In the United States Court of Federal Claims

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

* *

ORACLE AMERICA, INC.,

Plaintiff,

v.

THE UNITED STATES,

Defendant,

and

AMAZON WEB SERVICES, INC.,

Intervenor.

* *

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

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

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

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

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

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

OPINION

BRUGGINK, *Judge*.

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

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

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

BACKGROUND

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

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

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

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

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

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

Early Commitment to a Single Award and Tailored Acquisition Plan

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Development of the Tailored Solicitation Approach and Needs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

AR 422.

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

CO's Justification of Single Award Approach

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

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

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

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

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

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

The Under Secretary's Justification of Single Award Approach

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

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

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

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

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

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

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

> unclassified services shall not be higher than the price that is publicly-available in the commercial marketplace in CONUS, plus any applicable discounts, premiums or fees . . . .
>
> > a. New services that are proposed to be incorporated into the contract in advance of availability to the commercial marketplace may potentially be considered a noncommercial item. The JEDI Cloud Contracting Officer will make a fact specific commerciality determination. If the new service is not a commercial item and no other exception or waiver applies, the JEDI Cloud Contracting Officer may require certified cost and pricing data or other than certified cost and pricing data under FAR Subpart 15.4 to make a fair and reasonable price determination.
> >
> > > i. If there are any new fees associated with a new service that is proposed to be incorporated into the contract in advance of availability to the commercial marketplace, the new proposed fee must be provided to the JEDI Cloud Contracting Officer for review and, if appropriate, approval and incorporation into the contract.
>
> 4. The price incorporated into the JEDI Cloud catalog for new classified services may include a price premium as compared to unclassified services because of the additional security requirements. . . .

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

Section H3 provides:

> 1. Within 45 calendar days of the Contractor lowering prices in its publicly-available commercial catalog in CONUS, the Contractor shall submit a revised catalog for incorporation into Attachment J-1, Price Catalogs as follows:
>
> > a. For unclassified services, the revised catalog price shall match the commercially lower price.
> > b. For classified services, the revised catalog price shall be lowered by to be completed by Offeror percentage of

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

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

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

JEDI Cloud RFP

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

year option period.

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

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

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

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

offline across the 2 months.

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

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

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

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

AR 792.

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

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

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

Post-Solicitation Events

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

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

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

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

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

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

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

]

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

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

Conflicts of Interest Relating to the JEDI Cloud Procurement

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

Tony DeMartino

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

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

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

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

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

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

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

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

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

Deap Ubhi

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

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

Id.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

Victor Gavin

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

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

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

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

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

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

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

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

Organizational Conflict of Interest

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DISCUSSION

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

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

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

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

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

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

As discussed in the background, two single award determinations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> work at a reasonable price to the government; or
>
> (D) because of exceptional circumstances, it is necessary in the public interest to award the contract to a single source.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IV. Gate Criteria 1.2 Is Enforceable.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

V. The CO Rationally Set The Competitive Range.

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

established a range of all four offerors.

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

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

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

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

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

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

1. Individual Conflicts of Interest

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

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

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

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

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

A. Mr. DeMartino

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

B. Mr. Gavin

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

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

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

C. Mr. Ubhi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Alleged Organizational Conflict of Interest

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION

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

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