set forth enough facts and circumstances to clearly and convincingly justify the specific determination made" and to "detail the particular circumstances, facts, or reasoning essential to support the determination."

200. The U.S. Code identifies the following four single source prohibition exceptions:

> (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.

10 U.S.C. § 2304a(d)(3); *see* 48 C.F.R. § 16.504(c)(1)(ii)(D)(1)(ii).

201. "The requirement for a determination for a single-award contract greater than $112 million-(i) Is in addition to any applicable requirements of [FAR] Subpart 6.3...." 48 C.F.R. § 16.504(c)(1)(ii)(D)(3).

202. The statutory prohibition on large, single source IDIQ contracts reflects Congress' admonition (born of experience) that agencies maximize use of multiple award IDIQ contracts in order to achieve the benefits of task order level competition. Relevant legislative history

[redacted]

explains that the statutory prohibition ensures "that future contracts of this type provide for the competition of task and delivery orders unless there is a compelling reason not to do so." S. Rep. 110-77 at 368 (June 5, 2007).

203. The regulatory history to the FAR's implementing provisions notes the benefits of task order competition:

> The objective of this provision is to place greater emphasis on awarding multiple award contracts and enhancing the fair opportunity provisions within FAR Subpart 16.5. Competition of orders leads to improved contractor performance, stimulation of technological solutions, and reduction of costs over time. The tenets of this provision strike at the core of enhancing competition and ensuring competition continues to exist even after award of initial contract vehicles....

73 Fed. Reg. 54008, 54009 (Sept. 17, 2008).

204. Here, the Agency's single source D&F relies on one exception to the rule against awarding a single award IDIQ greater than $112 million. Specifically, the D&F claims that the JEDI contract purportedly will "provide[] only for [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), based on the mistaken belief that the cloud catalogs proposed will cover all services delivered across ten years. "The CLINS for cloud offerings (*i.e.*, IaaS, PaaS, and Cloud Support Package) will be priced by catalogs resulting from the full and open competition, thus enabling competitive forces to drive all aspects of the FFP pricing. All catalogs will be incorporated at contract award and cover the full potential 10 years." (*Id.* at 319.)

205. DoD misreported the same to Congress: "The JEDI Cloud contract will be FFP that uses pre-negotiated catalogs resulting from the ... competition." (AR Tab 109 at 6503.)

206. But the RFP and its technology refresh provisions neither identify the "specific tasks to be performed" nor call for prices on products that do not yet exist. Instead, in order to "keep[] pace with industry innovation and stay[] at the forefront of available technology" (AR

[redacted]

Tab 25 at 472), DoD structured the JEDI contract to include a customized technology refresh provision requiring the awardee to update continually the cloud services available on the contract as the awardee adds or removes services to its commercial cloud. (AR Tab 112 at 6673-74.) DoD's decision to apply this technology refresh approach prevents DoD from using the statutory exception that requires fixed prices for established services at the time of contract award.

207. As DoD's research reveals, 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." (AR Tab 137 at 9603.) To account for this dynamic nature, the RFP intentionally does not solicit fixed service catalogs or pricing.

208. In documents withheld from GAO, the record reveals that DoD issued an internal Justification and Approval ("J&A") for the contract's Section H2 technology refresh provision. (AR Tab 112 at 6673-74.) The J&A explains that DoD designed this "New Services" clause to ensure that the offerings made available on the JEDI contract "keep pace with advancements in industry," by requiring the contractor to update the catalogs consistently so that "as new commercial cloud services are available, the Contractor will provide these new services and apply and incorporate those services into the contract catalog." (*Id.* at 6674.)

209. When the Defense Procurement and Acquisition Policy office questioned the H clauses, the JEDI team explained that "the Iaas/PaaS offerings are not static and will be updated overtime [sic] both in terms of available services and applicable pricing." (AR Tab 130 at 8721.) Industry advised DoD that the H2 clause would result in "daily or weekly" updates to the service offerings and pricing. (*See* AR Tab 32 at 660 (Q17); *id.* at 668 (Q86-87).)

210. DoD cannot and has not solicited firm fixed prices for the future, undefined and unknown cloud services that the awardee will deploy on the contract. Contract clause H2 merely

[redacted]

attempts to peg the DoD's prices to future negotiation or to the awardee's future commercial market prices—an approach that the FAR does not countenance as a substitute for competition. 48 C.F.R. § 15.403-3(c) ("[t]he fact that a price is included in a catalog does not ... make it fair and reasonable," much less competitive).

211. Thus, the catalogs incorporated into the contract will not have established prices for all services to be performed over the ten-year period, rendering the cited exception inapplicable. The D&F's conclusion that 10 U.S.C. § 2304a(d) supports a single award IDIQ JEDI contract is wrong; the solicited contract does not meet the exception.

212. The Agency's improper D&F authorizing a single award under the JEDI Cloud RFP works competitive prejudice against Oracle. By limiting the number of awards available, the Agency deprived Oracle of the opportunity to compete for one of multiple JEDI Cloud awards, and all subsequent task order competitions. *Weeks Marine v. United States,* 575 F.3d 1352, 1361-62 (Fed. Cir. 2009); *WinStar*, 41 Fed. Cl. at 762-63 (holding protester was prejudiced where agency improperly adopted single-award IDIQ acquisition approach). Indeed, the use of multiple awards would also remove the justification for the competition prohibitive gates as DoD would not need to "get to one" company to fill DoD's substantial cloud computing needs. (AR Tab 47c at 3123.)

WHEREFORE, Oracle requests that the Court declare that the D&F violates 10 U.S.C. § 2304a(d)(3) and enjoin DoD from making a single award under the RFP absent compliance with 10 U.S.C. § 2304a(d)(3).

[redacted]

COUNT II
The CO's Conclusion That The FAR Requires DoD To Adopt A Single IDIQ Award Acquisition Approach For The JEDI Cloud RFP Lacks A Rational Basis

213. Oracle incorporates paragraphs 1 through 212 of the Complaint by reference.

214. Section 2304a of Title 10 of the U.S. Code and FAR 16.504(c) require the use of a multiple award IDIQ contracting approach "to the maximum extent practicable." 10 U.S.C § 2304a(d)(4). This is a separate and distinct statutory requirement from the requirement addressed in Count I. *See* Fed. Reg. Vol. 75, No. 52, 13416, 13419, 13420 (Mar. 29, 2010) (cmt. 10) (confirming distinct nature of requirements).

215. FAR 16.504(c)(1)(i) states that the contracting officer must (i) "give preference to making multiple awards" of an IDIQ contract under a single solicitation for the same or similar services to two or more sources to the "maximum extent practicable," and (ii) document the decision in the acquisition plan or acquisition file. 48 C.F.R. § 16.504(c)(1)(ii)(C).

216. The mandate that the contracting officer "must" favor multiple award IDIQ contracts "to the maximum extent practicable" is a material limit on contracting officer discretion. *See, e.g.*, *SMS Data Products Grp., Inc. v. United States*, 853 F.2d 1547, 1553-54 (Fed. Cir. 1988) (interpreting "shall," "to the maximum extent practicable" obtain competition when reprocuring following a default termination to mean that the contracting officer had to "conduct the reprocurement in the most competitive manner feasible."); *Palantir*, 129 Fed. Cl. at 269 ("The word 'maximum' in the phrase 'to the maximum extent practicable,' therefore, should not be ignored and read out of the statute.").

217. The challenged CO justification for a single award IDIQ acquisition approach must find support in the record and demonstrate that the CO rationally balanced Congress' strong preference for multiple awards to the maximum extent practicable by objectively assessing the

[redacted]

benefits and risks of both the multiple award and single award approaches. *See WinStar*, 41 Fed. Cl. at 764 (declaring contracting officer's determination regarding single award approach void as contrary to FAR 16.504(c)(1)). The CO's memorandum does neither.

218. As a matter procedure, the CO's memorandum post-dates DoD public statements regarding the single JEDI Cloud IDIQ contract approach by at least eight months. (*Compare* AR Tab 92 at 5957 (November 2017 stating chosen "Acquisition Strategy" of a "single-award [IDIQ] contract) *with* AR Tab 24 (CO July 2018 memorandum for the record).) The substantial timing incongruity raises questions about the actual bases for the CO's decision. *Citizens to Pres. Overton Park, Inc. v. Volpe*, 401 U.S. 402, 420 (1971) ("review is to be based on the full administrative record that was before the secretary at the time he made his decision."); *CRAssociates, Inc. v. United States*, 95 Fed. Cl. 357, 377 (2010) (an "essential premise of [Administrative Procedure Act ("APA")] review presupposes that the agency will establish its rationale at, or prior to, the time of its decision—not after.").

219. As a matter of substance, the CO cites three arguments for concluding that DoD must use a single award approach for JEDI: (i) based on the CO's knowledge of the market, more favorable terms and conditions, including pricing will result from a single award competition; (ii) the expected cost of administering multiple contracts outweighs the benefits of multiple awards; and (iii) multiple awards are not in the government's best interest. (AR Tab 24 at 457-64.)

220. The CO, however, never meaningfully considers the benefits of competition. The CO's failure to consider objectively the benefits of competition undermines each finding and prejudices Oracle. *WinStar*, 41 Fed. Cl. at 762 (holding contracting officer who made a single award IDIQ determination based on the same three maximum practical exceptions utilized here violated procurement law by focusing on difficulties and disregarding benefits).

[redacted]

221. Undoubtedly, significant benefits accrue to the government when it uses multiple award IDIQ contracts for technology. Indeed, Congress implemented the multiple award, maximum practicable preference to address just such contracts: "Use of multiple award contracts may be especially effective for maintaining better prices and quality in the IT market." (AR Tab 77 at 5310.) OMB has documented the competitive benefits achieved by numerous federal agencies through technology task order competition, noting that surveys revealed the costs after competition "averaged 16.7 percent less than the government's projected estimated costs." (*Id.* at 5310-11.) DoD Guidelines also recognize the many benefits of task order competition, including lower prices, innovation, better quality and performance, curbing fraud, and maintaining a strong defense industrial base—none of which the CO considers. (*Id.* at 5361-62.)

222. Moreover, in September 2018, Congress (aware of DoD's intended single award approach) mandated that DoD maintain cloud service provider competition under JEDI:

> None of the funds appropriated or otherwise made available … may be obligated or expended by the Department of Defense to migrate data and applications to the proposed Joint Enterprise Defense Infrastructure … until a period of 90 days has elapsed following the date on which the Secretary of Defense submits to the congressional defense committees—
>
> ....
>
> (2) a detailed description of the Department's strategy to implement enterprise-wide cloud computing, including the goals and acquisition strategies for all proposed enterprise-wide cloud computing service procurements; the strategy to sustain competition and innovation throughout the period of performance of each contract, including defining opportunities for multiple cloud service providers and insertion of new technologies….

Pub. L. 115-245, § 8137 at 50-51. DoD nevertheless seeks to have this Court accept a CO justification that presumes JEDI competition has no value.

223. In addition to the CO's failure to balance the noted benefits of competition against the purported disadvantages highlighted in the justifications, each of the purported disadvantages lack record support.

[redacted]

224. For instance, the CO's first purported justification for a single award IDIQ contract relies on two flawed assumptions: (i) without a single award approach, the offerors will charge higher prices for the classified and tactical edge offerings in order to recoup their investment into proposing such offerings and (ii) "fierce competition is expected under a single award scenario." (AR Tab 24 at 457-58.)

225. Turning to the latter assumption first, the CO's focus on base contract competition is misplaced. If base contract competition sufficed to overcome Congress' maximum practicable preference for multiple awards, the preference would be rendered meaningless. *WinStar*, 41 Fed. Cl. at 760 (finding unreasonable government's assumption that RFP could achieve "the same type of competitive benefits as multiple contract awards," and noting "this argument is not reasonably equivalent to multiple vendors competing head-to-head for each task order").

226. The CO's first assumption is similarly unsound. The record lacks any support for the conjecture that a single award contract will result in lower pricing. *WinStar*, 41 Fed. Cl. at 761-62 (rejecting similar unsupported claim).

227. Moreover, the underpinnings of the CO's assumption are wrong. For instance, the CO wrongly asserts that DoD cannot require awardees to compete for particular task orders. (AR Tab 24 at 457.) But, as DoD conceded to GAO, the FAR does not prohibit agencies from requiring each awardee to compete for all task orders. (AR Tab 71 at 5067-68 (citing FAR 16.505(b)).) The CO also wrongly assumes that a single award approach would guarantee the awardee the ability to recover its classified and tactical edge investments. Yet, the RFP only guarantees the awardee $1 million of work—1/100 of one percent of the JEDI value. (AR Tab 35 at 730; AR Tab 70 at 4985 (¶ 3).) As the CO testified: "The guarantee for the JEDI Cloud

[redacted]

requirement is a million dollars.... [Q: But there is no guarantee for tactical edge?] A: No. No separate guarantee for tactical edge...." (AR Tab 78 at 5592:16-5593:5.)

228. Although the JEDI contract does not guarantee what services the users will purchase or how many task orders the awardee will receive, the RFP requires each contractor to invest in the classified environment and tactical edge capabilities to compete. (*See, e.g.*, AR Tab 35 at 807-08 (requiring Category One tactical edge device in production by January 11, 2019 and the Category Two tactical edge device in production by day one of post-award kickoff).) The absence of any guarantee for classified or tactical edge services in the base competition evidences a fatal flaw in the CO's logic that a single award will result in better pricing

229. In the second purported justification, the CO overstates the costs of task order competition and disregards the benefits, which results in a series of severely flawed and misleading calculations:

	Multiple Award IDIQ	**Single Award IDIQ**	**Differential**
Cost Per Order	$127,851.84	$2,595.71	$125,256.31
Number of Orders	4,032	4,032	
TOTAL	**$515,498,618.88**	**$10,465,884.98**	**$505,032,733.90**

(AR Tab 24 at 456.)

230. By these unsupported calculations, the CO concludes that a single award approach purportedly will save DoD over $500 million and somehow "770 years worth of time ... of delaying warfighters" across a ten-year contract. (*Id.* at 460.)

231. The CO's assertions strain credulity. For instance, the CO reaches the patently baseless $500 million differential by assuming that DoD will have to expend 1688 hours awarding each multiple award task order versus 32 hours for a single award task order. The CO testified that she derived these hours from her "personal experience." (CO Test. at 322:1-5.) But the CO acknowledged that she has never purchased cloud services under an IDIQ contract before

[redacted]

and offered no explanation for how her prior experience related to task order competitions of the cloud computing services DoD solicits here. (*Id.* at 312:10-17.) No record support for the CO's hour estimations exists.

232. A GSA sponsored 2013 study revealed that agency time to award a task order averaged 119 to 168 hours depending on complexity. *Streamlining Task and Delivery Order Solicitations under MA/IDIQ Contracts* at 2, https://interact.gsa.gov/sites/default/files/ASI%20Advisory%20on%20Streamlining%20Final%206.9.2016.pdf (last visited 4/26/19). Conversely, the CO assumed 1688 hours for each task order competition—a 1318% increase that the CO could not explain. (AR Tab 24 at 466-67.)

233. The CO's claim that multiple award contracting will prevent "770 years worth of time … of delaying warfighters" across a ten-year contract is hardly credible. (*Id.* at 460.) The CO used a series of wholly unsupported inputs—4,032 task orders * 70 days (difference between 100 days the CO assumes for a multiple award order versus 30 days the CO assumes for a single award order) to arrive at 282,240 days. (*Id.*) Aside from the unsupported inputs, the reasoning seems to presume DoD will work one task order at a time, and not start any task order performance until DoD awards all 4,032 task orders.

234. The record also lacks any support for the CO's assumption that a competition for each task order will have the same duration and cost. At the hearing, the CO conceded: "You cannot predict across the board, how long that is going to take per task order." (AR Tab 78 at 5723:9-11.) Likewise, the record fails to corroborate the CO's assumption that the Agency will issue 4,032 task orders over the ten-year period. (AR Tab 24 at 456.) The funding profile in the Acquisition Plan casts serious doubt on the CO's task order estimates. (*Compare* AR Tab 23 at 432 [redacted] *with* AR Tab 24 at

[redacted]

456 [redacted].) The Agency offered no support for the CO's assumptions of 4,032 task orders of uniform size.

235. In a final catch-all exception, the CO concludes that the FAR precludes a multiple award acquisition strategy with task order competition because a single award of the JEDI Cloud contract is in the best interest of the government. (AR Tab 24 at 461-64.)

236. The CO's underlying suggestion that a multiple award approach would result in a prohibitive security risk or contravene DoD's interest by preventing data pooling or introducing complexity in administration fail for several reasons.

237. First, record documents contradict the CO's suggestion that DoD needs a single cloud approach because the security of multiple clouds will be too costly to manage. Several DoD entities and other federal agencies have awarded (or plan to award) contracts for multi-cloud offerings during the JEDI competition, undermining this purported security risk. DoD's own market research shows that the Defense Information Systems Agency ("DISA") MilCloud 2.0 leverages a multi-cloud approach. (*See* AR Tab 44 at 1009-11 ([redacted]).) DoD research also shows the Navy uses a multi-cloud approach. (*See* AR Tab 166 at 22919; *see also* AR Tab 161 at 22853 (indicating that NSA still has at least three smaller-scale private cloud deployments as well as its own large-scale SCI private cloud environment).)

238. Notably, the DoD CIO's Memorandum, issued with the RFP, reports that "DoD will always have a multiple cloud environment" (AR Tab 115 at 6788), and the Acquisition Strategy states that DoD "will continue to use disparate clouds." (AR Tab 25 at 505.) Indeed, in its Report to Congress about JEDI, DoD stated that it "is best served by a robust, competitive and

[redacted]

innovative technology industrial base." (AR Tab 109 at 6497.) DoD's multi-cloud environment contradicts the purported cost-prohibitive security risks.

239. Moreover, late last year, OMB published its government-wide Cloud Smart strategy recognizing that multi-cloud environments are "effective and efficient": "Industries that are leading in technology innovation have also demonstrated that hybrid and multi-cloud environments can be effective and efficient."[27]

240. Just weeks ago, the Central Intelligence Agency announced it is moving away from its current single cloud structure (using AWS) to a multi-cloud environment.[28]

241. And Congress has directed that DoD adopt a multi-cloud provider acquisition strategy for JEDI. Pub. L. No. 115-245, § 8137 at 50-51. It is impossible to reconcile the CO's assertions with the actions of DoD's largest and most secretive entities (awarding multi-cloud contracts during JEDI),[29] the DoD CIO's statements that DoD will always be multi-cloud, OMB's directive favoring multi-cloud, and Congress' JEDI multiple-provider direction.

242. Second, the DDS Deputy Director testified at GAO that the security risk arose not from the multi-cloud approach but instead from DoD's purported inability to manage that approach. (AR Tab 78 at 5452:15-54:4.) Given that DoD runs more than 500 different cloud efforts today, the suggestion that DoD cannot handle two or three JEDI contractors strains credulity and hardly provides a basis for limiting competition as DoD can contract that effort if need be. A contractor administers the DISA's MilCloud today. (AR Tab 44 at 1009-11; AR Tab

---

[27] OMB Cloud Smart Strategy, https://cloud.cio.gov/strategy/ (last visited 4/26/19).

[28] Aaron Gregg, *CIA long relied exclusively on Amazon for its cloud computing. Now it is seeking multiple providers for a massive new contract*, The Washington Post (Apr. 2, 2019), https://www.washingtonpost.com/business/2019/04/02/cia-long-relied-exclusively-amazon-its-cloud-computing-now-it-is-seeking-multiple-providers-massive-new-contract/?noredirect=on&utm_term=.d0e12cc1b805 (last visited 4/26/19).

[29] DoD entities such as DISA and the Navy do not have to use JEDI and the fact that these entities do not agree that a single cloud is more secure or better is telling.

[redacted]

25 at 471.) Notably, the CO's finding was that management of the multi-cloud approach would "increase costs" to DoD. (AR Tab 24 at 462.) But the CO neither quantifies nor explains how those costs exceed the benefits of competition.

243. Third, the record also belies the CO's suggestion that a single JEDI Cloud remains necessary to foster DoD's attempts to pool data. In lessons learned from 2011-2017 related to the CIA Commercial Cloud Service procurement and implementation (another document withheld from GAO), the Intelligence Community ("IC") reported that after five years the CIA has still not been able to implement a "data lake" due to slow migration of data to the cloud (IC analysts continue to use databases external to the cloud) and the fact that data maintained in different instances of the cloud, using different programs, is not pooled. (AR Tab 161 at 22856-57.)

WHEREFORE, Oracle requests that the Court declare that the CO's single award acquisition strategy violates 10 U.S.C. § 2304a(d)(4), FAR 16.504(c), Congress' latest direction in Pub. L. No. 115-245, § 8137 at 50-51 (Sept. 27, 2018), and otherwise lacks a rational basis, and enjoin DoD from pursuing an acquisition approach that fails "to sustain [cloud provider] competition and innovation throughout the period of performance" of the JEDI Cloud contract.

COUNT III
RFP Gate Criterion 1.1 (Elastic Usage) Exceeds DoD's Minimum Needs And Unduly Restricts Competition In Violation Of CICA

244. Oracle incorporates paragraphs 1 through 243 of the Complaint by reference.

245. Subfactor 1.1 requires each offeror to demonstrate that the DoD-provided, estimated JEDI cloud usage metrics (network, compute, and storage) are less than 50% of the offeror's Commercial Cloud Offering usage for the months of January-February 2018, i.e., nine months before the proposal deadline and eighteen months before the anticipated award date. (AR Tab 35 at 791.) The metrics are massive and the measurement time arbitrary, long

[redacted]

proceeding any possible need. JEDI Gate Criterion 1.1 consequently violates several independent U.S. Code and FAR provisions, including restrictions on qualification requirements, prohibitions on setting requirements prior to need, and using criteria to restrict competition to a few offerors without an appropriate justification and approval.

246. Agencies must solicit proposals "in a manner designed to achieve full and open competition." 10 U.S.C. § 2304(a); *id.* at § 2304a(c) (applying section 2304's competitive procedure requirements to task order contracts). If an agency believes that "the property or services needed by the agency are available from only one responsible source or only from a limited number of responsible sources," the head of the agency must issue an appropriate justification and approval document prior to restricting the competition. *Id.* at § 2304(c)(1).

247. DoD must "specify the agency's needs and solicit ... proposals in a manner designed to achieve full and open competition for the procurement" and "develop specifications in such manner as is necessary to obtain full and open competition...." *Id.* at § 2305(a)(1)(A)(i), (iii); 48 C.F.R. § 11.002(a)(1)(i). DoD may "include restrictive provisions or conditions only to the extent necessary to satisfy the needs of the agency or as authorized by law." 10 U.S.C. § 2305(a)(1)(B)(ii); 48 C.F.R. § 11.002(a)(1)(ii).

248. In furtherance of CICA's mandate, agencies may include restrictive requirements in a solicitation "<u>only to the extent they are necessary to satisfy the agency's legitimate needs</u>." *Am. Safety Council, Inc. v. United States*, 122 Fed. Cl. 426, 435 (2015) (finding solicitation clauses unduly restrictive); *Charles H. Tompkins Co. v. United States*, 43 Fed. Cl. 716, 723 (1999) (same). An agency cannot require an offeror to demonstrate the ability to meet a requirement at a point in time prior to when such requirement becomes relevant to the agency. *See, e.g.*, *USA Jet Airlines, Inc., Active Aero Grp., Inc.*, B-404666, Apr. 1, 2011, 2011 CPD ¶ 91.

[redacted]

249. Moreover, DoD may not use qualification requirement at all absent satisfaction of the various requirements set forth in 10 U.S.C. § 2319. A "'[q]ualification requirement' means a Government requirement for testing or other quality assurance demonstration that must be completed before award of a contract." 10 U.S.C. § 2319(a). To the extent that DoD (as here) seeks to impose qualification requirements in a solicitation, additional rules apply including that "the head of the agency shall, before establishing a qualification requirement—(1) 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(b)(1); *see W.G. Yates & Sons Constr. Co. Inc. v. Caldera*, 192 F.3d 987 (Fed. Cir. 1999) (declaring qualification requirement invalid where agency failed to follow statutory requirements). Still further, the U.S. Code prohibits DoD from denying offerors the opportunity to compete for contract award as long as the potential offeror can show that its solution meets the standard for qualification or <u>can meet</u> such standards by <u>the date specified for award of the contract</u>. 10 U.S.C. § 2319(c)(3).

250. DoD's failure to follow the proper statutory procedures for imposing Subfactor 1.1 as a qualification requirement render Subfactor 1.1 invalid and unenforceable as a matter of law. *W.G. Yates & Sons Constr.*, 192 F.3d at 992-93 ("any attempt by an agency to impose qualification requirements without following the procedures set out by Congress is a violation of § 2319, and such a qualification requirement must be struck down.").

251. As described by DoD, "Sub-factor 1.1. requires the Offeror to demonstrate that the JEDI Cloud portion of service usage will not constitute the majority (50% or more) of the Offeror's [Iaas] and [PaaS] usage, <u>once the Department of Defense's (DOD's) usage is added post award</u>." (AR Tab 42 at 944.) But DoD's characterization of Subfactor 1.1. is inaccurate. Gate

[redacted]

Criterion 1.1 does not measure which offerors can meet the Agency's needs when DoD usage is "added post award." Instead, Subfactor 1.1 measures which offerors can meet the Agency's usage metrics in January and February 2018—more than seventeen months before any award. If the Agency sought to measure each offeror's capability to meet the Agency's needs on or after award in July 2019, the Agency would have a much better argument. The Agency, however, does not seek to measure the offerors' ability to meet the Agency's needs at the time of award.

252. Instead, Subfactor 1.1 requires each offeror to demonstrate "for evaluation purposes" that the identified JEDI Cloud unclassified usage numbers for network ingress and egress, compute, and storage are less than 50% of the Commercial Cloud Offering usage for network ingress and egress, compute and storage during the months of January-February 2018. (AR Tab 35 at 791.) The criterion measures dated, historic usage (January-February 2018), while the rationale for including the criterion speaks to future capacity (July 2019 and later).

253. The Agency states that Subfactor 1.1. exists to ensure that: (1) the Cloud is capable of providing the full scope of services even under surge capacity during a major conflict or natural disaster event; and (2) the Cloud experiences ongoing innovation and development and capability advancements for the full potential period of performance. (AR Tab 42 at 944; AR Tab 78 at 5475:5-14, 5483:19-5484:1.)[30] But by soliciting historic usage data from early 2018, the Agency tests no such thing.

254. DoD's need for surge capacity will not arise until after contract award, when DoD places its data in the cloud. (*Id.* at 5476:5-9.) Stated otherwise, as long as the offeror at the time of award has the excess capacity to meet DoD's surge needs, the offeror will meet DoD's

[30] "[S]urge capacity is the ability to meet sudden unexpected demands in usage," and these metrics seek to assess whether the offeror's Cloud can handle a certain number of users and data in a future, worst-case disaster scenario. (AR Tab 78 at 5475:15-5476:9.)

[redacted]

minimum needs. (*Id.* at 5477:2-12.) What necessarily matters is relative capacity at the time of performance; not historic usage nine months before proposal submission and at least seventeen months before contract award.

255. Among other outsized usage requirements,[31] Subfactor 1.1 compels each offeror to demonstrate an existing commercial cloud offering storage usage of 200 Petabytes offline across two months (January – February 2018). (AR Tab 35 at 791.) For understanding, two Petabytes (1/100th of the standard set by DoD) equates to the volume of information housed in all U.S. academic research libraries.[32] DoD does not require such storage on contract day one, much less seventeen months earlier. Indeed, the Acquisition Strategy estimates a fiscal year 2019 spend of [redacted]. (AR Tab 25 at 491.) The network, compute, and other storage requirements contain equally restrictive requirements designed to close this competition to all but a few of the very largest providers.

256. Although the Subfactor 1.1 metrics are substantial, Oracle primarily objects to the timing of the application. By focusing on a historic period many months prior to proposal submission, and without considering the cloud's capacity at the same time, Subfactor 1.1 arbitrarily excludes offerors that can satisfy DoD's actual minimum performance needs from the

[31] Although DoD has required offerors to calculate an average storage usage by taking the sum of the total storage in use each day between January 1st and February 28th and dividing that amount by the total number of days in the time period (i.e., 59), the gate memorandum shows that DoD did not perform a similar calculation for the JEDI Cloud storage estimate in Subfactor 1.1. (AR Tab 42 at 946.) Instead, DoD found a monthly storage report for online storage for January 2018 and calculated a nearline and offline storage estimate for the same period based on a multiplier (1.5x for nearline and 4x for offline). (*Id.*) DoD then assumed the average storage usage for February was the same. (*Id.*) Accordingly, any comparison of the purported JEDI cloud storage usage in the RFP to how DoD directed each offeror to calculate the commercial cloud's storage usage is not an apples-to-apples comparison.

[32] http://pcbunn.cithep.caltech.edu/presentations/giod_status_sep97/tsld013.htm (last visited 4/26/19).

[redacted]

competitive field and allows offerors that cannot meet DoD's actual minimum performance needs into the competitive field.

257. Indeed, as written, an offeror that had customer usage in January and February 2018 slightly below the Subfactor 1.1 metrics and significant excess capacity, but had commercial paying customer usage growing materially month over month yet maintaining excess capacity, would fail the gate despite substantially exceeding the criteria at proposal submission and award. Conversely, an offeror with customer usage in January and February 2018 slightly above the metrics, but which has a diminishing client base and declining capacity, would pass the gate even though it could not satisfy the criteria at proposal submission or award. (AR Tab 78 at 5478:7-18; *id.* at 5480:18-5481:6.)

258. Thus, Subfactor 1.1 does not, as claimed by DoD, require the offeror to demonstrate that the JEDI Cloud portion of service usage will not constitute the majority of the Offeror's commercial cloud usage post award. The January-February 2018 historic usage metrics have little bearing on the offeror's future usage or capacity to meet DoD's actual compute, network, and storage needs in July 2019 (when the award is anticipated) and beyond.

259. DoD suggests that the January-February 2018 snapshot will "facilitate fair competition" by preventing offerors from "gaming" their usage numbers to compete. (AR Tab 42 at 945; AR Tab 78 at 5422:4-10; *see also id.* at 5423:8-14.) DoD offers no evidence for its dubious suggestion that offerors would give services away for the chance to compete considering JEDI requires significant investment already in DoD-unique capabilities, i.e., the production of tactical edge devices and the development of classified cloud services. Such an unwarranted concern does not provide a valid basis to narrow the competitive field. And, DoD had other less restrictive means of preventing gamesmanship in any event. For instance, DoD could resolve its

[redacted]

unfounded data manipulation concern by seeking usage from January-February 2018 and a more recent period and asking offerors to explain any difference.

260. Subfactor 1.1 competitively prejudices Oracle. The Agency deemed Oracle's proposal unacceptable under this subfactor and excluded Oracle from the competition. (TEB Report for Oracle at 4-5; CO Competitive Range Mem.)

261. Had the Agency removed or recrafted the criteria as the law required, Oracle would have remained in the competition. Likewise, had the Agency applied the criteria at an appropriate time (proposal submission or award), Oracle would have remained in the competition.

262. The Agency's irrational and unlawful decision to test each offeror's capacity for future performance needs based on historic usage in January and February 2018 (nine months before proposal submission and seventeen months before award) severely prejudiced Oracle.

WHEREFORE, Oracle requests that the Court declare that Subfactor 1.1 unduly restricts competition in violation of various U.S. Code and FAR provisions and enjoin DoD from awarding a contract under the RFP unless DoD removes or revises the flawed criterion, reopens the competition to excluded offerors, and evaluates the offerors against the revised criteria.

COUNT IV
Even If DoD Had A Legitimate Need For Evaluating Subfactor 1.1 Elastic Usage As Of January And February 2018 (Which DoD Did Not), The Agency's Competitive Range Determination Lacks A Rational Basis And Is Unequal

263. Oracle incorporates paragraphs 1 through 262 of the Complaint by reference.

264. DoD received only four potentially viable proposals under the JEDI RFP. DoD found the proposals [redacted]. Despite that [redacted], DoD, on April 9, 2019, established a competitive range limited to two of the [redacted] offerors (AWS and Microsoft) and eliminated two purportedly

[redacted]

unacceptable offerors (Oracle and IBM). (PCO Mem. Re: Competitive Range at 1.) Each of the offerors merited an equal opportunity to address their purported deficiencies.

265. When setting a competitive range, an agency must act in an even-handed manner toward the offerors. *L-3 Commc'ns EOTech Inc. v. United States*, 83 Fed. Cl. 643, 652 (2008) (granting judgment for protester where agency treated offerors differently).

266. Here, the CO deemed Oracle's proposal unacceptable and not eligible for inclusion in the competition range based on the Agency's unreasonable evaluation of Oracle's proposal against Subfactor 1.1. For Subfactor 1.1, the RFP specifies that the "Government will evaluate whether the proposal clearly demonstrates <u>that the addition of DoD unclassified usage will not represent a majority of all unclassified usage</u>, per the requirements in Section L for this sub-factor." (AR Tab 35 at 806.) In turn, Section L provides that the "Offeror's proposal, for all aspects of this Sub-factor, must explicitly depict CCO usage." (*Id.* at 791.)

267. Oracle's proposal demonstrated that under each of the Subfactor 1.1 metrics—network, compute, and storage—the addition of anticipated JEDI Cloud usage would not represent a majority of Oracle's total commercial cloud usage.

268. Specifically, for network, Oracle's proposal states on Tab A at page 2 that the JEDI unclassified ingress of 10.6 petabytes "is less than 50 percent of the <u>aggregate usage</u> during this time frame," and the unclassified egress of 6.5 petabytes "is <u>far less</u> than 50 percent of the aggregate usage during this time frame." Oracle further demonstrated this fact through the summary report table at Tab A, Appendix A:

[redacted]

TABLE 1: NETWORK

	Total Data Transfer 2 months (PB)	Bandwidth Required (~Gbps)	Bandwidth Required ~(PB/Day)	Oracle P99	% JEDI Usage to Oracle Usage
JEDI Ingress	10.6	16.57	0.1797	[redacted]	
JEDI Egress	6.5	10.18	0.1102		

269. The Table shows JEDI Ingress of 10.6 PBs equates to 16.57 Gbps, i.e., Oracle performed the mathematical conversion for DoD. (Oracle measures its network usage in Gbps.) During that same period, Oracle verified CCO Ingress network usage of [redacted] Indeed, in clarifications with the Agency, Oracle explained that this network utilization was conservative. (November 20, 2018 Email from Oracle to JEDI Team (explaining that "P99" reports network traffic utilization after smoothing out peak utilization numbers).) Adding 16.57 Gbps to [redacted] yields a total Ingress network ***usage*** of [redacted] In turn 16.57 Gbps is [redacted] of that total usage, as Oracle demonstrated by showing [redacted] as the percentage of JEDI Ingress usage relative to Oracle's total CCO Ingress usage.

270. The Table shows JEDI Egress of 6.5 PBs equates to 10.18 Gbps. During that same period, Oracle had CCO Egress network usage of [redacted]. 10.18 Gbps and [redacted] equates to a total network ***usage*** of [redacted] and 10.18 is [redacted] of that total usage, as reflected in the table showing [redacted] difference between the JEDI Egress aggregate usage to total CCO Ingress usage.

271. The evaluators, however, inexplicably "presumed" that the last column of the Oracle table—a column that is labeled "% JEDI ***Usage*** to Oracle ***Usage***" reflected a comparison of the "minimum network capacity the Offeror calculates … to support the JEDI Cloud aggregate network … usage and the ***total network capacity*** of the Offeror's CCO for the period of January 2018 through 2018." (TEB Report at 3 ("This proposal is found 'Unacceptable' for

[redacted]

Subfactor 1.1.(1) because the Offeror's 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.").)

272. Oracle's chart shows the numbers as a usage comparison, yet the Agency treated it as a capacity comparison. To the extent the last column of Oracle's Table 1 in the Summary Report of its proposal (despite that it twice says "usage") somehow confused the evaluators, the evaluators could and should have sought clarification from Oracle rather than presuming the word "usage" did not mean "usage," but instead meant "capacity." *L-3 Commc'ns EOTech*, 83 Fed. Cl. at 658 (recognizing that the "decision not to seek clarifications from an offeror must be reasonable under the circumstances of the procurement.").

273. The evaluators' compute metric assessment is likewise irrational. Oracle's proposal shows that the JEDI Cloud compute estimate in the RFP constitutes only [redacted] of the total CCO usage for Oracle, and thus demonstrated that the addition of JEDI compute usage <u>will not represent a majority of all compute usage</u>:

[redacted]

274. Nevertheless, the evaluators deemed Oracle's proposal unacceptable under the compute metric because Oracle did not duplicate the same table on the Summary Report Tab of its proposal. (Debriefing Response to question 21(b).)

275. Finally, even though Oracle's proposal established that since February 2018, the estimated JEDI storage usage would not comprise a majority of the average storage usage for the Oracle commercial cloud and was only a fraction of the Oracle cloud capacity which continued

[redacted]

to grow with usage, and that Oracle substantially exceeded the storage usage criteria as of proposal submission, the evaluators also deemed Oracle's proposal unacceptable under the storage metric based on the arbitrary and unduly restrictive January 2018 and February 2018 timeframe.

276. Given DoD's stated rationale for Gate Criterion 1.1, what matters is relative capacity of the Cloud at the time of performance. Oracle's proposal makes clear that Oracle's Cloud usage and capacity was growing month over month and that Oracle exceeded the arbitrary metric by March 2018 and far exceeded the metric by July 2018. Moreover, Oracle advised DoD that Oracle continues to invest in its commercial cloud and thus JEDI would never become a majority of Oracle's service: "As Oracle has announced plans to build 12 additional data centers globally, and continues to expand capacity at existing centers, Oracle Cloud will remain a majority commercial service even if JEDI capacity expands significantly beyond the numbers provided for evaluation purposes." (Oracle Proposal, Tab A at 1.)

277. Accordingly, because Oracle's proposal demonstrates that Oracle can satisfy the JEDI Cloud elastic usage storage requirements as of proposal submission and throughout performance and that Oracle has plenty of capacity to address any legitimate Subfactor 1.1 needs of DoD, no rational basis existed to find Oracle unacceptable under Subfactor 1.1 and exclude the Oracle proposal from further evaluation.

278. Further, if any doubt existed about Oracle's ability to meet DoD's purported Subfactor 1.1 needs, DoD should have given Oracle the same opportunity for discussions that DoD has opted to give the two [redacted] competitive range offerors. In this regard, each of the two proposals included in the competitive range [redacted], rendering both competitive range offerors [redacted] For instance, the initial

[redacted]

evaluation of AWS [redacted] (PCO Competitive Range Determination at 2-3.) The Agency also deemed AWS' [redacted]. (*Id.* at 3.) Stated otherwise, AWS [redacted] passed through to discussions and proposal revisions. The Agency also found Microsoft [redacted] and passed it through to discussions. Given the [redacted] for the competitive range offerors, no reasonable basis existed for the CO to exclude Oracle based on the Agency's confusion regarding Oracle's ability to meet Subfactor 1.1.

279. Given that [redacted], and in the interest of competition, the Agency should have included Oracle in the competitive range. Such a result is consistent with the RFP which provides: "The competitive range will be limited to no more than four proposals." (AR Tab 35 at 782.)

WHEREFORE, Oracle requests that the Court declare the Agency's evaluation of Oracle's proposal against Subfactor 1.1 and Oracle's exclusion from the competitive range to lack a rational basis and enjoin DoD proceeding with award until the Agency returns Oracle to the competitive range and provides Oracle with an opportunity to participate in discussions and update its proposal, like the [redacted] offerors comprising the competitive range.

COUNT V
RFP Gate Criterion 1.2 (High Availability And Failover) Exceeds DoD's Minimum Needs And Unduly Restricts Competition In Violation Of CICA

280. Oracle incorporates paragraphs 1 through 279 of the Complaint by reference.

281. Subfactor 1.2 seeks to leverage FedRAMP as a qualification requirement by mandating that each offeror have, at the time of proposal submission, no fewer than (i) three physically existing data centers (ii) within the customs territory of the United States (iii) that are

[redacted]

separated by at least 150 miles, (iv) capable of automated failover to the others, and (v) each "supporting at least one IaaS and 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 Tab 35 at 792; AR Tab 32 at 661 (*see* government responses to Q26 and Q27); AR Tab 42 at 947; AR Tab 78 at 5488:22-5489:7.) The offeror must satisfy all five conditions by the time of proposal submission to pass the gate and compete for the JEDI Cloud contract. (AR Tab 78 at 5489:7-10.)[33]

282. DoD admits that the JEDI contract does not require FedRAMP authorization at all—much less at the time of proposal submission: "[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…." (AR Tab 78 at 5495:5-14.) The offeror need not even propose the data centers and offerings used to clear the gate. (AR Tab 40 at 853 (Q233).) Still further, FedRAMP prohibits use of its authorizations as a bidding criterion. This gate criterion violates numerous statutory and FAR provisions. *See e.g.*, 10 U.S.C. § 2304(a); *id.* at § 2304a(c); *id.* at 10 U.S.C. §§ 2319(b), (c).

283. DoD describes Subfactor 1.2's FedRAMP authorization requirement 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.) Significantly, however, DoD will not require FedRAMP authorization as part of performance or even use of the data centers by which the offeror passes the gate; this is merely a qualification test governed by 10 U.S.C § 2319. (AR Tab 78 at 5495:5-14 ("[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

[33] DoD declared IBM, another massive commercial and government cloud provider, ineligible against this gate. DoD did not evaluate Oracle against this gate.

[redacted]

solution"); *id.* at 5496:3-6 ("Q: So if I understand correctly, your cybersecurity plan does not require FedRAMP authorization. A: Correct.").)

284. The Federal Circuit has explained that "qualification requirements" cover "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." *W.G. Yates & Sons Constr.*, 192 F.3d at 994.

285. But DoD did not follow the statutory and regulatory requirements to impose Subfactor 1.2 as a qualification requirement. The head of the agency did not issue a written justification stating the necessity for establishing the qualification requirement and the rationale for why the offeror must demonstrate that it meets the qualification prior to proposal submission. 10 U.S.C. § 2319(b)(1). Nor has DoD provided each potential offeror the opportunity to show that the offeror could satisfy the qualification requirement before the intended award date. *Id.* § 2319(c)(3). Instead, in order to compete for the contract, the RFP requires that offerors meet the Subfactor 1.2 requirements by the date of the proposal submission. (AR Tab 35 at 792.)

286. Subfactor 1.2 is therefore invalid and unenforceable as a matter of law. *W.G. Yates & Sons Constr.*, 192 F.3d at 992-93 ("any attempt by an agency to impose qualification requirements without following the procedures set out by Congress is a violation of § 2319, and such a qualification requirement must be struck down.").

287. In addition, and as a separate basis for finding Subfactor 1.2 unlawful, DoD has not and cannot establish a <u>legitimate need</u> for "FedRAMP Moderate Authorized" cloud service offerings in three data centers <u>at the time of proposal submission</u>.

288. FedRAMP, the government-wide program providing the standardized approach for security assessments, authorizations, and monitoring of cloud products, <u>prohibits</u> the exact

[redacted]

requirement DoD seeks to apply here—requiring FedRAMP authorization as a precondition to bid. FedRAMP has established this prequalification prohibition because procuring agencies lack a legitimate need for FedRAMP authorized offerings until after contract award ***when the systems will hold federal data***: "Federal Agencies cannot require CSPs 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." *FedRAMP Tips & Cues Compilation 2015-2017* (Jan. 2018) at 7, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Tips_and_Cues.pdf; *see also id.* at 13 ("Agencies can request a CSP to have a timeline for obtaining an ATO but should not limit the request to CSPs with ATOs.").

289. The record offers no valid rationale for DoD violating the FedRAMP guidance. Instead, DoD has acknowledged that it has no need for failover capabilities unless and until DoD data is placed in the Cloud. (AR Tab 78 at 5487:10-15.) Similarly, DoD confirmed in response to offeror solicitation questions that DoD has no need for three operational unclassified data centers until after contract award: "The requirement is that the three unclassified data centers must be online and available thirty days after the conclusion of the post award kick-off event." (AR Tab 32 at 675 (answer to Q157).)

290. In short, DoD cannot articulate any legitimate, pre-proposal need for FedRAMP Moderate Authorized offerings in three data centers. *See USA Jet Airlines, Inc., Active Aero Grp., Inc.*, B-404666, Apr. 1, 2011, 2011 CPD ¶ 91 (sustaining pre-award protest where agency failed to show why offerors needed certifications prior to performance); *LBM, Inc.*, B-286271, Dec. 1, 2000, 2000 CPD ¶ 194 (describing exclusionary effect of requiring certification by proposal deadline where agency lacked need until contract performance).

[redacted]

291. DoD's suggestion that the Cyber Security Plan's requirements justify Subfactor 1.2 likewise fails. The Cyber Security Plan does not require authorization through the FedRAMP process. (AR Tab 78 at 5495:5-14); *id.* at 5496:3-6.) Instead, the RFP and contract contemplate that DoD will work with the awardee post-award to ensure the proposed offerings and data centers comply with the Cyber Security Plan, outside of the FedRAMP process. (*Id.* at 5496:7-5498:15; *see also* AR Tab 5 at 159.)

292. DoD's response to RFP question 233 also establishes that Subfactor 1.2 does not reasonably relate to the contract requirements. DoD advised offerors that they did not even have to propose the data centers and offerings used for the gate: "the RFP does not restrict an Offeror from proposing its latest technologies, even if not FedRAMP authorized at the time of proposal. The RFP does not prescribe which specific IaaS offering and which specific PaaS offering is used to satisfy the Sub-Factor 1.2 Gate Criterion." (AR Tab 40 at 853 (Q233).)

293. Subfactor 1.2 thus bears no rational relationship to DoD's actual and legitimate needs or the JEDI contract terms, and DoD offers no rational reason for deviating from the FedRAMP requirements and standard DoD practice.

294. The unduly restrictive requirements in Subfactor 1.2 cause Oracle significant competitive prejudice. Oracle began investing heavily in its Next Generation Government Cloud offerings in late 2017 and seeks to offer this latest state-of-the-art technology to JEDI Cloud users. (AR Tab 187 at 23981 (¶ 12).)

295. Oracle's Next Generation Cloud will consist of [redacted] (*Id.* (¶ 13).) [redacted] (*Id.* (¶¶ 15-16).)

[redacted]

296. Subfactor 1.2 will affect Oracle's ability to compete for the JEDI Cloud contract, even though Oracle can meet the JEDI Cloud contract security requirements.

297. Therefore, the Agency's unreasonable and unlawful inclusion of Gate Criterion 1.2 causes Oracle "a non-trivial competitive injury which can be redressed by judicial relief." *Weeks Marine*, 575 F.3d at 1362. This Court can redress Oracle's competitive injury by enjoining DoD from making award under the current RFP and directing the Agency to remove or revise the unduly restrictive Subfactor 1.2 Gate Criterion.

WHEREFORE, Oracle requests that the Court declare Gate Criterion 1.2 improper and unduly restrictive of competition in violation of CICA and enjoin DoD from making award under the RFP until DoD amends the RFP to eliminate or relax Gate Criterion 1.2 and allows offerors to submit proposals in accordance with the compliant requirements.

COUNT VI
RFP Gate Criterion 1.6 (Marketplace) Exceeds DoD's Minimum Needs And Unduly Restricts Competition In Violation Of CICA

298. Oracle incorporates paragraphs 1 through 297 of the Complaint by reference.

299. Subfactor 1.6 requires demonstration, at the time of proposal submission, that the offeror has an online marketplace of third-party platform and software offerings that JEDI Cloud users can access to purchase and provision software. (AR Tab 35 at 793-94.) Other RFP provisions, including the SOO and contract clause H10, specify this marketplace requirement. (AR Tab 27 at 616; AR Tab 35 at 748-49.) DoD's stated reasoning for this requirement is to evaluate "the range of offerings in such a marketplace," and confirm that "the user can easily go from the entry point (post log in) to deployment of the offering in a reasonable timeframe." (AR Tab 42 at 950-51.)

[redacted]

300. DoD cannot establish a legitimate need for the required online software marketplace because DoD lacks authority to procure such a market. By outsourcing the selection of third-party software applications available for purchase by DoD to the Cloud provider, DoD has abdicated its responsibility to procure supplies and the many legal and regulatory requirements that govern such a procurement. *See* 48 C.F.R. § 7.503(a) ("[c]ontracts shall not be used for the performance of inherently governmental functions."). The RFP also lacks any provisions or controls to address the manifest organizational conflicts of interest that will arise from DoD delegating the control of DoD's software marketplace to a contractor.

301. In Section 846 of the FY2018 NDAA, Congress authorized the GSA Administrator, not DoD, to "establish a program to procure commercial products through commercial e-commerce portals," directed GSA to implement the program through a phased approach and required GSA to "carry out the program ... through multiple contracts with multiple commercial e-commerce portal providers...." Pub. L. 115-91, § 846(a), Dec. 12, 2017, 131 Stat. 1483. Section 846 defines a "commercial e-commerce portal" as "a commercial solution providing for the purchase of commercial products aggregated, distributed, sold, or manufactured via an online portal." *Id.* § 846(k)(3).

302. Per the RFP, the JEDI Cloud offering will include the commercial vendor's online commercial marketplace from which JEDI Cloud users can "purchase [] software, and then provision" it onto their systems. (AR Tab 78 at 5504:11-22.) The RFP's online marketplace thus falls within Section 846's definition of an "e-commerce portal."

303. This Court recently declared that another federal agency's attempt to use a vendor-overseen marketplace violated CICA. *Electra-Med Corp.*, 140 Fed. Cl. at 104 ("By outsourcing the selection of suppliers to the PVs [Prime Vendors] entirely, the government has avoided the

[redacted]

multitude of legal and regulatory requirements appurtenant to a federal procurement...."). The Court should similarly find that the solicited marketplace here contravenes the law.

304. DoD has not identified any authority permitting it to set up an online marketplace or how such a vendor-run marketplace complies with CICA. (*See, e.g.*, AR Tab 42 at 950-51.) Instead, DoD contends that Oracle (which has a marketplace for its commercial customers) suffers no harm from DoD exercising authority it does not have. That commercial cloud providers (including Oracle) may offer an online software marketplace, and that DoD may want one, does not justify DoD including such requirements in an RFP when DoD lacks authority to procure one.

305. The Subfactor 1.6 requirement competitively prejudices Oracle. The Federal Circuit has made clear that injury stemming from an illegal solicitation term suffices to establish prejudice in a pre-award protest because contractors have a "definite economic stake in the solicitation being carried out in accordance with applicable laws and regulations." *Weeks Marine*, 575 F.3d at 1362-63.

306. Here, Oracle, a JEDI actual bidder and DoD software provider, has an "economic stake" in DoD carrying out the RFP in accordance with applicable law, including those related to DoD's lack of authority to procure an enterprise-wide commercial software marketplace. *Id.* at 1363.

307. The Agency's improper inclusion of Gate Criterion 1.6 causes Oracle "a non-trivial competitive injury which can be redressed by judicial relief." *Weeks Marine*, 575 F.3d at 1362. Specifically, this Court can redress Oracle's competitive injury by enjoining DoD from making award under the current RFP and directing DoD to remove the unlawful requirement.

[redacted]

WHEREFORE, Oracle requests that the Court declare the marketplace Gate Criterion and associated requirements unlawful and unduly restrictive of competition and enjoin issuance of a contract pending removal of Gate Criterion 1.6 and related requirements.

COUNT VII
The CO Irrationally Determined That Ubhi's Misconduct Did Not Impact The JEDI Acquisition

308. Oracle incorporates paragraphs 1 through 307 of the Complaint by reference.

309. DoD and Ubhi violated numerous legal proscriptions by failing to screen Ubhi as required, permitting Ubhi's participation in JEDI despite severe conflicts, and failing to take the steps necessary to remove the taint caused by these improprieties. (Oracle addresses AWS' role in Ubhi's misconduct by Count X.)

310. Corrupt procurement systems rank among the highest risks to a free, democratic society. Consequently, to maintain the integrity of the procurement system, FAR 3.101-1 requires the government to conduct its business "in a manner above reproach ... with complete impartiality and with preferential treatment for none," demands personnel adhere to an "impeccable standard of conduct," and prohibits even the appearance of conflicts of interest in government-contractor relationships. 48 C.F.R. § 3.101-1. Recognizing that "many Federal laws and regulations place restrictions on the actions of government officials", FAR 3.101-1 further requires that their conduct "must, in addition, be such that they would have no reluctance to make a full public disclosure of their actions." *Id.*; *see also* 48 C.F.R. § 1.102-2(c)(1) (highlighting the criticality of "maintaining the public trust").

311. Several statutory and regulatory systems underpin the FAR's broad mandate to avoid even the appearance of conflicts in government-contractor relationships. *See* FAR Subpart 3.1 (incorporating 18 U.S.C. § 208 and 5 C.F.R. Part 2635). These laws, which serve to "insure

[redacted]

honesty in the Government's business dealings," set an objective standard of conduct, and "whenever a government agent fails to act in accordance with that standard, he is guilty of violating the statute, regardless of whether there is positive corruption." *United States v. Mississippi Valley Generating Co.*, 364 U.S. 520, 548-49, 562 (1961).

312. By design, Congress has not limited the proscriptions to final decisionmakers. *Id.* at 554-55. Instead, anytime a government employee "personally and significantly" participates in a particular matter, the prohibitions apply. *See, e.g.*, 5 C.F.R. § 2635; 48 C.F.R. § 3.104-1 (FAR providing that restrictions cover actions even though "not determinative of outcome" and noting that even participation in a single procurement-critical step may be substantial).

313. When a violation occurs, the involved agency may not simply sweep the violation aside as a matter of convenience, need, or otherwise: "To find that the interest of the public, the rights of the competing bidders, and the integrity of the federal procurement process can be ignored because DOE chooses, in this instance, to do so would be senseless and self-defeating." *TRW Envtl. Safety Sys., Inc. v. United States*, 18 Cl. Ct. 33, 67 (1989) (sustaining bid protest).

314. Critical in assessing the impact of all such conflicts is "protect(ing) the public from the corruption which might lie undetectable beneath the surface of a contract conceived in a tainted transaction." *K & R Eng'g Co., Inc. v. United States*, 616 F.2d 469, 474 (Ct. Cl. 1980).

315. The Court of Federal Claims has identified three relevant questions – (1) did the government employ the individual; (2) did the individual participate "personally and substantially" in the contract letting, performance, or administration; and (3) did the individual have a prohibited conflict. *Id.* at 472. If the answer to all three is yes, the agency must act to preserve trust in the procurement system—including terminating contracts and excluding implicated contractors.

[redacted]

316. As to Ubhi, the answer to all three relevant questions is "yes," as acknowledged by the Agency's own re-assessment. Equally significant, the record makes abundantly clear that Ubhi's misconduct has severely tainted and impacted JEDI—no matter what the DDS personnel who failed to screen Ubhi and contemporaneously missed the improprieties may now assert.

317. First, DoD acknowledges (and the record establishes) that DDS employed Ubhi.

318. Second, DoD acknowledges (and the record establishes) that Ubhi participated personally and substantially in JEDI. (Ubhi Mem. at 14 (¶ 61) (CO finding that Ubhi violated FAR 3.101 by seeking employment with a potential offeror while being personally and substantially involved in JEDI).)

319. Third, DoD acknowledges that Ubhi's actions violated FAR 3.101 at a minimum and quite likely 18 U.S.C. § 208 and its implementing regulations. (*Id.* at 14 (¶ 62).)

320. Indeed, no legitimate dispute exists that Ubhi had a prohibitive conflict and violated numerous procurement statutes and regulations. Section 208 of Title 18 requires a government employee to disqualify himself from engaging in official activities that may affect the financial interests of a prospective employer. Under the applicable implementing regulations, a federal employee must recuse himself from particular matters having a direct and predictable effect on the financial interests of a <u>prospective employer</u> with whom the employee seeks employment. 5 C.F.R. § 2635.604. Moreover, a federal employee, who has an agreement to return to a private sector employer at a future date, may not work on matters involving that entity. *See id.* at §§ 2635.403, 606.

321. The applicable regulation defines "seeking employment" broadly to include an unsolicited communication regarding possible employment or a response, other than a rejection to an unsolicited communication regarding possible employment. *Id.* at § 2635.603(b)(1). "The

[redacted]

term is not limited to discussions of specific terms and conditions of employment in a specific position." *Id.*

322. Section 2103 of Title 41 likewise requires an agency official "participating personally and substantially in a Federal agency procurement", who contacts or is contacted by an offeror in that procurement regarding possible employment, to (i) promptly report the contact in writing to the official's supervisor and to the agency ethics official, and (ii) either reject the employment or disqualify himself from further participation. FAR 3.104-3(c) implements this statutory provision.

323. As with FAR 3.101, Ubhi did not comply with 18 U.S.C. § 208, 41 U.S.C. § 2103, or the respective implementing regulations (FAR and 5 C.F.R.). To the contrary, Ubhi engaged in extensive <u>undisclosed</u> employment discussions with AWS throughout 2017, including throughout the time Ubhi worked as the JEDI lead PM, a particular matter involving AWS. (Ubhi Mem. at 15-16 (¶ 65); *id.* at 10-11 (¶¶ 39-42).)

324. On August 23, 2017, a few weeks after General Mattis visited AWS regarding DoD cloud computing, Ubhi emailed AWS, indicating Ubhi would consider AWS' earlier offer to "craft [Ubhi's] own role" to come back to AWS. (*Id.* at 11 (¶ 42).) Ubhi did not disclose this contact to DoD.

325. Instead, Ubhi shortly thereafter accepted his DoD role as lead PM for JEDI, joining the four-person DDS team leading the acquisition effort in mid-September 2017. (AR Tab 47a at 2793, 2813.)

[redacted]

326. DoD neither properly screened Ubhi nor obtained an executed non-disclosure agreement from Ubhi. (*Cf.* AR Tab 53.) Had DoD done so, Ubhi never could have participated on JEDI.[34]

327. In mid-September, Ubhi (in active employment discussions with AWS) set up the Google drive to act as DoD's "repository for *everything*" JEDI related. (AR Tab 47a at 2910.) Ubhi and the DDS team subsequently convinced all of the DoD JEDI participants "to data dump everything into Google Folder." (AR Tab 47b at 2986.)

328. On September 22, 2017, during JEDI, AWS and Ubhi further discussed Ubhi rejoining AWS. (*Id.* at 15 (¶ 65.ii.b).) Neither Ubhi nor AWS advised DoD of these discussions.

329. Three days later, on September 25, 2017, Ubhi asked to serve as DoD's point of contact for all JEDI competitors and to lead the associated offeror capabilities meetings. (AR Tab 47b at 3049 (Ubhi saying "[m]ake it me please").)

330. Significantly, at or about this point, AWS necessarily both knew that AWS had made offers to Ubhi and Ubhi had not recused himself from AWS matters as the law required. Indeed, on September 25, 2017, [redacted], AWS' [redacted], emailed Chris Lynch of DDS. (AR Tab 34 at 697.) Lynch responded two days later, on September 27, 2017 "adding Deap on our team to help get something scheduled." (*Id.*) On October 2, 2017, Ubhi responded to the AWS JEDI point of contact, advising AWS that Ubhi was "running point on all [JEDI] industry touch points." (AR Tab 34 at 699.) Plainly, AWS knew Ubhi had not recused himself from AWS matters (including JEDI) as Title 18, the Procurement Integrity Act ("PIA"), the FAR, and 5 C.F.R. required. Still neither AWS nor Ubhi advised DoD of the ongoing AWS-Ubhi employment communications—a potential violation for

[34] DDS claims that it orally screened Ubhi and he lied about his AWS relationship. (Ubhi Mem. at 5 (¶ 23).)

[redacted]

both participants. *See* 48 C.F.R. § 3.104-3(c) (requiring DoD employee to provide notice and recuse); *Id.* at § 3.104-8(b) (requiring contractor to provide notice where contractor knows that employee has not complied with 3.104-3).

331. On October 4, 2017, Ubhi verbally committed to accept AWS' offer and return to AWS. (Ubhi Mem. at 15 (¶ 65.ii.d).) Again neither Ubhi nor AWS notified DoD of the employment agreement.

332. Rather than recuse himself from JEDI, Ubhi stepped up his efforts to obtain valuable DoD JEDI information, to misappropriate JEDI competitor information, and to shape JEDI for AWS.

333. For instance, at some point during this period Ubhi downloaded all of the Google drive to his laptop—taking all of DoD's JEDI information outside of DoD's oversight and control. (Dkt. 40-1 at 6 (DoD admitting that Ubhi had downloaded the entire google drive to his laptop).) Despite DoD verifying that Ubhi downloaded this information to his laptop, DoD has taken no steps to investigate what Ubhi downloaded, when he downloaded the information, or what Ubhi did with the information (for instance by obtaining Ubhi's laptop and conducting a forensic analysis—basic protocol where someone has improperly taken electronic information), and what steps DoD took to remove the information from Ubhi's laptop. Instead, the CO's investigation ignores this fact completely and states erroneously that "all of his access to JEDI Cloud information in Google drive" was immediately revoked on October 31, 2017. (Ubhi-No Impact Determination at 8-9.)

334. Similarly, despite his October 4 oral commitment to rejoin AWS, Ubhi throughout October 2017 set meetings with DoD insiders purportedly to obtain information on DoD constituent needs for use in structuring the JEDI acquisition. On October 6, 2017, Ubhi

[redacted]

traveled to SPAWAR for an internal meeting with Trudy Morgan about the tactical edge, whom Ubhi described as "schooling [him] on the tactical edge." (Tab 47c at 3172.) Ubhi messaged others at DDS about Morgan's "compelling takes on looking at hybrid options, i.e. Azure Stack." (*Id.* at 3174.) He added: "she says the tactical edge will always suffer from inconsistent comms, therefore hybrid solutions become essential, since they can work with NO comms." (*Id.*; *see also e.g.*, AR Tab 47c at 3168-69.) Ubhi participated in numerous other internal JEDI needs meetings during October 2017. (*See* AR Tab 47a at 2941 (Ubhi offering to "huddle" on technical requirements); *id.* at 2802 (Ubhi arranging a meeting with Air Force personnel); AR Tab 47b at 3065-75 (referencing Ubhi Navy JEDI meeting).)

335. Still further, during October 2017—under verbal commitment to rejoin AWS, Ubhi operated as the lead DDS advocate for a single source award—a position favored only by AWS among JEDI competitors. For instance, in an October 9th message among DDS team members, Woods indicated that Ubhi planned to attend the next CESG meeting to advocate for a single award approach: "Deap [Ubhi] has a specific way he wants to tackle this [one versus multiple providers] and will be attending in person for this purpose." (AR Tab 47c at 3181.) Ubhi attended the CESG meetings, including one held in mid-October 2017, arguing robustly for the single award approach favored by AWS. (AR Tab 78 at 5742:7-14.)

336. Still further, while under oral agreement to rejoin AWS, Ubhi worked on JEDI requirements and metrics and drafted and revised source selection documents. Ubhi drafted the "Problem Statement" for DoD leadership that "explains the problem we are solving with this initiative," including "why can't we solve the problem with multiple clouds," and "why is only one cloud a truly necessary requirement." (AR Tab 47b at 2986; *id.* at 2992.) Ubhi contributed to the Business Case Analysis. (AR Tab 21 at 399; AR Tab 78 at 5442:21-5443:6; *id.* at 5572:4-

[redacted]

11.) In late October 2017, Ubhi also revised the draft requirements document for the JROC and finalized the RFI. (*Id.* at 27 (¶ 95 iii).)

337. Also throughout October 2017—with the oral agreement to rejoin AWS in hand, Ubhi set up meetings and met with potential JEDI competitors as a DoD official, conducting "highly technical" meetings regarding anticipated offeror JEDI approaches and capabilities.

338. Of some note, AWS itself participated in a JEDI vendor meeting with DDS. On October 18, 2017, weeks after Ubhi verbally committed to rejoin AWS, Ubhi and Kasper held a one-on-one meeting with AWS. (*See e.g.*, AR Tab 34 at 696-97, 699, 714.) Despite that Ubhi and AWS had agreed on Ubhi returning to AWS and Ubhi obviously had not recused himself, again no one from AWS or Ubhi disclosed to DoD that AWS and Ubhi had an employment agreement.

339. On October 19, Ubhi and Kasper conducted a one-on-one JEDI meeting with Microsoft, during which Microsoft discussed extensive information "marked proprietary and confidential." (*Id.* at 19 (¶ 72.iii.); *see also* AR Tab 47a at 2787 (Microsoft); AR Tab 47c at 3102 ("All industry contacts that have been funneled to me have received a response."); AR Tab 78 at 5463:12-5464:11.)

340. On October 24, 2017, Ubhi and Kasper conducted a one-on-one JEDI meeting with VMWare. (Ubhi Mem. at 18 (¶ 72.ii.); AR Tab 47e at 3337.)

341. That same day, Ubhi allegedly had a telephone call with the AWS recruiter, during which Ubhi purportedly advised her that he must recuse himself from the DoD program he is working on and is precluded from working with the AWS public sector team. (Ubhi Mem. at 16 (¶ 65.h.).) The recruiter did not ask about the program, note the discrepancy with Ubhi's prior written submissions, or tell anyone else about Ubhi's restrictions. (AWS OCI Mem. at 4.)

[redacted]

Still neither Ubhi nor AWS advised DoD of the employment arrangement.

342. On October 25, 2017, three weeks after the oral commitment, AWS formalized its offer to Ubhi in writing. (Ubhi Mem. at 16 (¶ 65.i).)

343. On October 26, 2017, Ubhi and Kasper hold the one-on-one "highly technical" meeting with Google (another expected JEDI competitor) about its solution. (AR Tab 47e at 3740; Ubhi Mem. at 20 (¶ 72.v).)

344. On October 27, 2017, Ubhi returns the signed letter, formally accepting employment and receiving a substantial bonus. (*Id.* (¶ 66.ii).)

345. Still neither Ubhi nor AWS advised DoD of the employment discussions that had taken place across JEDI. Instead, evidencing knowledge that the foregoing misconduct violated the law, Ubhi, on October 31, 2018, fabricated a story about Amazon potentially renewing its offer to purchase Ubhi's company Tablehero:

> As per guidance from SOCO (Eric Rishel) and our in-house general counsel Sharon Woods, I am hereby recusing myself from the DDS's further involvement in facilitating SecDef and DSD'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....

(*See* AR Tab 45 at 2773-74.) AWS has admitted that no such communications took place regarding Tablehero in late 2018. (Dkt. 60-1 at 6 ("Those discussions concluded (with no deal and no future business relationship) in December 2016.... AWS does not know why Mr. Ubhi's October 2017 recusal letter references 'further partnership discussions' with Amazon.").)

346. The CO correctly finds that Ubhi's misconduct violated FAR 3.101. However, rather than analyze the facts against the conflict-of-interest proscriptions in 18 U.S.C. § 208 and its implementing regulations, the CO avoids the finding by asserting more investigation is

[redacted]

necessary and referring the matter to the DoD IG. (Ubhi Mem. at 14 (¶ 63).)

347. To be clear, Ubhi's conduct violates numerous federal procurement statutes and regulations besides FAR 3.101-1 and 18 U.S.C. § 208, though these violations are all that is required. For instance, Ubhi violated 41 U.S.C § 2103. The CO finds otherwise based on the flawed view that this prohibition applies only after potential competitors have submitted formal proposals. The CO's reading of 41 U.S.C. § 2103 and FAR 3.104-3(c) contravenes the statutory definition of procurement. 41 U.S.C. § 2101 ("federal agency procurement means the acquisition (by using competitive procedures and awarding a contract) of goods or services (including construction) from non-Federal sources by a Federal agency using appropriated funds."); *see also* 41 U.S.C. § 111 ("'procurement' includes all stages of the process of acquiring property or services, beginning with the process for determining a need for property or services and ending with contract completion and closeout").

348. Ubhi also failed to comply with FAR 3.104-3(b)—a provision the CO did not consider in her reassessment of Ubhi. FAR 3.104-3(b) prohibits a person, other than as provided by law, from "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." Applicable regulations required Ubhi to recuse himself from all matters involving AWS (including JEDI) while he was seeking employment with AWS, and certainly after he verbally committed to rejoin AWS. 5 C.F.R. §§ 2635.604, 607. There could be no doubt in Ubhi's mind about AWS' interest in JEDI. By late September 2017, AWS had already shown an interest in the JEDI acquisition to DDS and Ubhi. (AR Tab 34 at 697.)

349. Ubhi also violated FAR 3.104-3(c) requiring immediate notice to DoD and recusal when AWS contacted him during JEDI, regarding employment.

[redacted]

350. Further, contrary to the CO's "no impact conclusion," Ubhi's violation of the conflict-of-interest statutes and the procurement integrity provisions tainted the procurement and harmed the public trust requiring relief for Oracle. *Express One Int'l, Inc. v. United States Postal Service*, 814 F. Supp. 93, 98 (D.D.C. 1992) (sustaining protest: "The temptation to assist the source of future employment … is exactly the type of conflict of interest that statutes and ethical principles are designed to prevent."); *cf. Quinn v. Gulf and Western Corp.*, 644 F.2d 89, 94 (2d Cir. 1981) (ignoring a prohibited conflict would "equally require the court to sanction an 'infected bargain' and deny the public the protection from corruption among public officials granted by Congress.").

351. But under pressure to proceed with this significant procurement, the CO spins a different narrative that contradicts the facts and, in some cases, contradicts the CO's prior testimony. For instance, the CO's latest findings assert that Ubhi could not understand or contribute to the vendor meetings because Ubhi was a business person. (Ubhi Mem. at 18 (¶ 70).) The CO further concludes that Ubhi's misconduct could not have impacted the procurement because purportedly "Ubhi did not have the technical expertise to substantially influence the JEDI Cloud requirements" (*id.* at 24 (¶ 90)), or the "level of technical understanding necessary to make the case for some of the most important foundational decisions." (*Id.* at 24-25 (¶ 91).)

352. The CO's latest account directly contradicts testimony by the DDS Deputy Director and the CO during the GAO hearing. When asked whether Ubhi "biased anyone towards a single award decision," the Deputy Director testified: "It would be hard to say. Right, again, Deap is a technical expert. That's why he was hired on to the DDS team." (AR Tab 78 at 5445.) The CO also testified about Ubhi's technical expertise: "So following the Secretary's

[redacted]

memo, in mid-September, there was a lot of activity surrounding who would support these functions.... [T]he technical expert that was pegged to support this -- support aspects of this was Deap Ubhi." (*Id.* at 5571; *id.* at 5610 ("Based on his [Ubhi's] cloud expertise, when it became known that the Deputy Secretary wanted to make this initiative, they searched for somebody purposely for cloud expertise in order to come and consult with us on this, to get this right for the government.").)

353. The CO's latest narrative also contradicts the record showing that Ubhi drove the DDS technical decision to adopt a single award approach. For example, in a September 29, 2017 message to Ubhi, DDS counsel Sharon 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." (AR Tab 47c at 3114.)

354. The CO also seeks to downplay the effect of Ubhi actively and successfully seeking employment with AWS while serving on the team leading the acquisition, by interpreting each of his Slack messages to give Ubhi the benefit of every doubt and then some.[35] (Ubhi Mem. at 21-24 (¶¶ 78-89).) For instance, the CO interprets Ubhi's request to DDS counsel on September 25, 2017, within three days of AWS presenting Ubhi with a new opportunity at AWS, to make Ubhi the main point of contact for industry ("make it me"), as simply Ubhi purportedly thinking he was "better equipped to handle the industry capabilities meetings based on his skillset and expertise" over Daniel Griffin, the DDS Deputy Chief of Staff, "due to the general administrative nature of Mr. Griffith's position with DDS. (*Id.* at 23 (¶ 85).)

[35] Although many of Ubhi's messages attack government officials and other companies, the CO excuses Ubhi's "overall tone ... as being an attempt at humor while performing work tasks." (Ubhi Mem. at 22 (¶ 81).)

[redacted]

355. The CO's attempt to put a positive spin on each of Ubhi's Slack messages is not a valid reason for concluding that he had no bias in favor of AWS. The conflict of interest laws establish the bias by virtue of Ubhi engaging AWS for employment while serving on the JEDI acquisition team. The CO's contrary conclusions lack legal merit.

356. The CO also suggests that none of the information disclosed to Ubhi and Kasper during the industry meetings had competitive value, claiming that everything provided to Ubhi by AWS' competitors was high level, publicly available information. (Ubhi Mem. at 18-20 (¶ 72).) The record again contradicts the CO's characterization of the information shared by industry with Ubhi in any event. In fact, the record repeatedly refers to the meetings as "highly technical." (*See, e.g.*, AR Tab 78 at 5436:11-5437:3; *id.* at 5463:12-5464:11.)

357. A review of the standard questions asked to each vendor contradicts the CO's unsupported conclusion in any event. (*Id.* at Appx. I.) For instance, the last question DDS asked each vendor was "what is your biggest weakness and how are your working to improve in that area?" (*Id.*) None of the website links relied on by the CO discuss vendor weaknesses or how the vendor intends to address it weaknesses. (*See id.* at Appx. 2.)

358. Moreover, the CO acknowledges that various vendors provided material to DDS marked "proprietary". (*See e.g.*, *id.* at Appx. 3, pg. 7, 8.) Rather than engage with any of those companies whose information Ubhi improperly accessed to assess the reasons for the markings, the CO relies on the unsupported DDS judgments about the markings. For instance, DDS employee Kasper opines that Microsoft marked certain information proprietary simply "because it had Microsoft product names on it," and notes "those names could be swapped out for another vendor and the diagram would still be valid." (*Id.* at 7.)

[redacted]

359. Despite attempting to paint all vendor information Ubhi received as publicly available, Kasper nevertheless acknowledges certain cloud vendors provided proprietary, non-public information, noting e.g., "there are some minor business particulars that VMware may not want shared," but then inexplicably discounts the harm stating, without support, "it is unlikely that the information in this document would give a competitive advantage to any other vendor bidding on JEDI." (*Id.* at 10.) DoD does not explain the basis for such a conclusion.

360. The CO's reassessment also does not meaningfully consider the other nonpublic information which Ubhi accessed and contributed in his role as the JEDI PM. For instance, the CO dismisses the fact that Ubhi had access to the DoD user's individual needs, problems, and lessons because these meetings purportedly occurred before December 2017 when the JROC approved the warfighting requirements. (Ubhi Mem. at 20 (¶ 73); *see also id.* at 21 (¶ 75) ("Although Mr. Ubhi had access to information as a result of his attendance at the [JEDI Cloud] meetings that may be considered nonpublic information, it could not be considered completely useful because the acquisition was in its predecisional phase planning phase without any requirement document").) The CO's coupling of nonpublic information about the DoD's cloud needs as having competitive value only after a requirements document has been finalized lacks a rational basis. The information Ubhi accessed was JEDI source selection information. The CO even acknowledges that a draft "requirements" document existed while Ubhi led the procurement <u>and</u> that Ubhi revised the document, further undermining her stated rationale. (*Id.* at 27 (¶ 95.iii).)

361. The CO's tallying of purported edits made by Ubhi to Google drive documents that DoD previously claimed it could not produce also does not support the conclusion that Ubhi securing employment with AWS while leading the JEDI effort had no impact on the

[redacted]

procurement. (Ubhi Mem. at 25 (¶ 92).) The CO's determination does not explain how the CO chose the documents she reviewed (the Problem Statement, the RFI, Vendor Meeting Notes).[36] The CO did not attempt to identify and analyze all JEDI information that Ubhi created or accessed. It is also unclear how the CO determined what "input" Ubhi provided.

362. Despite knowing that Ubhi downloaded the Google drive to his laptop while working for DDS, the CO failed to acknowledge this happened or investigate it in any way. (*See* Dkt. No. 40-1, DOJ Opp. Appx., Kasper Decl. ¶ 11 ("I know that Mr. Ubhi synced Google Team Drives to his laptop while working for DDS").) Instead, the CO ignores this fact completely and states erroneously that "all of his access to JEDI Cloud information in Google Drive" was immediately revoked on October 31, 2017. (Ubhi-No Impact Determination at 8-9.)

363. Ubhi's conduct at issue here was brazen. After indicating to AWS that he wanted to rejoin the company, Ubhi participated personally and substantially in the JEDI procurement, by among other things, creating the problem statement for the Business Case, attending meetings with DoD entities and industry to gather information about needs and capabilities, helping draft requirements, while at the same time securing employment with AWS. AWS knew of his role in acquisition—he advised AWS officials that he was the "industry point of contract" and then met with the AWS JEDI Cloud team about their capabilities after accepting the informal AWS offer. After verbally committing to AWS, Ubhi met with other AWS competitors, advocating robustly for a single award approach, downloaded the entire repository of acquisition sensitive documents to his laptop, and continued to serve on the team leading the acquisition for nearly one month. The CO's dismissal of Ubhi's conduct because it happened during the first two months of the procurement renders the conflict-of-interest provisions meaningless.

---

[36] DDS has averred to this Court that any document uploaded to the Google drive would not evidence who created the document. (Dkt. 47-1 at 6.)

[redacted]

364. Finally, the CO's reliance on affidavits by Ubhi and AWS to conclude that Ubhi purportedly did not disclose any nonpublic competitively useful information in violation of FAR 3.104-3(a) also lacks a rational basis. (Ubhi Mem. at 16-17 (¶¶ 68, 69).)

365. Contrary to the CO claims that, given Ubhi's other misrepresentations, she "did not give much weight or credibility to the statements Mr. Ubhi provided in his declarations," the CO fully credits Ubhi on the material fact of whether he disclosed JEDI-related information to AWS. (*Compare* AWS OCI Mem. at 2 *with* Ubhi Mem. at 17 (¶ 68.i.).)

366. In fact, although [redacted] (Ubhi's [redacted]) averred that he never had any conversations with Ubhi about Ubhi's work at DoD or any particular restrictions, the CO "find[s] it credible that Mr. [redacted] was aware that Mr. Ubhi was precluded from working" with AWS public sector because Ubhi averred that he "informally firewalled himself by duly notifying his manager [redacted] that he should not be involved in JEDI Cloud activities because of potential conflict issues." (*Compare* AWS OCI Mem. at 3 *with* Ubhi Mem. at 6-7 (¶ 29).) The CO's decisions to credit Ubhi's self-serving statements despite inconsistent statements from his manager, lack a rational basis.

367. The CO also ignores inconsistencies between Ubhi and the AWS recruiter about Ubhi's post-government restrictions. These inconsistencies required reconciliation, not indifference by the CO. For instance, the CO relies on a Government Entity Questions Form apparently submitted in mid-October 2017, during which Ubhi falsely represented to AWS that to the best of his knowledge he did <u>not</u> have any employment restrictions "from handling any specific types of matters if employed by Amazon or its subsidiaries." (Ubhi Mem. at 10 (¶ 35).)

368. Yet, the CO also credits the affidavit of the AWS [redacted] Recruiter who avers that within a week of Ubhi submitting the false form claiming he had no restrictions, Ubhi

[redacted]

allegedly declared that he had to recuse himself from a program he worked on at the DoD and could not work with the AWS public sector team. (*Id.* at 16 (¶ 65.ii.h).) The recruiter never resolved Ubhi's directly conflicting statements about his post-government restrictions, and claims she never "asked for any detail, about the program that he was working on for DoD." (AWS OCI Mem. at 4.) And AWS never explained the discrepancy between Ubhi's no-restriction averment on the employment questionnaire and the recruiter's affidavit, including why AWS would proceed to hire someone that had made false statements on his Government Entity Question Form and why AWS did not contact DoD to address these inconsistencies. The CO did not seriously consider the glaring inconsistencies.

369. Nor did the CO ask what the recruiter did (if anything) to implement the restrictions Ubhi purportedly raised in late October 2017. Instead, the CO found that the "[b]est business practice would have been for [redacted] [the recruiter] to forward the information about Mr. Ubhi's preclusion to attorneys working with the AWS WWPS [AWS Public Sector group] to ensure this preclusion was known to both AWS's Commercial organization and AWS WWPS." (AWS OCI Mem. at 3-4.) Although AWS did not follow this best practice, the CO nevertheless deemed AWS' procedures "effective to maintain the integrity of the procurement process." (*Id.*) The CO does not explain the rationale for such a conclusion.

370. Notably, AWS did not take any formal firewall measures to prevent Ubhi from disclosing JEDI information until May 11, 2018, nearly six months after Ubhi joined AWS, when AWS purportedly sent around email notices to the JEDI Proposal team setting up "information firewall." (*Id.* at 2.) Alleged after-the-fact mitigation measures have no legal value as a matter of law. *See NetStar-1*, 101 Fed. Cl. at 528.

[redacted]

371. The CO did not investigate why AWS waited six months to institute a firewall between Ubhi and the JEDI proposal team, when Ubhi purportedly advised AWS' recruiter of his post-employment restrictions. To the contrary, the CO inaccurately characterized AWS' procedures as "proactive[]." (Ubhi Mem. at 6 (¶ 27).)

372. The CO's reliance on the belated firewalls also renders irrational the CO decision that Ubhi did not violate FAR 3.104-3(a) because the AWS firewall, as described by the CO, comprises no more than an email sent by AWS management directing individuals on the proposal team not to exchange information with Ubhi and to comply with AWS policy. (Ubhi Mem. at 17 (¶ 68.iii.).) "Such bare bone promises are a far cry from the detailed procedures, as well as physical and electronic barriers, that the decisional law have found adequate when timely implemented." *NetStar-1*, 101 Fed. Cl. at 529.

373. The CO did not investigate the interactions between each member of the JEDI proposal team and Ubhi prior to the firewall or confirm that the proposal team had not indirectly received nonpublic information from Ubhi.

374. For these reasons, the CO's determination that Ubhi's multiple and blatant violations of government ethics and procurement laws did not impact the JEDI acquisition is arbitrary, capricious, an abuse of discretion, and otherwise contrary to law.

375. These substantial improprieties in the procurement process caused severe competitive prejudice to Oracle, by depriving Oracle of its right to participate in a fair, lawfully executed procurement process.

WHEREFORE, Oracle requests that the Court declare the CO's no-impact determination irrational and enjoin DoD from awarding a contract under the RFP until DoD fully investigates

[redacted]

the Ubhi procurement improprieties and DoD mitigates the harm to Oracle and the procurement caused by Ubhi's misconduct.

COUNT VIII
The CO Irrationally Determined That [redacted] Misconduct Did Not Impact The JEDI Acquisition

376. Oracle incorporates paragraphs 1 through 375 of the Complaint by reference.

377. During JEDI, AWS hired [redacted], the former [redacted] of the Navy for [redacted], even though [redacted] participated in JEDI Cloud meetings both while seeking employment with AWS and after he accepted a position with AWS Public Sector as [redacted].

378. The CO found that [redacted] violated FAR 3.101-1 and possibly 18 U.S.C. § 208 and its implementing regulations by attending at least one JEDI Cloud meeting regarding the draft Acquisition Strategy in April 2018 after [redacted] had accepted an AWS offer to serve as the AWS Public Sector [redacted]. ([redacted] Mem. at 4.)

379. The CO nevertheless concluded that [redacted] unlawful conduct did not negatively impact JEDI. This determination lacks a rational basis.

380. Despite having accepted an offer from AWS to run its public sector business development and having been directed to recuse himself from all matters involving AWS, [redacted] participated in the source selection sensitive JEDI acquisition strategy meeting and then shortly thereafter moved to AWS with the information. (*Id.* at 3-4 (¶¶ 14, 16, 22-25).) The CO acknowledges that the information was source selection sensitive and improperly accessed by an individual under employment agreement with a known competitor. (*See id.*) Yet, the CO

[redacted]

errantly concludes that such misconduct did not impact JEDI. (*Id.* at 4.) The CO arrived at this legally and factually flawed conclusion without first conducting an adequate investigation.

381. A FAR 3.104-7 investigation such as the CO purports to have conducted requires consideration of "all information available." 48 C.F.R. § 3.104-7(b). The CO, nevertheless, did not interview [redacted], review his relevant emails, or work product. As a result, the CO's assessment lacks material facts.

382. The CO did not attempt to determine the scope of [redacted] JEDI related work. Instead, the CO based her conclusions on the two meetings "known by [her]," and relied on her personal knowledge to conclude that [redacted] "participation was limited to two meetings." ([redacted] Mem. at 3 (¶ 20).) But even a review of the current Ubhi emails produced by DoD evidence that [redacted] likely attended other JEDI meetings, including a Cloud Focus Session with Gartner, in November 2017. (*See* AR Tab 47a at 2837 (showing the meeting as initial schedule for Nov. 2, 2017); AR Tab 47a at 2846 (evidencing the meeting moved to Nov. 8, 2017).)

383. The CO also failed to consider all applicable legal standards. Although the CO acknowledged that [redacted] attendance at the April 2018 JEDI Cloud meeting discussing the draft acquisition strategy "may have constituted personal and substantial participation in the JEDI Cloud procurement ..., which may be a violation of 18 U.S.C. § 208," the CO did not consider whether [redacted] conduct also violated 41 U.S.C. § 2103 and its implementing regulations.

384. The CO also did not consider whether [redacted] earlier communications with AWS triggered recusal. According to AWS, from August 2017 to early 2018, [redacted] apparently engaged with an AWS recruiter, [redacted], and [redacted], the [redacted] at AWS, about his retirement and post-government plans. [redacted], however, did not recuse himself until January 11, 2018. ([redacted] Mem. at 3 (¶13).)

[redacted]

385. Of note, 5 C.F.R. § 2635.603(b)(1) defines "seeking employment" broadly to include an unsolicited communication regarding possible employment or a response, other than a rejection to an unsolicited communication regarding possible employment. "The term is not limited to discussions of specific terms and conditions of employment in a specific position." 5 C.F.R. § 2635.603(b)(1)(i). The CO's determination does not detail the substance of these material communications, and thus the CO cannot and did not determine whether [redacted] should have recused himself from JEDI before January 2018.

386. Moreover, based on the limited facts known by the CO, [redacted] violated FAR 3.104-3(b), which prohibits a person, other than as provided by law, from "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." Applicable regulations required [redacted] to recuse himself from all matters involving AWS (including JEDI) while he was seeking employment with AWS, and certainly after he accepted a position with AWS on April 2, 2018. 18 U.S.C. § 208; 5 C.F.R. §§ 2635.604, 607.

387. The findings made by the CO lack adequate support, and her reliance on AWS submissions misplaced because the CO knows those submissions are inaccurate and incomplete.

388. For instance, the CO relies on an affidavit from [redacted] submitted with AWS' proposal, in which he states, that he had no role in JEDI except a single meeting in "the first quarter of 2018" during which he "provided information on the Navy's experience with cloud services" and "input on a high-level strategy document for JEDI Cloud." ([redacted] Mem. at 3 (¶ 10).) The CO assumes the single meeting to which [redacted] refers is the October 2017 CESG meeting instead of the April 5, 2018 JEDI Cloud meeting because [redacted] states that the meeting "occurred before DoD issued any draft JEDI solicitation." (*Id.*) Whichever meeting [redacted]

[redacted]

intended to disclose (an issue the CO never resolved), it is clear that [redacted] initial affidavit was inaccurate based on the CO's own knowledge and the limited record already produced. [redacted] participated in multiple JEDI meetings.

389. [redacted] also apparently stipulated in his original affidavit that he "had no access to the DoD's acquisition plan, source selection procedures, or any other information that could provide a competitor an unfair advantage." (AWS OCI Mem. at 6 (¶ 9).) But the CO also know this statement to be false as [redacted] had access to the draft Acquisition Strategy, a document the CO acknowledges is nonpublic source selection information that has not been shared with any other offeror. ([redacted] Mem. at 4 (¶¶ 24-25).)

390. In addition, the CO's finding that [redacted] did not provide any inputs into or have access to nonpublic JEDI information (other than the draft Acquisition Strategy document) is incorrect (*id.* (¶ 26.b), because [redacted] own initial affidavit states otherwise, admitting [redacted] provided "input on a high-level strategy document for the JEDI Cloud." (*Compare* [redacted] Mem. at 4 (¶ 26.b) *with* AWS OCI Mem. at 6-7 (¶ 9).)

391. The AWS submissions also misreport that "[redacted] prior federal employment did not grant him access to nonpublic information about DoD's JEDI Cloud requirements." (AWS OCI Mem. at 5 (¶ 9)), which the CO knows to be false given [redacted] access to the draft Acquisition Strategy, nonpublic, completely-useful JEDI source selection sensitive information.

392. The CO also failed to consider whether [redacted] knowledge of the cloud computing needs and experiences of the Navy, an intended JEDI Cloud user, was nonpublic, competitively useful information as part of her review. The CO did not consider [redacted] former position as the [redacted] of the Navy for acquisitions at all. In this role, [redacted] served as the principal Navy advisor for the acquisition of [redacted], like JEDI.

[redacted]

393. AWS' description of its OCI mitigation plan efforts also raises more questions than it answers, yet the CO again failed to investigate and resolve the issues to protect the integrity of the procurement. For instance, although [redacted] started work at AWS in mid-June 2018, AWS apparently did not establish an email firewall between [redacted] and the JEDI proposal team until July 31, 2018. The CO did not investigate this delay nor determine the interactions between the JEDI proposal personnel and [redacted] prior to July 31, 2018.

394. Instead, the CO "determined it immaterial that the firewall notice was not sent until five days after [the Agency] published the JEDI Cloud RFP." (AWS OCI Mem. at 6.) The CO does not explain the basis for this conclusion.

395. The CO also determined that AWS' information firewall plan and procedure "were reasonable and effective to maintain the integrity of the acquisition process." (AWS OCI Mem. at 6.) The CO does not explain the basis for this conclusion either.

396. The CO's reliance on the belated firewall also renders irrational the CO decision that [redacted] did not violate FAR 3.104-3(a) because the AWS firewall, as described by the CO, comprises no more than an email sent by AWS management directing individuals on the proposal team not to exchange information with [redacted] and to comply with AWS policy. (AWS OCI Mem. at 5.) "Such bare bone promises are a far cry from the detailed procedures, as well as physical and electronic barriers, that the decisional law have found adequate when timely implemented." *NetStar-1*, 101 Fed. Cl. at 529.

397. The CO did not investigate the interactions between each member of the JEDI proposal team and [redacted] prior to the firewall or confirm that the proposal team had not indirectly received nonpublic information from [redacted].

[redacted]

398. In short, the CO failed to give serious consideration to whether [redacted] disclosed nonpublic, competitively useful information to AWS in violation of FAR 3.104-3(a).

399. The CO's failure to reasonably investigate and resolve the [redacted] conflict prejudices Oracle. *See Jacobs Tech. Inc. v. United States*, 100 Fed. Cl. 198, 213 (2011) (finding in a pre-award protest that the "failure to conduct additional OCI analysis" prejudiced the protester because absent an adequate analysis the protester "is not assured that it is competing on a level playing field").

WHEREFORE, Oracle requests that the Court declare the CO's [redacted] no-impact determination irrational and enjoin DoD from awarding a contract under the RFP until DoD properly investigates the [redacted] matter and mitigates the harm to Oracle and the procurement caused by [redacted] misconduct.

COUNT IX
DeMartino Violated The Conflict of Interest Regulations And The CO's No-Impact Determination Lacks A Rational Basis

400. Oracle incorporates paragraphs 1 through 399 of the Complaint by reference.

401. As noted, to maintain the integrity of the procurement system, FAR 3.101-1 mandates government business "be conducted in a manner above reproach, with complete impartiality and with preferential treatment for none," requires "an impeccable standard of conduct," and strictly prohibits even the appearance of conflicts of interest. 48 C.F.R. § 3.101-1.

402. 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 in the matter," absent appropriate authorization. 5 C.F.R. § 2635.502(a); 48 C.F.R. § 3.104-2.

[redacted]

403. Although the standard rule prohibits such involvement where a covered relationship exists for at least one year, 5 C.F.R. § 2635.502, Executive Order 13770 extends this restriction to two years where the individual serves as a political appointee. 82 Fed. Reg. 9333 (Jan. 28, 2017). These rules apply equally to former consultants. *See* 5 C.F.R. § 2635.502(b)(1)(iv).

404. DeMartino, previously the Chief of Staff for the Secretary and DSD and a former AWS consultant, served as a senior executive branch official, and was prohibited from participating personally and substantially on JEDI based on his prior consulting relationship with AWS. *K & R Eng'g Co.*, 616 F.2d at 472.

405. Indeed, due to financial ties with AWS, DoD's SOCO sent DeMartino an ethics letter in April 2017, warning him not to work on matters involving AWS without approval:

> This email is to alert you to and assist you in avoiding potential conflicts of interest between your duties as a Government official and your actual or imputed financial interests and affiliations... In this instance, you may have a regulatory prohibition under 5 C.F.R. §2635.502.... In particular, Amazon, Palantir and Bloomberg do business with DoD, and therefore, you should be vigilant and consult with our office before participating in any matters involving these entities until the one year period has expired.

(AR Tab 51 at 4345.)

406. DeMartino ignored SOCO's written direction and participated in JEDI from its inception without seeking SOCO's consent. (*See generally* AR Tab 51.) DeMartino, participated personally and substantially in the acquisition by, among other things, advocating procurement strategies, participating substantively in JEDI Cloud meetings and briefings, and editing official communications and other procurement-related documents.

407. More than eight months elapsed before DeMartino asked SOCO for guidance about his JEDI involvement, apparently in reaction to press FOIA requests questioning

[redacted]

DeMartino's role. (AR Tab 75 at 5233 (¶ 13).)[37] SOCO then instructed DeMartino to recuse himself immediately from JEDI in April 2018. (*Id.*)

408. The CO did not conduct the purported FAR 3.104-7 assessment until July 2018. (AR 33 at 685.)

409. The CO's assessment that DeMartino did not participate personally and substantially in JEDI (AR Tab 33 at 683) and that his involvement was "ministerial and perfunctory in nature" such that it did "not "negatively impact the integrity" of JEDI (*id.* at 685) lacks material facts and ignores contrary law.

410. For example, the CO did not undertake the necessary steps for such an assessment. The CO did not interview DeMartino, review his emails, or assess his work product. (AR Tab 78 at 5686:11-14; *id.* at 5695:2-9 ("I didn't investigate ... all of the emails and everything that he sent.... I wasn't aware of this ... article from anyone at Amazon.... I largely relied on conversations that I had with the DDS legal counsel who provided advice in concert with SOCO."); AR Tab 75 at 5239 (¶ 33 ("there are relatively few documents that I considered in my investigation").)

411. In testimony to GAO, the CO did not remember when, or exactly how, the issue of DeMartino's conflict of interest came to her attention. (AR Tab 78 at 5668:16-5669:5.) The CO had not even seen the prior ethics warning that SOCO issued to DeMartino prior to completing her investigation. (*Id.* at 5669:12-5670:13.) Yet, DeMartino's disregard of SOCO's instruction itself was improper. 5 C.F.R. § 2635.502(a).

---

[37] The documents released pursuant to this FOIA request reveal that DeMartino also engaged in questionable communications with AWS throughout his time at DoD and specifically regarding JEDI. *JEDI: Emails Between AWS and DoD Officials Reveal Questionable Judgment, Ethics Experts Say*, Capital Forum Vol. 6 dated August 17, 2018; *see also* AR Tab 51 at 4429.

[redacted]

412. The CO did not confer with SOCO (*id.* at 5675:4-8) or consider the materials that SOCO reviewed (if any) when SOCO directed DeMartino in April 2018 not to participate further in JEDI. (AR Tab 78 at 5674:1-5675:3). The CO conducted a perfunctory, "check-the-box" exercise insufficient to illuminate any conflict. *NetStar-1*, 101 Fed. Cl. at 521.

413. The CO based her no-impact determination on the mistaken assumption that "Mr. DeMartino worked with the SOCO throughout his DoD employment to ensure compliance with all applicable rules." (AR Tab 33 at 685.) But the record confirms that DeMartino did not follow SOCO's April 2017 direction, he ignored it until FOIA requests arrived. (AR Tab 51 at 4345; AR Tab 75 at 5233 (¶ 13).)

414. Contrary to the CO's unsupported findings, the record makes clear that DeMartino did not perform "ministerial and perfunctory" activities.[38] The record (largely unreviewed by the CO) evidences that DeMartino participated personally and substantially in (and impacted) JEDI. DoD concedes that the DSD, on whose behalf DeMartino oversaw JEDI, participated "personally and substantially." (AR Tab 64 at 4862.) As the Chief of Staff for the organization driving DoD's cloud strategy, DeMartino shaped JEDI from a policy level all the way down to specific details regarding the acquisition. DeMartino obtained and edited JEDI briefings on behalf of the Secretary of Defense and DSD, directed JEDI activities, and participated in JEDI strategy meetings that discussed the Acquisition Strategy, Security Strategy, Business Case, and the single award approach.

415. DeMartino also directed efforts and strategized as to the most likely way to garner approval for the single source approach. (AR Tab 51 at 4366-67 ("I would nuance this with the language about single 2 year award and that there are going to [sic] OPPORTUNITIES for other

[38] DoD has not produced, and the CO never reviewed, the purported notes taken by DeMartino.

[redacted]

companies to compete for other awards later in the lifecycle.").)

416. DeMartino coordinated with DoD's Cost Assessment and Program Evaluation office to obtain information to support projected savings from the single source acquisition approach, among other data. (*Id.*)

417. DeMartino commented on the JEDI industry day briefing and coordinated and shaped the press strategy for JEDI. (*Id.* at 4402, 4404; AR Tab 47f at 3831; *id.* at 3880; AR Tab 47e at 3319.)

418. DeMartino received and commented on JEDI acquisition sensitive information. (*See* AR Tab 47e at 3310, 3315-16.) DeMartino also almost certainly met and substantively discussed JEDI with the DSD routinely. But since the CO neither interviewed DeMartino nor anyone else, the scope of such communications is unknown.

419. The FAR makes clear that "[p]articipation may be substantial even though it is not determinative of the outcome of a particular matter," and that "the single act of approving or participating in a critical step may be substantial." 48 C.F.R. § 3.104-1. OGE opinions also are instructive in showing DeMartino participated "personally and substantially" in JEDI, and indicate that a wide variety of activities qualify, including advocating for the acceptance of a program plan,[39] and reviewing recommendations and issuing communications,[40] all of which DeMartino did. Given the CO's findings regarding [redacted] participation in the April 2018 meeting DeMartino's participation is plainly personal and substantial.

420. Despite that Oracle raised each of these issues prior to the CO's conflict

[39] OGE Opinion 96 x 21, Nov. 5, 1996, at https://www.oge.gov/Web/OGE.nsf/All+Advisories/0DBDD3F25EB8971885257E96005FBE98/$FILE/b491b2086be74d4791507906d501ef3c3.pdf?open (last visited 4/26/19).

[40] OGE Opinion 83 x 12, Aug. 3, 1983, at https://www.oge.gov/web/oge.nsf/Legal%20Advisories/486F71347E36660185257E96005FBBE0/$FILE/8a664c07fd4040008b68a00b4a4f30795.pdf?open (last visited 4/26/19).

[redacted]

reassessment, the CO did not remedy the legal and factual errors in her July 2018 no-impact assessment with regard to DeMartino. The CO did not consider DeMartino's conduct in her April 2019 reassessment at all.

421. Had the CO reasonably investigated DeMartino's conflicts and JEDI involvement, the CO would have found that DeMartino personally and substantially participated in the acquisition in violation of FAR 3.101-1, the ethics rules, and SOCO's express direction—all to the detriment of the public's trust in the JEDI procurement.

422. The CO's failure to reasonably investigate and resolve the DeMartino conflict prejudices Oracle. *See Jacobs Tech. Inc.*, 100 Fed. Cl. at 213 (finding in a pre-award protest that the "failure to conduct additional OCI analysis" prejudiced the protester because absent an adequate analysis the protester "is not assured that it is competing on a level playing field").

WHEREFORE, Oracle requests that the Court declare the CO's no-impact determination irrational and enjoin DoD from awarding a contract under the RFP until DoD properly mitigates the harm to Oracle and the procurement caused by DeMartino's unlawful misconduct.

COUNT X
The CO's Determination That AWS Did Not Violate The Procurement Integrity Act And That AWS Does Not Have An Unfair Advantage Caused By Its Hiring Of Multiple Former Government Cloud-Related Employees During JEDI Lacks A Rational Basis

423. Oracle incorporates paragraphs 1 through 422 of the Complaint by reference.

424. The record now establishes that AWS: (i) hired at least two JEDI officials during the procurement; (ii) AWS did not notify DoD of its employments communications with either official; (iii) AWS did not request ethics letters from either official; (iv) both officials failed properly to recuse themselves from JEDI—violating by DoD admission at least FAR 3.101-1 and potentially 18 U.S.C. § 208 and related regulations; (v) both officials had access to nonpublic, competitively useful inside JEDI information; and (v) AWS failed to set up timely, adequate

[redacted]

firewalls to prevent misuse of JEDI information. The record and procurement law require AWS' exclusion.

425. Maintaining the integrity of the federal procurement system takes on particular importance where a contractor hires a federal employee involved with a procurement. Indeed, numerous FAR provisions require both the contractor and federal employee to maintain particular vigilance in such circumstances. *See, e.g.*, 48 C.F.R. §§ 3.104-2(b)(2), 3.104-3(c), 3.104-5, 3.104-8(b). To that end, "where a firm may have gained an unfair competitive advantage through its hiring of a former government official, the firm can be disqualified from a competition based upon the appearance of impropriety which is created by this situation, even if no actual impropriety can be shown...." *Int'l Res. Grp.,* B-409346.2 *et al.*, Dec. 11, 2014, 2014 CPD ¶ 369 (sustaining protest where "former [agency] director potentially had access to competitively useful non-public information, and the record shows that the CO failed to analyze the full extent of the former director's involvement in the procurement.").

426. Further "[a] long line of cases holds that when a potential significant OCI is identified, prejudice stemming from that OCI is presumed." *NetStar-1*, 101 Fed. Cl. at 529. "Thus a protester need not show that the persons who drafted an offeror's proposal were actually in possession of proprietary information [or procurement sensitive information], but merely must show that the information was accessible to those employees and that the potential OCI created by that access has not been avoided for adequately mitigated." *Id.* "Nor must a protester ... show that the information possessed by its competitor specifically benefitted the latter's proposal. That too is presumed." *Id.* (internal citation omitted); *Dell Servs. Fed. Gov't, Inc.*, B-414461.3 *et al.*, June 19, 2018, 2018 CPD ¶ 213 ("once it has been determined that an actual or potential OCI exists the protester is not required to demonstrate prejudice; rather, harm from the conflict is

[redacted]

presumed to occur"); *Int'l Res. Grp., B-409346.2 et al.*, Dec. 11, 2014, 2014 CPD ¶ 369 ("An unfair competitive advantage is presumed to arise where an offeror possesses competitively useful non-public information that would assist that offeror in obtaining the contract, without the need for an inquiry as to whether that information was actually utilized by the awardee in the preparation of its proposal.").

427. Under the facts about Ubhi's employment contacts with AWS, as even described by AWS, Ubhi was an official subject to the restrictions in FAR 3.104-3 in late September 2017 when AWS engaged Ubhi about rejoining AWS.

428. AWS also knew that Ubhi did not reject the employment offer or recuse himself as required by FAR 3.104-3(c)(1). Instead, after verbally committing to AWS on October 4 and submitting his application on October 17, Ubhi as JEDI PM and industry point of contact, met with AWS regarding the DoD Cloud Memo (i.e., JEDI) on October 18, 2017. (*See e.g.*, Tab 34 at 696-97, 699, 714.)

429. Thereafter, on October 25, 2017—the same day AWS extended its formal offer to Ubhi, the AWS JEDI team emailed Ubhi and DDS JEDI colleagues Jordan Kasper and Alex Romero, encouraging them to attend the AWS "re:invent" event for potentially helpful "tech deep dives, customer success stories/use cases, and new service rollouts." (AR Tab 47a at 2784.) The AWS email acknowledged that Ubhi, Kasper, and Romero would be "restricted in terms of how [they] can interact with the AWS team directly," indicating AWS had emailed Ubhi in his capacity as a JEDI team member. (*Id.*) Moreover, the AWS email copied [redacted]—who [redacted], indicating that AWS management knew of and sanctioned this outreach to the Ubhi. (*See* AR Tab 122 ([redacted] leading AWS team in JEDI Q&A session).)

[redacted]

430. These record facts show that AWS knew both that AWS had extended an employment offer (indeed Ubhi had accepted the offer informally by October 4) and that Ubhi had not recused himself from JEDI. AWS also knew that Ubhi was operating as the industry point of contact gathering competitors' information as well. FAR 3.104-8(b) required AWS to notify DoD: "An offeror who engages in employment discussion with an official subject to the restrictions of 3.104-3, knowing that the official has not complied with 3.104(c)(1), is subject to the criminal, civil, or administrative penalties set forth in 41 U.S.C. 2105."

431. Here, AWS did not merely know of its offer to Ubhi and Ubhi's failure to recuse himself from JEDI—AWS continued to leverage Ubhi as a JEDI Official even after extending an offer of employment to Ubhi.

432. But AWS' complicity in Ubhi's acknowledged misconduct is hardly the only problem for AWS. AWS' pervasive employment discussions and hiring of JEDI officials, without notice to DoD, and without adequate firewalls has created an unmitigable unequal access OCI for AWS. Indeed, the record also makes clear that AWS failed to take the necessary steps to firewall Ubhi and [redacted] fully and adequately when they joined AWS and the CO's suggestion to the contrary contradicts existing law.

433. Notwithstanding AWS' misconduct and the legal presumption that the hiring harmed the JEDI competitors, on or about April 9, 2019, the CO determined that AWS' employment of Ubhi, [redacted], [redacted], and [redacted], all former government officials involved in the JEDI effort or other DDS cloud-related efforts, did not create an unfair competitive advantage under FAR Subpart 3.1 or FAR 9.500. (AWS OCI Mem. at *passim*.) The CO erred.

434. Whether an offeror has obtained an alleged unfair competitive advantage based on the hiring of a former government official and that official's knowledge of non-public

[redacted]

information, depends on a variety of factors, including whether the individual had access to nonpublic information not otherwise available to the other competitors and whether that information had competitive value. *See e.g., Health Net Fed. Servs., LLC*, B-401652.3, B-401652.5, Nov. 4, 2009, 2009 CPD ¶ 220 (sustaining protest).

435. First, even though the CO failed to investigate the extent of [redacted] nonpublic competitive useful information, the CO concedes that [redacted] had nonpublic competitively useful information not known by the other offerors in the form of the draft Acquisition Strategy. ([redacted] Mem. at 4 (¶¶ 24-26).)

436. The CO nevertheless determines that [redacted] did not in fact provide any nonpublic information to AWS based on affidavits from [redacted], [redacted], and [redacted], and the OCI Mitigation Plan submitted by AWS. (AWS OCI Mem. at 4.)

437. The CO's reliance on the self-serving and incomplete AWS affidavits and AWS' belated and incomplete mitigation procedures fails under procurement law for several reasons.

438. As previously discussed, the CO knows that the affidavit submitted by [redacted] was inaccurate. For example, [redacted] averred in his original affidavit that he "had no access to the DoD's acquisition plan, source selection procedures, or any other information that could provide a competitor an unfair advantage." (AWS OCI Mem. at 6 (¶ 9).) But the CO knew this statement was inaccurate given that she attended the JEDI Cloud meeting with [redacted] during which the participants discussed the source selection sensitive, draft acquisition plan. Significantly, the CO determined this much without conducting any search of the JEDI records related to [redacted].

439. The CO's reliance on the AWS' Mitigation Plan as related to [redacted] is equally baseless. For instance, AWS' email firewall incorrectly states that [redacted] prior federal

[redacted]

employment did not grant him access to nonpublic information. (*Id.*) In addition, AWS did not firewall [redacted] from the AWS proposal until more than one month after [redacted] joined AWS as a [redacted]. (*Id.*) AWS also did not timely notify DoD so that DoD could monitor the firewall. (*Id.*) And, the belated firewall itself was inadequate, consisting of nothing more than an email notice to [redacted] and the JEDI Proposal Team. *NetStar-1*, 101 Fed. Cl. at 526 ("Such bare bone promises are a far cry from the detailed procedures, as well as physical and electronic barriers, that the decisional law have found adequate to mitigate 'unequal access to information' conflicts.")

440. This Court also likewise has rejected as arbitrary and capricious a CO's reliance on such declarations from the party engaged in the misconduct:

> Can it be that the drafters of the FAR dedicated a whole subpart's worth of guidance to how and when to identify such conflicts, as well as how and when to mitigate the conflicts so identified, yet subscribed to the notion that the failure to follow these procedures could be cured by having the awardee swear up and down it did nothing improper? Of course not. As this court stated in granting plaintiff's motion for preliminary injunction, "if the latter were enough, one must wonder why the drafters of the FAR bothered to develop an extensive set of rules to deal with such conflicts...."

Id. (citation omitted.)

441. The CO's assertion that AWS' hiring of Ubhi likewise did not create an unfair competitive advantage for AWS fails for similar reasons.

442. Contrary to the CO's unsupported findings, the record confirms that Ubhi had unrestricted access to nonpublic competitively useful information about DoD's cloud computing needs and commercial cloud vendor capabilities.[41] Ubhi met with and obtained nonpublic

[41] Gate Criterion 1.1 provides and one example regarding the value of metrics information known to Ubhi. DoD seeks to defend its arbitrary January-February 2018 timeframe, claiming that this timeframe prevented potential competitors from gaming the criteria because they did not know the measurement timeframe before the March 2018 draft RFP. According to DoD, an

[redacted]

information from DoD officials regarding JEDI. Ubhi met with and obtained nonpublic information from vendors regarding their proprietary, anticipated JEDI solutions. Ubhi participated in setting the metrics and requirements. Ubhi even synched the entire Google Drive, the central repository for all JEDI information to his laptop while working for DDS, and the CO never investigated what happened to this information.

443. AWS' hiring of Ubhi during the procurement resulted in an unfair competitive advantage for AWS.

444. The CO's reliance on the Ubhi and AWS statements that they did not misuse the non-public competitively useful information known to Ubhi was arbitrary and capricious

445. The Ubhi and AWS affidavits are rife with inconsistencies.

446. For instance, the AWS [redacted] Recruiter avers that within a week of Ubhi submitting the false Government Entity Questions Form claiming he had no restrictions, Ubhi verbally declared to the recruiter that he had to recuse himself from a program he was working on at the DoD and was precluded from working with the AWS public sector team. (*Id.* at 16 (¶ 65.ii.h).) The recruiter never addressed Ubhi's directly conflicting statements about his post-government restrictions, and claims she never "asked for any detail, about the program that he was working on for DoD." (AWS OCI Mem. at 4.)

447. The CO never inquired about what the recruiter did (if anything) to implement the restrictions Ubhi purportedly verbally raised in late October 2017, or why she did not ask the name of the program or further address the matter. Instead, the CO found that the "[b]est business practice would have been for [redacted] [the recruiter] to forward the information

---

offeror who knew that DoD would use such measurements as gates could easily manufacture numbers meeting the criteria. Ubhi was involved in setting the metrics. No formal firewall existed at AWS for six months after Ubhi arrived consequently the law presumes that AWS alone among the competitors knew this information.

[redacted]

about Mr. Ubhi's preclusion to attorneys working with the AWS WWPS [AWS Public Sector group] to ensure this preclusion was known to both AWS's Commercial organization and AWS WWPS." (AWS OCI Mem. at 3-4.) Although AWS did not follow this best practice, the CO nevertheless deemed AWS' procedures "effective to maintain the integrity of the procurement process." (*Id.*) The CO does not explain the rationale for such a non sequitur.

448. Ubhi's manager claimed that he too never had any conversations with Ubhi about Ubhi's work at DoD or any particular restrictions. (*Compare* AWS OCI Mem. at 4.) But the CO somehow concludes that the manager's knowledge about Ubhi's work on JEDI and any restrictions lack relevance to her determination because the manager purportedly did not assign Ubhi to any public sector work. (*Id.*)

449. Notably, AWS took no affirmative measures to prevent Ubhi from disclosing JEDI information until May 11, 2018, nearly six months after Ubhi joined AWS, and then only sent around email notices to the JEDI Proposal team setting up an "information firewall." (AWS OCI Mem. at 2.) Such measures, implemented long after Ubhi actually joined AWS, are far too little, far too late. *See NetStar-1*, 101 Fed. Cl. at 528 ("remedies adopted after-the-fact cannot be effective if they look only forward and fail adequately to address unequal access problems that have occurred in the past."). This Court has rejected such paper promises directing AWS employees not to share competitively information and to follow AWS' OCI rules as inadequate methods to mitigate an unfair competitive advantage. *See NetStar-1*, 101 Fed. Cl. at 526 & n.19.

450. The CO did not investigate why AWS waited six months to institute an inadequate firewall between Ubhi and the JEDI proposal team, when Ubhi purportedly advised AWS' recruiter of his post-employment restrictions with the AWS public sector.

[redacted]

451. Inexplicably, the CO inaccurately characterized AWS' actions as "proactive[]." (Ubhi Mem. at 6 (¶ 27).)

452. The CO also did not investigate the interactions between each member of the JEDI proposal team and Ubhi or confirm that the proposal team had not indirectly received nonpublic information from Ubhi.

453. In short, the CO failed to give serious consideration to whether Ubhi possessed nonpublic, competitively useful information to AWS and disclosed that information to AWS. Instead, the CO relied on self-serving, post-hoc declarations by AWS employees. *NetStar-1*, 101 Fed. Cl. at 526.

454. The CO's consideration of whether AWS' hiring of [redacted], a former DDS engineer to the [redacted], and [redacted], who participated on JEDI for the JCS office, also are incomplete. For example, with regard to [redacted], the CO asked three limited questions: (i) his start date at AWS, (ii) whether AWS asked that he provide nonpublic information about the JEDI Cloud or DoD's cloud service needs <u>during his employment negotiations</u>, and (iii) whether prior to his employment with AWS, anyone from AWS asked him for nonpublic information about the JEDI Cloud requirement. (AWS OCI Mem. at 7.)

455. Because [redacted] left DDS on September 1, 2017, before the DSD issued the Cloud Memorandum, the CO determined that [redacted] participation on the AWS [redacted] created no issue. Absent from the CO's analysis and investigation was whether [redacted] had any nonpublic information about DoD's cloud service needs when he left DDS and joined AWS that would provide AWS a competitive advantage in this procurement. Without answering these basic questions, the CO could not reasonably determine whether AWS' hiring of [redacted] gave AWS an unfair competitive advantage.

[redacted]

456. The CO's investigation into whether AWS' hiring of [redacted] creates an unfair competitive advantage was likewise unreasonable. The CO's finds that the only nonpublic JEDI information that [redacted] accessed was "drafts of the JROCM." (AWS OCI Mem. at 8.) But the CO acknowledges that [redacted] also attended initial meetings at the Cloud Cybersecurity Working Group and that the [redacted] provided bi-weekly updates to the Vice Chief JCS regarding the status of the JEDI Cloud through April 2018, when a new staff member took over cloud efforts. (*Id.* at 7.)

457. It also is unclear the mitigation efforts AWS promised to implement when. [redacted] starts work there, if any. Instead, it appears that [redacted] or [redacted] have stated "[redacted] will not and would not work on [AWS]'s JEDI Cloud proposal effort." (*Id.* at 8.)

458. AWS has given the CO no reason to trust the integrity of this procurement to AWS. AWS not only remained silent about Ubhi's misconduct prior to Ubhi rejoining AWS, but AWS also reluctantly and incompletely discussed Ubhi's misconduct thereafter. The redacted GAO decision, made publicly available November 19, 2018, confirms that DoD's position on Ubhi's conflict and the GAO decision were based on misrepresentations regarding the Ubhi relationship with AWS. As relevant here, the redacted GAO decision excerpts the CO's memorandum regarding conflicts of the Digital Service Expert from DDS, revealing the CO's flawed misunderstanding that: "In late October 2017, AWS expressed an interest in purchasing a start-up owned by [the Digital Service Expert]...." *Oracle Am., Inc.*, B-416657 *et al.*, Nov. 14, 2018, 2018 CPD ¶ 391.

459. AWS thus knew as of November 19, 2018 that Ubhi had misrepresented his relationship with AWS to DoD, and that the CO relied on that misrepresentation in finding no

[redacted]

impact to the procurement, but AWS did not seek to "clarify" this misrepresentation until February 12, 2019—months into the Court of Federal Claims litigation.

460. Even if AWS did not read the GAO's redacted decision, Oracle filed its redacted Complaint on December 10, 2018. The redacted Complaint revealed publicly AWS' conflict of interest allegations, the full Contracting Officer's ethics memorandum, and the basis for Ubhi's recusal. (ECF No. 13 at 42-44, 83-91, n.21.) AWS had the December 10, 2018 redacted Complaint in its possession a full two months before AWS finally informed DoD (and, indirectly, DOJ, Oracle, and the Court) that DoD's then-public conflicts memorandum, as well as Ubhi's recusal letter, contained false information regarding Ubhi and AWS.

461. And, even when AWS belatedly raised Ubhi's misrepresentation to the CO in February 2019, AWS only told half-truths, disclosing that AWS and Ubhi began employment discussions in "late September 2017". (Dkt. 60-1 at 6.) Conversely, after questions by the CO, AWS provided emails showing that AWS and Ubhi had recommenced employment discussions as early as August 2017.

462. Oracle suffered prejudice as a result of the CO's flawed determination which allows AWS the fruits of its persistent improper hiring of JEDI officials and AWS' failure to timely disclose such actions. In a fair and lawful competition, Oracle would have a substantial chance for a JEDI contract award.

WHEREFORE, Oracle requests that the Court declare the CO's investigation into AWS' employment negotiations with JEDI officials and hiring of such officials has yielded AWS an unfair competitive advantage, either find AWS ineligible based on the existing known conduct or remand the matter for further investigation, and enjoin DoD from making award under the RFP

[redacted]

until DoD resolves the unfair competitive advantage and mitigates the associated impact to this tainted procurement.

VII. PRAYER FOR RELIEF

Oracle, accordingly, respectfully requests that this Court:

A. Issue the declaratory and injunctive relief set forth above; and

B. Provide such other and further relief as the Court deems just and proper.

Dated: April 26, 2019

Respectfully Submitted,

ARNOLD & PORTER KAYE SCHOLER LLP

/s/ Craig A. Holman

Craig A. Holman
601 Massachusetts Ave., N.W.
Washington, D.C. 20001
Phone: (202) 942-5722
Fax: (202) 942-5999

Attorney of Record for Oracle America, Inc.

Of Counsel:

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

[redacted]

CERTIFICATE OF SERVICE

I hereby certify that on this 26th day of April 2019, I caused a true and correct copy of the foregoing Supplemental Complaint to be served by electronic delivery on:

William P. Rayel
U.S. Department of Justice
Post Office Box 480
Ben Franklin Station
Washington, D.C. 20044
Telephone: (202) 616-0302
Facsimile: (202) 307-0972
E-mail: William.Rayel@usdoj.gov

Counsel for Defendant

Daniel R. Forman
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2595
Telephone: (202) 624-2504
Facsimile: (202) 628-5116
E-mail: dforman@crowell.com

Counsel for Defendant-Intervenor

/s/ Craig A. Holman