

**IN THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST**

AMAZON WEB SERVICES, INC.,

Plaintiff,

v.

UNITED STATES OF AMERICA,
by and through the U.S. Department of Defense,

Defendant,

and

MICROSOFT CORPORATION,

Defendant-Intervenor.

Case No. 19-cv-01796

Judge Campbell-Smith

[REDACTED]

FINAL REDACTED VERSION

**PLAINTIFF'S [REDACTED] MEMORANDUM IN SUPPORT OF ITS MOTION FOR A
TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION**

[REDACTED]

TABLE OF CONTENTS

INTRODUCTION 1

QUESTION PRESENTED 7

STATEMENT OF THE CASE 7

ARGUMENT 9

 I. AWS HAS SHOWN A LIKELIHOOD OF SUCCESS ON THE MERITS. 10

 A. Egregious Evaluation Errors with Respect to Factors 5, 8, and 3
 Unfairly Tilted the Source Selection in Microsoft’s Favor. 10

 1. DoD Misedevaluated Microsoft’s Technical Approach for Price
 Scenario 6. 11

 2. DoD Ignored Microsoft’s [REDACTED]
 [REDACTED] under Factor 8. 17

 3. DoD’s Evaluation of the Offerors’ Tactical Edge Devices Was
 Unreasonable and Plagued by Disparate Treatment. 26

 B. Additional Serious Evaluation Discrepancies Minimized AWS’s
 Technical Superiority. 35

 1. DoD Improperly Minimized the Cloud Security Benefits of AWS’s
 Nitro Hypervisor. 36

 2. DoD Misedevaluated AWS’s Third-Party Marketplace Offerings
 Based on Misleading and Unequal Discussions. 42

 C. DoD Misedevaluated the AWS and Microsoft Proposals in a Host of
 Other Ways. 45

 1. DoD Removed Previously Recognized Strengths Only from
 AWS’s Final Evaluation. 46

 2. AWS Deserved Several Additional Strengths for Exceeding
 Demonstration Requirements. 47

 3. DoD Unreasonably Evaluated the Offerors’ Management
 Approaches. 48

 II. THE REMAINING INJUNCTIVE FACTORS ALL FAVOR AWS. 50

- A. Continued Performance of the JEDI Contract Will Result in Immediate and Irreparable Harm to AWS 52
- B. The Balance of Hardships Favors Granting Injunctive Relief..... 54
- C. Injunctive Relief Is in the Public Interest. 58

CONCLUSION AND PRAYER FOR RELIEF 59

TABLE OF AUTHORITIES

Cases

BayFirst Sols., LLC v. United States,
102 Fed. Cl. 677 (2012)10

Bilfinger Berger AG Sede Secondaria Italiana v. United States,
97 Fed. Cl. 96 (2010)57

Cherokee Nation Techs., LLC v. United States,
116 Fed. Cl. 636 (2014)58

Cigna Gov’t Servs., LLC v. United States,
70 Fed. Cl. 100 (2006)53

FCN, Inc. v. United States,
115 Fed. Cl. 335 (2014)52

FMC Corp. v. United States,
3 F.3d 424 (Fed. Cir. 1993).....9

FMS Inv. Corp. v. United States,
136 Fed. Cl. 439 (2018)9, 10

GTA Containers, Inc. v. United States,
103 Fed. Cl. 471 (2012)57

Heritage of Am., LLC v. United States,
77 Fed. Cl. 66 (2007)52

HP Enter. Servs., LLC v. United States,
104 Fed. Cl. 230 (2012)51, 59

Oracle Am., Inc. v. United States,
144 Fed. Cl. 88 (2019)56

Palantir USG, Inc. v. United States,
1299 Fed. Cl. 218 (2016)54

Palladian Partners, Inc. v. United States,
119 Fed. Cl. 417 (2014)52

PGBA, LLC v. United States,
57 Fed. Cl. 655 (2003)58



Reilly's Wholesale Produce v. United States,
73 Fed. Cl. 705 (2006)55

Serco, Inc. v. United States,
101 Fed. Cl. 717 (2011)9

Veterans Contracting Grp., Inc. v. United States,
133 Fed. Cl. 613 (2017)10

Statutes

28 U.S.C. § 1491(b)(4)10

INTRODUCTION

Plaintiff Amazon Web Services, Inc. (“AWS”) requests that the Court issue a temporary restraining order and preliminary injunction, ordering Defendant United States, by and through the Department of Defense (“DoD” or “the Agency”), and Defendant-Intervenor Microsoft Corporation (“Microsoft”), to immediately cease premature performance of the Joint Enterprise Defense Infrastructure (“JEDI”) Contract pending the Court’s resolution of this bid protest. AWS’s strong likelihood of success on the merits of its protest challenging the propriety of the JEDI award to Microsoft, as well as the balance of harms among the parties and the public that would result from an injunction, warrant the Court’s order of immediate equitable relief.

AWS filed its Complaint on November 22, 2019. The Administrative Record (“AR”), delivered by the Government on January 3, 2020, although incomplete, confirms AWS’s detailed allegations that DoD’s award of the JEDI Contract to Microsoft suffers from numerous fatal errors—none of which is explained in the AR.¹ In evaluating the proposals, DoD blatantly favored Microsoft by ignoring the failure of its cloud solution to meet fundamental technical requirements and by obfuscating the clear superiority of AWS’s cloud solution. This is not the typical bid protest where a disappointed offeror complains about subjective judgments made by the Government regarding the relative qualities of technical solutions. Here, DoD placed its thumb firmly on the source selection scale and skewed the evaluation in Microsoft’s favor.

¹ Although these errors entitle AWS to relief regardless of the reason they occurred, it is possible, if not likely, they are the product of unprecedented and inappropriate pressure and interference by President Donald J. Trump to drive the award away from AWS. AWS has filed a Renewed Motion to Supplement the Administrative Record and a Motion to Complete the Administrative Record to determine whether, in fact, President’s Trump’s very public bias infected the JEDI source selection process. *See* Pl. Sealed Renewed Mot. to Suppl. the Administrative R., ECF No.124; *see also* Pl. Sealed Mot. to Complete the Administrative R., ECF No.127.

DoD's dubious evaluation rests on clear violations of the solicitation ("RFP") requirements and a gross misreading of the proposals. The defective evaluation implicates virtually every source selection criterion. As the errors highlighted below demonstrate, any one of them is so obvious and serious that it alone should persuade the Court to grant the requested injunctive relief, even before considering the numerous flaws in other areas.

DoD Accepted a Plainly [REDACTED]

DoD ignored the fact that Microsoft proposed a squarely noncompliant technical approach for one of the RFP's price scenarios. Under Factor 5 (Application and Data Hosting and Portability), Price Scenario 6 required offerors to price [REDACTED]

[REDACTED] AWS's proposal described and priced a technical solution for [REDACTED], as required by the RFP. Microsoft's proposal, [REDACTED]

[REDACTED]. According to the Price Evaluation Board ("PEB"), [REDACTED]

The PEB erroneously assumed Microsoft's [REDACTED]

[REDACTED] That error, while not excusable, was perhaps understandable, given the PEB's focus on price rather than on the technical aspects of the proposals. But the Technical Evaluation Board ("TEB") and the Source Selection Evaluation Board ("SSEB"), each of which should have been alert to this kind of technical issue, also failed to recognize Microsoft's

[REDACTED] And, despite their visibility into both the technical and price proposals, the Source Selection Advisory Council ("SSAC") and the Source Selection Authority

[REDACTED]

(“SSA”) failed to recognize [REDACTED] This DoD misevaluation turned the source selection dramatically in Microsoft’s favor, transforming its [REDACTED]

[REDACTED]

DoD Ignored [REDACTED]

DoD also overlooked Microsoft’s [REDACTED]

[REDACTED].² The demonstration, which was intended to determine whether an offeror’s proposed cloud solution could actually perform the RFP requirements, was comprised of four test scenarios. Microsoft [REDACTED] scenarios during the second demonstration. Among these scenarios, Microsoft was required to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Microsoft responded by [REDACTED]

[REDACTED]

[REDACTED], Microsoft responded by [REDACTED]. [REDACTED]

[REDACTED]

[REDACTED] During key phases

of these portions of the test, Microsoft [REDACTED]. [REDACTED]

[REDACTED]

[REDACTED] DoD recorded Microsoft’s [REDACTED]

² The Factor 8 evaluation relied most heavily on the second of two demonstrations because DoD’s administration of the first demonstration was plagued by technical difficulties.

[REDACTED]

[REDACTED]

In multiple test scenarios, the DoD evaluators [REDACTED]

[REDACTED]

[REDACTED] DoD inexplicably rated both offerors as Good and Low Risk for Factor 8.

DoD Created False Parity on Tactical Edge Solutions Despite A Superior AWS Offering

As a third example, DoD's evaluation of each offeror's tactical edge solution under Factor 3 reveals that the Agency's evaluation neutralized AWS's clear technical advantage. The RFP's Tactical Edge criteria were intended to judge the capabilities of a proposed cloud solution for the full range of military operations in hostile environments, including its portability for use by soldiers on the move. AWS offered [REDACTED]

[REDACTED]. Microsoft offered [REDACTED]

[REDACTED]. DoD nevertheless rated the two offerors technically equal for this requirement, and it rested this false equivalence on [REDACTED] it wrongly attributed to AWS's solution.

For example, DoD erroneously concluded that both AWS and Microsoft [REDACTED]. That is true for Microsoft, but it is not for AWS, which offered [REDACTED]. Indeed, DoD went so far as to criticize AWS for [REDACTED], including its [REDACTED]. In this regard, the SSEB complained that [REDACTED]

[REDACTED]

[REDACTED] DoD's criticism of AWS's tactical edge solutions, while ignoring [REDACTED] in Microsoft's offering, is impossible to explain based on the record, rationality, and fairness. Unless this Court steps in, the impact of this obviously invalid evaluation will be collateral damage on the warfighter and national security.

DoD's Evaluation is Fraught With Other Blatant and Dispositive Errors

Any one of the foregoing errors, standing alone, would entitle AWS to relief. But they are only the tip of the iceberg. Clear and material evaluation errors pervade many of the other RFP criteria as well, including two discrepancies that further expose how DoD's miscalculation expunged AWS's considerable technical advantage in cloud technology.

First, under Factors 2 and 4, DoD minimized the importance of AWS's unparalleled hypervisor solution, which uses a novel hardware-based approach to cloud security to ensure separation of each user's virtual trusted space. After the TEB and SSEB recognized AWS's "Nitro" hypervisor architecture as [REDACTED] in the SSEB's words—the SSAC [REDACTED], but brushed aside its importance for cloud security. In doing so, however, the SSAC put forth a rationale that both runs contrary to the RFP's cloud security requirements and ignores Nitro's unique capabilities for protecting against a broad range of security breaches. Second, DoD misread AWS's proposal as [REDACTED]

[REDACTED] This evaluation error deprived AWS of the competitive advantage provided by its [REDACTED] third-party offerings, by far the most of any cloud provider.

Whether the Court considers each of these evaluation errors on their own or in totality, there should be little doubt that AWS is likely to prevail on the protest's merits. And that does not

even include the errors which are still being developed through this bid protest, including AWS's claims that are focused on President Trump's interference in the procurement process.

The Court also should be satisfied that the balance of harms weigh heavily in favor of injunctive relief. The harm to AWS compared to Microsoft is clear when viewed in light of AWS's strong case on the merits. Wrongful deprivation of a contract is undeniably irreparable harm under the Court's precedent. Without an injunction, continued performance of the JEDI Contract could jeopardize the relief available to AWS if it prevails in the protest. In contrast, because Microsoft has no rightful claim to the JEDI Contract, it would not suffer any cognizable harm at all.

DoD, in turn, claims that continued JEDI performance is necessary for national security, but its position does not reflect reality or withstand scrutiny. DoD and its agencies are satisfying their cloud computing requirements today using a host of existing contracts. DoD can continue to meet its needs that way for the foreseeable future, just as it has for many years (including during the RFP process and the entire evaluation period). Contrary to the impression left by the Government, no user is waiting for the JEDI Contract to obtain cloud computing services.

Indeed, Defendant's claim of urgency is inconsistent with its conduct in this bid protest—DoD had already voluntarily agreed to stay substantive contract performance until February 11, 2020, and it was the Government that sought delay in its production of the Administrative Record (which remains incomplete). Under these circumstances, DoD will suffer little or no harm by pausing performance until the Court decides this protest. And, of course, national security is not furthered by jamming through an inferior JEDI offering.

Finally, the public interest, including the interests of both the nation's taxpayers and its warfighters, will benefit from an injunction. Preserving the status quo and the opportunity for a complete protest remedy, and making sure DoD selects the actual best value cloud solution for the

critical JEDI Contract—in a rational and fair way—is clearly in the best interest of this country, its citizens, its soldiers, and national security. Accordingly, the Court should grant Plaintiff's motion for a temporary restraining order and preliminary injunction in this case.

QUESTION PRESENTED

Is AWS entitled to a temporary restraining order and preliminary injunction, based on its likelihood of success on the merits of its protest, the irreparable harm that would result without injunctive relief, the balance of hardships on the parties, and the public interest?

STATEMENT OF THE CASE

This bid protest challenges the award of the JEDI Contract to Microsoft based on DoD's flawed and unfair evaluation of proposals and the resulting invalid best value award decision.

The JEDI RFP set forth nine evaluation factors: (1) Gate Evaluation Criteria; (2) Logical Isolation and Secure Data Transfer; (3) Tactical Edge; (4) Information Security and Access Controls; (5) Application and Data Hosting and Portability; (6) Management Task Order ("TO") 001; (7) Small Business Participation Approach; (8) Demonstration; and (9) Price. AR Tab 342 at 151503-09. Factors 2, 3, and 5 included among their criteria the requirement that DoD evaluate the offerors' proposed approaches to six price scenarios for "technical feasibility." *Id.* at 151495-96, 151498, 151505-06. Factor 9 required DoD to evaluate the offerors' price volumes for "accuracy and completeness," and to calculate each proposal's total evaluated price as the sum of the proposed prices for the six price scenarios and twelve contract line items ("CLINs") for portability plans and program support. *Id.* at 151499-50, 151507-09. DoD was to award the JEDI Contract to the offeror whose proposal represents the best value. *Id.* at 151502.

DoD ranked the importance of Factors 2-8 as follows (from most to least important):

- Factor 2 (Logical Isolation and Secure Data Transfer);
- Factor 3 (Tactical Edge);
- Factor 4 (Information Security and Access Controls);
- Factor 5 (Application and Data Hosting and Portability);
- Factor 8 (Demonstration),
- Factor 6 (Management and TO 001); and
- Factor 7 (Small Business Participation Approach).

Id. at 151502. Factors 2-8, when combined, were more important than Factor 9 (Price). *Id.* However, Factor 9 was to become increasingly important where proposals were relatively equal as a technical matter. *Id.* For Factors 2-6 and 8, DoD was to assign ratings for technical aspects (Outstanding, Good, Acceptable, Marginal, and Unacceptable) and risk (Low, Moderate, High, Unacceptable).³ *Id.* at 151510-11. DoD was to eliminate from the competition any offeror who received a Marginal or Unacceptable rating, or a risk rating of High, under Factor 8. *Id.*

The RFP specified DoD's evaluation would proceed in two phases. *Id.* at 151502-03. Phase One required DoD to evaluate each offeror under Factor 1, Gate Evaluation Criteria, to determine award eligibility. *Id.* at 151502. Phase Two required evaluation of award-eligible proposals under Factors 2-6 and 9. *Id.* at 151503. Based on this evaluation, DoD would make a competitive range determination and invite the remaining offerors to submit information responsive to Factor 7, and to demonstrate their cloud solutions under Factor 8. *Id.* DoD also would invite offerors within the competitive range to engage in discussions, as appropriate. *Id.* After discussions, DoD would request Final Proposal Revisions ("FPR"), and then evaluate FPRs under Factors 2-7 and 9. *Id.* The RFP stated DoD would deem offerors' FPRs to include the already conducted Factor 8 demonstration and evaluation. *Id.*

³ The RFP stated DoD would assign similar ratings based on different criteria under Factor 7. *Id.*

On October 25, 2019—a few months after President Trump’s call for DoD to “look . . . very closely” into AWS’s proposal and Secretary of Defense Mark Esper’s announcement that he would be “examining” the process—DoD announced it had awarded the JEDI Contract to Microsoft. AR Tab 480 at 176608. In the Source Selection Decision Document (“SSDD”), the SSA indicated Microsoft represented the best value because it was technically superior and lower priced than AWS. AR Tab 459 at 176417. The SSA found that, although Microsoft and AWS were relatively equal under Factors 2, 3, 4, 7, and 8, Microsoft was “significantly superior to AWS” under Factors 5 and 6. *Id.* at 176415-16. The SSA also noted Microsoft’s total evaluated price of \$678,517,417.38 was [REDACTED] less than AWS’s total evaluated price of [REDACTED]. *Id.* at 176417; AR Tab 457 at 176405. Following a debriefing, and DoD’s refusal to provide substantive responses to AWS’s questions, AWS filed this protest.

ARGUMENT

“This Court has broad authority to order injunctive relief in the context of bid protests.” *FMS Inv. Corp. v. United States*, 136 Fed. Cl. 439, 442 (2018). In considering whether preliminary injunctive relief is appropriate, the Court weighs four factors: (1) the likelihood of plaintiff’s success on the merits; (2) whether plaintiff will suffer irreparable harm absent injunctive relief; (3) the balance of hardships; and (4) the public interest. *Id.*; *see also Serco, Inc. v. United States*, 101 Fed. Cl. 717, 720 (2011) (considering same factors for temporary restraining order). “No single factor is determinative, and the weakness of the showing regarding one factor may be overcome by the strength of the others.” *FMS Inv. Corp.*, 136 Fed. Cl. at 442 (quotations omitted); *see also FMC Corp. v. United States*, 3 F.3d 424, 427 (Fed. Cir. 1993). AWS satisfies all of the factors for immediate injunctive relief.

I. AWS HAS SHOWN A LIKELIHOOD OF SUCCESS ON THE MERITS.

To demonstrate likelihood of success on the merits, AWS must show that it is “more likely than not” to succeed on its claims that DoD’s actions were “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 28 U.S.C. § 1491(b)(4) (citing 5 U.S.C. § 706); *Veterans Contracting Grp., Inc. v. United States*, 133 Fed. Cl. 613, 621 (2017). AWS need only raise “serious questions over [DoD]’s evaluation of proposals in this procurement” by, for example, “point[ing] to inconsistencies, omissions, unequal treatment of offerors, and cherry-picked data.” *FMS Inv. Corp.*, 136 Fed. Cl. at 443. Serious questions are raised where, as here, the agency has deviated from the solicitation’s evaluation criteria and disparately evaluated proposals, thereby denying offerors a fair opportunity to compete for the contract. *See e.g., BayFirst Sols., LLC v. United States*, 102 Fed. Cl. 677, 695 (2012) (holding protester showed success on merits where record demonstrated a “flawed source selection process”).

The JEDI source selection was compromised by DoD’s unfair evaluation. Virtually every aspect of the evaluation was undermined by serious errors that [REDACTED] while depriving AWS of credit for its compliant and far more capable offering. Even the currently incomplete AR makes clear that, but for DoD’s disparate and unreasonable evaluation, AWS would have received the JEDI Contract. AWS is likely to succeed on the merits of its claims.

A. Egregious Evaluation Errors with Respect to Factors 5, 8, and 3 Unfairly Tilted the Source Selection in Microsoft’s Favor.

Among the many discrepancies in the AR, three errors stand out as particularly egregious, unfair, and determinative of the award decision: (1) DoD’s evaluation of Microsoft’s technical approach and price for [REDACTED] under Factor 5, Price Scenario

6, which ignored Microsoft's explicit [REDACTED]
[REDACTED]; (2) DoD's [REDACTED]
[REDACTED] and (3) DoD's evaluation of the tactical edge solutions under Factor 3, which created a perception of technical equality by unfairly criticizing AWS's objectively superior devices and [REDACTED]

Each of these errors had a material impact on the competitive standing of the two offerors. Standing alone, and certainly in totality, these evaluation defects dramatically tilted the source selection in Microsoft's favor. As a consequence, and at the expense of the nation's taxpayers, its warfighters, and the integrity of the procurement process, DoD made award to Microsoft— [REDACTED]

1. DoD Miscalculated Microsoft's Technical Approach for Price Scenario 6.

DoD committed two critical errors in its evaluation of Microsoft's technical approach for Price Scenario 6. First, DoD determined that Microsoft proposed a technically feasible approach

[REDACTED]
[REDACTED]. DoD should have considered Microsoft's [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] Each of these errors independently undermines DoD's source selection decision, and requires reevaluation of proposals and a new award decision.

[REDACTED]

a. Microsoft's Proposal Was Ineligible for Award Because It

DoD failed to recognize that Price Scenario 6 required [REDACTED]
[REDACTED] RFP Amendment 0005 revised the instructions for all price scenarios to require offerors to "[a]ssume that all data in these price scenarios is *highly accessible unless otherwise stated.*" AR Tab 302 at 64310 (emphasis added). Following issuance of Amendment 0005, an offeror submitted the following question to DoD:

The Government has introduced a new term "highly accessible" without definition. Could the government confirm that the term "highly accessible" is defined as either "Online Storage" or "Nearline Storage" as defined in Attachment J-8?

AR Tab 304 at 64332. DoD responded: "The term 'Highly Accessible' is meant to be understood as *online and replicated storage.*" *Id.* (emphasis added).

The RFP defines Online storage as "[s]torage that is immediately accessible to applications without human intervention." AR Tab 29 at 650. It defines Nearline storage as "[s]torage not immediately available, but can be brought online quickly without human intervention." *Id.* Although the RFP does not define "replicated storage," the term refers to the practice of storing data more than once so that there are multiple copies of the data. In other words, it is an additional requirement for backup rather than an alternative to Online storage. AR Tab 304 at 64332.

Unlike some of the other price scenarios, Price Scenario 6 did not identify a specific storage type. For example, whereas Price Scenarios 3 and 4 reference Online, Nearline, and Offline storage, Price Scenario 6 does not reference those terms. AR Tab 302 at 64319-24, 64327-29. According to the RFP, this silence as to storage type meant offerors were to "[a]ssume that all data in [the] price scenario[] is *highly accessible,*" which the RFP defined as Online storage. AR Tab 304 at 64332 (emphasis added).

The Price Scenario 6 requirements, however, went further to make clear that the offerors were to propose Online storage: Price Scenario 6 repeatedly stated that data should be “highly available”—*i.e.*, stored Online:

The maintenance system converts each record into a 500 KB structured record, which is sent via API call to a *highly available* JEDI Cloud serverless function, which requires 2.5GB of RAM to run. This serverless function parses the incoming data for validity and stores it in a *highly available* JEDI Cloud NoSQL document-based data store....

The flight operations system will push an event to a separate, *highly available* JEDI Cloud serverless function for each flight mission once that flight’s operational data has been uploaded....

The results of this analysis consume 5 MB of data and are stored in a *highly available* simple NoSQL key-value based data store.

AR Tab 302 at 64327 (emphasis added); AR Tab 304 at 64332.

In the Price Scenario 6 evaluation, however, DoD overlooked Microsoft’s proposal of

[REDACTED]

[REDACTED]

First, DoD failed to recognize that, [REDACTED]

[REDACTED] AR Tab 408

at 173315. [REDACTED]

See *e.g.*, AR Tab 420 at 174754-57; AR Tab 430 at 175810. [REDACTED]

[REDACTED]

[REDACTED] AR Tab 455

at 176363 (noting [REDACTED]

[REDACTED] (emphasis added)).

[REDACTED]

Because it proposed [REDACTED], Microsoft did not satisfy the Price Scenario 6 requirements. DoD should have found Microsoft's technical approach unfeasible, assigned a deficiency, and eliminated Microsoft from the competition.⁴ AR Tab 305 at 64355 (defining "deficiency" as a "material failure of a proposal to meet a Government requirement..."). Instead, DoD inexplicably did the opposite, finding Microsoft proposed a "technically feasible approach" [REDACTED] AR Tab 332 at 151328; AR Tab 455 at 173363. There is no explanation in the record for this unreasonable conclusion.

Second, DoD failed to recognize that Microsoft's technical narrative for Price Scenario 6 [REDACTED] [REDACTED] (AR Tab 420 at 174754-57; AR Tab 430 at 175810), [REDACTED] (AR Tab 412 at 173697-99).⁵ [REDACTED] [REDACTED].⁶ Under a rational evaluation, the TEB would have deemed Microsoft's [REDACTED] to be another deficiency and eliminated Microsoft from the competition.⁷ See AR Tab 305 at 64355.

⁴ Because the Government has not provided a complete record, it is unclear whether DoD identified Microsoft's [REDACTED] during discussions.

⁵ In contrast, AWS's technical narrative for Price Scenario 6 clearly indicated AWS was proposing [REDACTED]. AR Tab 371 at 152866-67; AR Tab 455 at 176363.

⁶ Without this information, it is not even clear Microsoft [REDACTED]. For example, Microsoft identifies [REDACTED]. See AR Tab 412 at 173697.

⁷ Because the Government has produced an incomplete record, it also is unclear whether DoD identified this deficiency during discussions. See *supra* Footnote 4.

Third, DoD failed to recognize [REDACTED]

[REDACTED] The SSAC—which considered both the technical and price evaluations when making a recommendation to the SSA—should have noticed that Microsoft proposed [REDACTED]

[REDACTED] Indeed, the SSAC scrutinized AWS’s proposal in that manner when considering AWS’s third-party marketplace offerings under Factor 5. *See* AR Tab 457 at 176402 (noting the SSAC deviated from the TEB’s findings because [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]). Under a fair evaluation, the SSAC would have [REDACTED]

[REDACTED] Had it done so, it would have recognized Microsoft’s proposed technical approach—on its face—does not comply with the RFP. *See* AR Tab 305 at 64355.

b. Had Microsoft Proposed a Technically Feasible Approach, [REDACTED]

In addition to its flawed evaluation of Microsoft’s technical approach to Price Scenario 6, DoD also failed to recognize that Microsoft’s [REDACTED]

[REDACTED]
[REDACTED]

The RFP required DoD to calculate each offeror’s total evaluated price for the JEDI Contract by combining the total price for each of the six price scenarios with the total price for Portability Plan, Portability Test, and Cloud Computing Program Office (“CCPO”) Program Management Support CLINs. AR Tab 342 at 151508-09.

[REDACTED]

AWS—which proposed compliant [REDACTED] for Price Scenario 6—had a total evaluated price of [REDACTED] for the scenario. AR Tab 455 at 176363. In contrast, Microsoft—which proposed [REDACTED]—had a total evaluated price of [REDACTED] for Price Scenario 6. *Id.* The PEB explained [REDACTED]

[REDACTED]

[REDACTED]

AR Tab 455 at 176363 (emphasis added). As the PEB observed, Microsoft [REDACTED]

[REDACTED] *See id.*

Critically, AWS's total evaluated price for the JEDI Contract exceeded Microsoft's by approximately [REDACTED]. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] *See AR Tab 459*

at 176417.

[REDACTED]

Correction of these errors would upend the JEDI award decision entirely. Had DoD correctly assigned Microsoft [REDACTED]

[REDACTED] At best, and to the extent it has not already done so, DoD would have to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In either event, AWS would have a substantial chance of receiving the JEDI Contract.

2. DoD Ignored Microsoft's [REDACTED] under Factor 8.

DoD's misevaluation of Microsoft's demonstration under Factor 8 is another egregious, readily apparent error in the JEDI source selection process.

Factor 8 required DoD to evaluate the extent to which each offeror demonstrated its cloud solution using its proposed approaches for Factors 1 through 6 in different scenarios. AR Tab 342 at 151507. DoD planned only one demonstration, but after technical difficulties during the first demonstration, DoD amended the RFP to hold a second demonstration. AR Tab 290. The amended RFP explained that although DoD would consider both demonstrations in the Factor 8 evaluation, DoD would give more weight to the second demonstration "in light of it reflecting each Offerors [sic] ability to best showcase their offerings." AR Tab 342 at 151507. After considering both demonstrations, DoD was to assign each offeror a technical capability rating and a risk rating

[REDACTED]

consistent with the evaluation scheme for Factors 2-6. *Id.* at 151510. If an offeror received a Marginal or Unacceptable rating, or a High risk rating, it was ineligible for award.⁸ *Id.* at 151503.

The AR shows Microsoft [REDACTED] specified second demonstration scenarios, yet DoD inexplicably gave Microsoft a [REDACTED] grade in each instance. In contrast, AWS demonstrated its cloud capabilities to the complete letter of the Factor 8 requirements during the second demonstration, and received the same grade. DoD's disparate evaluation is a clear violation of the RFP and procurement standards.

a. Microsoft [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Second Demonstration of Scenario 8.2, and Therefore Was Not [REDACTED]

Although DoD concluded Microsoft's second demonstration of Scenario 8.2 was [REDACTED] the AR shows that rating to be contrary to the facts. Scenario 8.2 required the offerors to scale up the number of available servers (*i.e.*, nodes) as the load on those servers increased, and scale down the number of available servers as the load on those servers decreased—a basic test of an offeror's ability to scale servers elastically in response to load. AR Tab 287 at 64173. This is reflected in the instructions for Scenario 8.2, which stated:

A successful implementation of 8.2 will, at time of demonstration, create a dynamically created pool of compute resources to respond to incoming requests from a client. *As the client increases the number of incoming requests, it is expected that the number of compute nodes will seamlessly increase as the number of incoming*

⁸ A Marginal rating is appropriate if a proposal “does not clearly meet requirements and has not demonstrated an adequate approach and understanding of the requirements.” AR Tab 342 at 151510. An Unacceptable rating is appropriate if a proposal “does not meet the requirements and contains one or more deficiencies and is unawardable.” *Id.* A High risk rating is appropriate if a proposal “contains a significant weakness or combination of weaknesses which is likely to cause disruption of schedule, increased cost or degradation of performance” and “[i]s unlikely to overcome the difficulties, even with special contractor emphasis and close Government monitoring.” *Id.* at 151511

requests exceed the predefined maximum requests per node. As the test client reduces usage, it is expected that there will be the seamless shutdown of excess nodes.

AR Tab 270 at 63044 (emphasis added); AR Tab 287 at 64173 (emphasis added).

To assess whether the offerors could effectively scale the number of available servers up and down as load increased and decreased, DoD scaled loads over four phases:

- Phase 1: the 8.2(4.a) script generated 5 requests per second for 90 seconds;
- Phase 2: the 8.2(4.b) script generated 150 requests per second for 360 seconds, with a 60 second ramp up time;
- Phase 3: the 8.2(4.c) script generated 450 requests per second for 360 seconds, with a 75 second ramp up time; and
- Phase 4: the 8.2(4.d) script generated 60 requests per second for 360 seconds, with a 60 second ramp up time.

AR Tab 308 at 64414; AR Tab 287 at 64174. After the four phases, DoD was to implement a cool down period of four minutes. AR Tab 287 at 64174. At the end of each phase and the cool down period, DoD was to record the number of online servers before moving to the scenario's next phase or step. *Id.* at 64174-75.

Microsoft's servers [REDACTED]. The TEB found that Microsoft had [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] AR Tab 308 at 64414; *see also* AR Tab 291 at

01:35:50-02:02:16.⁹ [REDACTED]

⁹ In contrast, AWS's reported nodes count during its second demonstration of Scenario 8.2 was [REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] AR Tab 308 at 64414.
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] 10

AR Tab 308 at 64414. Microsoft [REDACTED], yet DoD gave Microsoft a [REDACTED] grade with no explanation.¹¹ AR Tab 308 at 64415.

Making matters worse, during Phases 3 and 4, the demonstration video shows [REDACTED]
[REDACTED]

See AR Tab 291 at 01:47:27- 01:54:11. Moreover, [REDACTED]
[REDACTED] (AR Tab 308 at 64414; AR Tab 291 at 02:02:16), [REDACTED]

[REDACTED] See AR Tab 287 at 64174. The TEB [REDACTED]. AR Tab 308 at 64415. Under a fair evaluation, Microsoft would have received a [REDACTED]

[REDACTED]
[REDACTED]

¹⁰ During the demonstration video, the screen shows [REDACTED]
See AR Tab 291 at 1:58:01. However, [REDACTED]
[REDACTED] AR Tab 287 at 64174. Accordingly, because [REDACTED]
[REDACTED] See *id.*; see also AR Tab 307 at 64391 ([REDACTED]).

¹¹ The TEB's [REDACTED]
[REDACTED] See AR Tab 307 at 64391-92.

[REDACTED]
[REDACTED]

b. Microsoft [REDACTED] [REDACTED] [REDACTED] [REDACTED] Its Second Demonstration of Scenario 8.4, and Therefore Was Not [REDACTED]

Microsoft also [REDACTED] its second demonstration under Scenario 8.4, which required offerors to demonstrate key security capabilities. *See* AR Tab 287 at 64178. For this scenario, the instructions stated: “A successful implementation will demonstrate that the security controls and user Access Control Lists (ACL’s) *work as expected, and audit logs are generated during the course of any access, security, and API events during the course of this exercise, both through the GUI [and] interactively via a command line interface (CLI).*” AR Tab 287 at 64178 (emphasis added). Microsoft’s second demonstration failed to meet this standard.

Step 2 of Scenario 8.4 required offerors to enable policy-based access. *Id.* at 64179. Specifically, the offerors were to generate time-limited access tokens for two users via the Application Program Interface (“API”), use those tokens to log into the cloud service provider portal, and then wait for one of the tokens to expire, while revoking the other token via the Graphical User Interface (“GUI”) before expiration. *Id.* at 64179-80. After the one token expired, and after the offeror revoked the second token, the offeror had to demonstrate “attempting to log in using the same [respective] token” and confirm such attempts failed. *Id.* at 64180.

At the beginning of this step, Microsoft explained that it [REDACTED]
[REDACTED]
[REDACTED] *See* AR Tab 291 at 04:18:21-04:34:27. DoD told Microsoft that [REDACTED]
[REDACTED]

[REDACTED] *Id.* at 04:33:11. Thus, from the outset, [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]. *Id.*

at 04:45:01-04:50:37. In other words, [REDACTED]
[REDACTED].¹²

Id. Thus, Microsoft [REDACTED]
[REDACTED]. Although the TEB Report mentioned that Microsoft [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED] See AR Tab 308 at 64422.

Step 3 of Scenario 8.4 required offerors to configure access to data and services using tagging capabilities. AR Tab 287 at 64180. Part of this step entailed tagging files, and then restricting a user's access to certain files based upon the file's tag. *Id.* (steps 3(d)-(h)). Microsoft again [REDACTED]. AR Tab 291 at

04:59:01. [REDACTED]
[REDACTED]. *Id.* at 04:59:01-
05:04:54. [REDACTED]. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

In other words, the goal of the tagging requirement was to ensure users can access the same storage

¹² This is in stark contrast to AWS's demonstrated ability to [REDACTED]
[REDACTED]. See AR Tab 295 at 04:29:59-4:30:18, 04:39:45.

[REDACTED]
[REDACTED]

locations, but not necessarily the same contents within that location. AR Tab 287 at 64180 (step 3(h)). This capability is critical to eliminating the risk that an individual could impermissibly grant access to certain users by inadvertently saving files to the wrong folder. [REDACTED]

[REDACTED], [REDACTED].

Finally, [REDACTED]

AR Tab 308 at 64422. [REDACTED]

See AR Tab 307 at 64400. [REDACTED] DoD concluded that,

[REDACTED]
[REDACTED]

AR Tab 308 at 64422 (emphasis added). DoD added: [REDACTED]

[REDACTED]
[REDACTED]

Id. at 64423. In other words, the

TEB recognized [REDACTED]

[REDACTED]

. See *id.* at 64422-23. [REDACTED]

runs directly contrary to the RFP's requirement for a demonstration.

Microsoft's [REDACTED] second demonstration of Scenario 8.4 were material and should have precluded a [REDACTED]. Instead, Microsoft should have received a [REDACTED] rating, which, when combined [REDACTED] should have resulted in, at best, a Marginal rating under Factor 8, and Microsoft's elimination from the competition.

[REDACTED]

c. [REDACTED] in its Second Demonstration of Scenario 8.3 Should Have Resulted in a Significant Risk Increase.

In addition to [REDACTED], Microsoft also exposed a [REDACTED]—in its tactical edge solution during Scenario 8.3. This scenario required offerors to “show the features allowing successful use of the tactical device in tactical edge environments.” AR Tab 287 at 64175. [REDACTED]

[REDACTED] AR Tab 287 at 64178.

[REDACTED]. See AR Tab 291 at 3:33:30-3:52:36. [REDACTED]

[REDACTED]. See *id.*

At minimum, [REDACTED] should have warranted an increased risk assessment. The fact that [REDACTED]

[REDACTED] This is especially so given the [REDACTED]

[REDACTED] See AR Tab 410 at 173645 [REDACTED]

[REDACTED]); AR Tab 342 at 151505. [REDACTED]

[REDACTED]

The TEB, [REDACTED], DoD's assignment of a Low risk rating to Microsoft [REDACTED] was unreasonable. *See* AR Tab 342 at 151511 (defining Low risk as "hav[ing] little potential to cause disruption of schedule, increased cost or degradation of performance," and "normal contractor effort and normal Government monitoring will likely be able to overcome any difficulties"). This is especially true considering the additional risks associated with [REDACTED]

d. DoD's Failure to Assign Microsoft a Marginal Rating is Evidence of Disparate Treatment that Prejudiced AWS.

[REDACTED] discussed above should have resulted in Microsoft receiving, at best, a Marginal technical rating and a Moderate risk rating under Factor 8, especially given the scrutiny with which DoD evaluated AWS.¹³ This would have resulted in Microsoft's elimination from the competition and award to AWS.

Even if a Marginal rating somehow were not appropriate, however, under no circumstances could DoD have rationally determined that Microsoft's [REDACTED] [REDACTED] *At best*, Microsoft [REDACTED] [REDACTED] Scenarios 8.2 and 8.4. In contrast, AWS truly earned its [REDACTED] ratings under all four scenarios in its second demonstration. *See* AR Tab 307 at 64387, 64392,

¹³ During the first demonstrations, DoD subjected AWS to strict rating standards, although Microsoft was not held to that same standard. For example, [REDACTED]

[REDACTED] Compare AR Tab 307 at 64386 ([REDACTED]) with AR Tab 308 at 64420-21 [REDACTED]). Additionally, [REDACTED]

[REDACTED] Compare AR Tab 307 at 64399 with AR Tab 308 at 64407.

[REDACTED]

64397, 64400. Indeed, AWS *surpassed* most of the performance benchmarks (some by a substantial margin) and received no noted deficiencies or failures. *See infra* Section I(C)(2). Under a rational evaluation, DoD would have eliminated Microsoft from the competition, or at least assigned Microsoft lower technical capability and risk ratings under Factor 8.

3. DoD's Evaluation of the Offerors' Tactical Edge Devices Was Unreasonable and Plagued by Disparate Treatment.

Yet another egregious error involved the evaluation of each offeror's Tactical Edge solution. Factor 3 required offerors to propose at least one tactical edge device in each of two tactical device categories, and it encouraged offerors to propose additional devices to satisfy the "full range of military operations." AR Tab 342 at 151494, 151505. Category One devices include durable, ruggedized, and portable compute and storage devices. *Id.* at 151494. Category Two devices include static, modular, rapidly deployable data centers. *Id.* DoD determined neither AWS nor Microsoft was technically superior under Factor 3. AR Tab 457 at 176401. That conclusion, however, was predicated on evaluation errors that minimized the gap between AWS's robust and currently deployed tactical edge offerings and Microsoft's inferior solution.

a. DoD Disparately Evaluated the Offerors' Tactical Edge Devices With Respect to Portability and Dismounted Operations Capabilities.

DoD engaged in disparate treatment when assessing the portability and dismounted operations capabilities of the offerors' respective tactical edge devices. Whereas DoD held AWS to an exacting and comparatively unfair standard, DoD allowed Microsoft's proposed devices to escape meaningful scrutiny. As a result, DoD created a false equivalency between the offerors' proposed tactical edge devices.

The record shows that AWS's Category One tactical edge devices are [REDACTED]

[REDACTED] than their counterparts at Microsoft:

[REDACTED]

Compare AR Tab 324 at 151166-67 with AR Tab 330 at 151279-80. Nevertheless, DoD assigned [REDACTED] to AWS with respect to portability and dismounted operations that Microsoft's [REDACTED] devices inexplicably did not receive.

For example, despite recognizing that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] AR Tab 324 at 151166. Yet, when evaluating [REDACTED]

[REDACTED]. AR Tab 330 at

151279-80. Instead, the TEB simply characterized [REDACTED]

[REDACTED]

[REDACTED] *Id.*

[REDACTED]

The TEB also assigned [REDACTED]

[REDACTED] AR Tab 324

at 151175-76. However, when evaluating [REDACTED]

[REDACTED] AR Tab 330 at 151289 (noting [REDACTED]

[REDACTED] *see also id.* at 151290.

DoD's evaluation judgments are incorrect and irrational. If Microsoft's [REDACTED]

[REDACTED].¹⁴ DoD's conclusion to the contrary is unreasonable and not supported by the record.¹⁵

b. DoD Unreasonably Penalized Only AWS for [REDACTED]

DoD assigned [REDACTED]

[REDACTED] AR Tab 324 at 151169, 151171. The RFP, however, did not require offerors to meet

[REDACTED] AR Tab 342 at 151494. It required only that each

¹⁴ This is especially true if, as the evaluation record suggests, DoD also determined Microsoft's [REDACTED]. *See* AR Tab 330 at 151289 [REDACTED].

¹⁵ If the approximately [REDACTED] [REDACTED] *See* AR Tab 330 at 151289; AR Tab 324 at 151166. The same is true for Microsoft's [REDACTED]

[REDACTED] AR Tab 330 at 151279. In this scenario, each individual would hold [REDACTED]

[REDACTED] *See id.*; AR Tab 324 at 151166.

offeror address [REDACTED]
[REDACTED] *Id.* Offerors therefore were free to propose tactical edge devices that complied with [REDACTED]. *See id.*

AWS and Microsoft each [REDACTED]
[REDACTED] AR Tab 369 at 152805, 152809; AR Tab 410 at 173641, 173643. Notwithstanding this identical approach, [REDACTED]
[REDACTED].¹⁶ Compare AR Tab 324 at 151169, 151171 with AR Tab 330 at 151283-84. In fact, not only did DoD not assign [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

AR Tab 330 at 151283-84.

There was no reasonable basis for DoD to treat [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] ¹⁷

AR Tab 369 at 152805, 152809; AR Tab 410 at 173641, 173643. Moreover, although Microsoft's [REDACTED]
[REDACTED]

[REDACTED], which, as DoD well knows, have already been [REDACTED] and have been [REDACTED] AR Tab 369 at 152801.

¹⁷ Microsoft's Factor 3 volume provides the [REDACTED] AR Tab 410 at 173641, 173643. However, Microsoft [REDACTED] [REDACTED]. *See id.*

[REDACTED]—AWS’s devices still would be considerably [REDACTED]

[REDACTED] :

[REDACTED]

AR Tab 330 at 151283-84; AR Tab 369 at 152805, 152809; AR Tab 410 at 173641, 173643.

Ultimately, not only did DoD rely on an unstated evaluation criterion in its Factor 3 evaluation, it also applied that unstated criterion unequally, to AWS’s competitive detriment.

c. DoD Wrongly Concluded AWS Did Not Propose a [REDACTED].

DoD also erroneously concluded AWS did not propose a [REDACTED]

[REDACTED]. In the SSAC Report, DoD stated:

[REDACTED]

[REDACTED]

AR Tab 457 at 176401. This conclusion, however, is belied by the TEB's evaluation findings.

Although neither the RFP nor the SSAC defined [REDACTED] the only reasonable interpretation is that it refers to [REDACTED]. AWS's tactical edge device portfolio includes [REDACTED]

The TEB found AWS [REDACTED]. For example, the TEB found that AWS's [REDACTED]. AR Tab 324 at 151166 [REDACTED] see also AR Tab 369 at 152805-06. It reached the same conclusion with respect to AWS's [REDACTED]. AR Tab 324 at 151171 [REDACTED]; see also AR Tab 369 at 152809. And, although not acknowledged by DoD, AWS's [REDACTED]. AR Tab 369 at 152809 [REDACTED]

Despite the TEB's findings, the SSAC inexplicably reached the opposite conclusion, finding [REDACTED] AR Tab 457 at 176401. The SSAC then used this arbitrary conclusion to draw false equivalency between AWS's tactical edge devices and Microsoft's [REDACTED] devices, claiming both offerors suffered from the same [REDACTED]. *Id.* This is not true.

[REDACTED] AR Tab 330 at 151279-80. [REDACTED] AR Tab 330 at 151283-84; AR Tab 410 at 173641, 173643. The [REDACTED] grows even more pronounced if Microsoft

[REDACTED]

[REDACTED]. AR Tab 330 at 151280. AWS's [REDACTED]
[REDACTED] than their counterparts at Microsoft. DoD's apparent attempt to minimize
AWS's advantage with respect to these devices was unreasonable and unfair.

d. DoD Penalized AWS for Proposing an [REDACTED]
[REDACTED] When Microsoft Did Not [REDACTED]
[REDACTED]

DoD's evaluation also failed to recognize that AWS's [REDACTED] was a key
discriminator between the offerors. Instead, DoD assigned AWS [REDACTED]
[REDACTED], effectively neutralizing the impact [REDACTED] in the competition. AR Tab 324
at 151170-71, 151174-75. DoD's evaluation of the [REDACTED] was unreasonable.

First, as evident from the tables in the sections above, AWS's [REDACTED] does not have
[REDACTED] [REDACTED]. *See supra* Section I.B.1, 2. It is a [REDACTED]
[REDACTED] tactical edge device [REDACTED] as the TEB found,
[REDACTED]
[REDACTED] AR Tab 324 at 151171.
Given DoD's finding that [REDACTED]
[REDACTED]—a key RFP requirement—[REDACTED] unique capabilities
should have been a key discriminator in the evaluation and should have resulted in a higher rating
for AWS. *See* AR Tab 330 at 151279, 151287, 151289-90.

Second, the RFP expressly required offerors to provide a tactical edge solution “that more
broadly addresses the full range of military operations rather than a proposed solution that only
addresses a subset of the range of military operations.” AR Tab 342 at 151505. As DoD found,
[REDACTED]

[REDACTED]. AR Tab 324 at 151166-67; AR Tab 330 at 151279-80; AR Tab 456 at 176376. However, DoD failed to recognize that [REDACTED] [REDACTED]. Through [REDACTED], AWS addressed the perceived (erroneous) gaps in the capabilities—[REDACTED]—of its other devices. AR Tab 324 at 151167. In contrast, Microsoft—[REDACTED] [REDACTED]. Consequently, only AWS provided a complete tactical edge solution to address the full range of military operations.

Rather than credit AWS for its more robust tactical edge offering, DoD inexplicably viewed it as a vice. The SSEB claimed the [REDACTED] [REDACTED] [REDACTED] [REDACTED] AR Tab 456 at 176376. Particularly given the RFP's stated desire for a full range of options, the notion that DoD would be [REDACTED] is preposterous, and underscores DoD's desire to award the JEDI Contract to Microsoft notwithstanding AWS's superior capabilities. Indeed, consistent with the TEB's lower standard for the Microsoft evaluation, the SSEB did not even remark [REDACTED]

[REDACTED]. AR Tab 456 at 176378. Accordingly, DoD should have found AWS's [REDACTED] was a key discriminator among the offerors, and assigned AWS correspondingly higher ratings under Factor 3.

e. DoD Disparately Evaluated the Offerors With Respect to Battery Power.

DoD's disparate treatment continued in its evaluation of the offerors' battery power, where DoD persistently skewed its evaluation to hide Microsoft's shortcomings and AWS's clear advantages. The RFP required offerors to demonstrate their tactical edge devices could "be powered by battery and standard military grade generators that produce alternative current at 120 volts. For battery, describe the characteristics, capacity, and runtime under standby and 100% utilization." AR Tab 342 at 151494.

During the initial evaluation, DoD determined [REDACTED]

[REDACTED]

[REDACTED] AR Tab 208 at 57972. However, after observing in the final evaluation that Microsoft

[REDACTED]

[REDACTED], stating:

[REDACTED]

AR Tab 330 at 151288 (emphasis added).

This [REDACTED] is unexplained in the AR. And it is especially problematic when comparing the offerors' capabilities. Microsoft stated it could [REDACTED]

[REDACTED]. See

[REDACTED]

id. In comparison, AWS stated [REDACTED]
[REDACTED]
[REDACTED]. AR Tab 369 at 152805.¹⁸ Moreover, the [REDACTED]
[REDACTED]. *Id.* at 152809. AWS's
battery power capabilities are [REDACTED] than Microsoft's.

But for DoD's unreasonable and disparate evaluation of the offerors' tactical edge devices, AWS would have received higher ratings under Factor 3, the second most important evaluation factor. Given the relative weighting of the evaluation factors, AR Tab 342 at 151502, this alone would have resulted in DoD concluding that AWS is the technically superior offeror, especially when accounting for DoD's numerous other evaluation errors.

B. Additional Serious Evaluation Discrepancies Minimized AWS's Technical Superiority.

AWS's advantages in cloud computing include two capabilities called out in the JEDI RFP's requirements: (1) a hypervisor solution for cloud security, and (2) a third-party marketplace offering customers access to software for use on the AWS cloud platform. AWS's cloud solution utilizes its unparalleled hypervisor solution—the hardware-based Nitro architecture—to provide the most secure logical isolation of users' virtual trusted space. [REDACTED]
[REDACTED]

[REDACTED] AWS also enjoys an advantage over Microsoft (and every other cloud provider) in terms of its third-party marketplace. AWS offered a third-party marketplace for JEDI comprised [REDACTED] software offerings—the largest third-party marketplace of any cloud provider. However,

¹⁸ [REDACTED]
[REDACTED]. AR Tab 369 at 152805.

DoD effectively neutralized AWS's advantage in these key areas by minimizing the importance of hypervisor security in violation of the RFP, mischaracterizing Nitro's security benefits, and misreading AWS's third-party marketplace proposal.

1. DoD Improperly Minimized the Cloud Security Benefits of AWS's Nitro Hypervisor.

In a cloud environment, two users might have separate virtual machines that reside on the same physical hardware. Ensuring that one virtual machine remains protected from the other is paramount, especially when the cloud in question has highly classified material that needs to be protected from insider threats and sophisticated nation states. The RFP recognized this and correspondingly gave great weight to offerors' hypervisors under Factors 2 (Logical Isolation and Secure Data Transfer) and Factor 4 (Information Security and Access Controls).

AWS's hardware-backed Nitro hypervisor provided DoD with the highest level of security and logical isolation and separation possible, prompting DoD to correctly recognize that Nitro was the [REDACTED] AR Tab 457 at 176400. Nevertheless, DoD minimized the importance of the hypervisor to draw false parity among the offerors under these two factors when, in reality, AWS's solution was far superior.

a. DoD Arbitrarily Minimized AWS's Advantage in Logical Isolation and Separation.

Factor 2 required DoD to evaluate offerors' proposed logical isolation and separation architecture and implementation for unclassified and classified offerings, as well as their solutions for secure data transfer. AR Tab 342 at 151492. With respect to logical isolation and separation, the RFP emphasized the importance of the hypervisor, which is the core technology that allows users to create, manage, and secure scalable virtual machines within cloud environments. *Id.* With respect to secure data transfer, the RFP emphasized the importance of transferring data between

logical enclaves within the JEDI Cloud, to external destinations, and across classification levels.

Id. When making its source selection decision, DoD failed to evaluate proposals equally and in accordance with these criteria.

AWS's proposal detailed how Nitro represents a leap forward in hypervisor technology because it leverages purpose-built hardware, firmware, and software modules to virtualize network and storage resources for DoD users. AR Tab 368 at 152762-63. This hardware-based architecture offers unparalleled security because, among other things, it eliminates the risk of devastating "hypervisor breakout attacks," in which malicious actors break out of user-designated space and hijack the trusted space operated by the cloud administrator to take control over users' virtual machines. *Id.* at 152795.

Despite recognizing that AWS's hypervisor solution is a [REDACTED]

[REDACTED]

[REDACTED] the SSAC downplayed its significance because there allegedly was [REDACTED]

[REDACTED]

[REDACTED] and because [REDACTED]

[REDACTED]

[REDACTED] AR Tab 457 at 176400-

01. Both of these reasons for discounting the technical advantages of Nitro's security capabilities are dead wrong.

First, AWS's hardware-backed solution unequivocally is far superior in mitigating the severity of hypervisor attacks. The TEB—which of course was comprised of DoD's technical experts—[REDACTED]. AR Tab 323 at 151129-31. The SSEB also recognized [REDACTED], calling it

[REDACTED]

[REDACTED]

[REDACTED] AR Tab 456 at 176369. The SSAC, which lacked the TEB's and the SSEB's technical expertise, was simply wrong to discount the superiority of AWS's hardware-based solution.

Second, as the TEB explicitly noted, [REDACTED]

[REDACTED]:

[REDACTED]

AR Tab 329 at 151247 (emphasis added); *see also id.* at 151249. Although, as the SSAC noted, many cyberattacks are based on user error (*e.g.*, poorly written software, misconfigured software, *etc.*), hypervisor breakout attacks are much more devastating because a malicious actor can gain access and control over sensitive user virtual machines without the victim's knowledge. In downplaying this security risk, the SSAC ignored the fact that hypervisor breakout attacks are often enabled by user error within individual customer environments. The SSAC also overlooked the fact that Factor 2 specifically focused on hypervisor security. AR Tab 342 at 151492. It thus was simply incorrect for the SSAC to downplay the importance of hypervisor attacks.

Moreover, in addition to substantially mitigating the severity of hypervisor breakout attacks, Nitro significantly mitigates, or completely eliminates, the risks associated with the other types of cyberattacks cited by the SSAC—as well as insider threats, data exfiltration/theft, and many other infrastructure vulnerabilities—by eliminating administrator access to customer cloud environments and enabling active monitoring of all interactions. AR Tab 370 at 152834; AR Tab

323 at 151130. Nitro also uses [REDACTED] to ensure the security and integrity of the Nitro boot process and interface prior to software deployment, and it allows for patching in milliseconds—which far exceeds the RFP’s requirement for patching within eight hours of a vulnerability notification (SOO at 14 (Table 5.1))—without disruption to customer workloads. AR Tab 370 at 152827-29, 152831. Thus, even if hypervisor attacks were not a serious concern (as the SSAC erroneously suggests), AWS’s Nitro solution still provides [REDACTED]

The SSAC’s efforts to minimize AWS’s comparative advantage in logical isolation and separation did not stop there. In addition to understating the importance of Nitro, the SSAC manufactured an advantage for Microsoft with respect to [REDACTED]—[REDACTED] [REDACTED]—by erroneously finding:



AR Tab 457 at 176401 (emphasis added). This is inaccurate.

AWS proposed both its [REDACTED] [REDACTED].¹⁹ AWS

¹⁹ To the extent DoD ignored [REDACTED] offering because it is still under development, this was unreasonable and disparate, given DoD gave Microsoft credit for proposing solutions currently under development in other areas. For example, the RFP required offerors to demonstrate their capability to tag both resources *and* objects (*i.e.*, a type of resource) for billing

[REDACTED]

proposed [REDACTED] AR
Tab 368 at 152797. In addition, AWS proposed [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] *Id.* Thus, directly
contrary to the SSAC's finding, AWS proposed a [REDACTED]
[REDACTED]. Microsoft's perceived advantage simply does not exist.

In light of all this, DoD's conclusion that AWS and Microsoft proposed equal solutions to logical isolation and secure data transfer is unreasonable. Because both offerors proposed a [REDACTED], AWS's hardware-backed hypervisor is the remaining key discriminator for Factor 2. DoD therefore should have assigned AWS higher ratings than Microsoft under Factor 2, or at least recognized that AWS was qualitatively superior.

b. DoD Failed to Recognize AWS's Nitro Architecture Ensures the Highest Level of Information Security.

Factor 4 required DoD to evaluate offerors' approaches to information security by assessing each offeror's physical and logical isolation capability (*e.g.*, the hypervisor), automated breach identification and mitigation capability, and patching capability. AR Tab 1 at 91. When evaluating AWS's proposal, DoD failed to recognize key features that AWS's Nitro architecture provides to deliver the highest level of information security currently possible.

tracking, access control, and assignment of technical policy. AR Tab 342 at 151506. Microsoft, however, [REDACTED] AR Tab 411 at 173674. It [REDACTED] AR Tab 408 at 173306; *see also id.* at 173239-40. Yet DoD determined [REDACTED] AR Tab 331 at 151306.

As discussed above, AWS proposed its purpose-built Nitro architecture to provide DoD with the most secure hypervisor available. One of the key features of the Nitro architecture is that host hardware cannot access the cloud infrastructure unless AWS first provisions resources (such as CPU, storage, or network) to cloud users. AR Tab 370 at 152830-31. The provisioning process includes a strong technical control that overwrites all firmware on host hardware, eliminating the possibility that compromised hardware will access the cloud. *Id.* at 152831.

Moreover, the Nitro architecture provides substantial security benefits for supply chain integrity by leveraging [REDACTED] to ensure the integrity of firmware accessing the cloud. *Id.* When a host accesses a virtual machine, Nitro holds the system [REDACTED] [REDACTED]. *Id.*

AWS's Nitro architecture also includes AWS's proprietary, automated patching technology, which allows AWS to "hot-patch" millions of virtual machines in *milliseconds*—far exceeding the RFP's 8-hour patching requirement (AR Tab 7 at 191-95)—*without disruption* to DoD operations. AR Tab 370 at 152827-29.

Finally, Nitro substantially mitigates the risks of insider threats and data exfiltration/theft by eliminating administrator access to customer cloud environments and enabling active monitoring of every single interaction. AR Tab 370 at 152834. DoD's failure to recognize these critical information security features under Factor 4 was unreasonable and again created false parity between the offerors. Under a rational evaluation, DoD would have determined AWS's information security solution was qualitatively superior to Microsoft's.

2. DoD Miscalculated AWS's Third-Party Marketplace Offerings Based on Misleading and Unequal Discussions.

Factor 5 required DoD to evaluate offerors' proposed approach to application and data hosting and application and data portability. AR Tab 342 at 151496. In this regard, offerors were required to "[p]rovide the ability to rapidly and securely deploy [cloud service provider] and third-party platform and software service offerings from an online marketplace with baseline template configurations." AR Tab 27 at 616.

AWS's proposal included [REDACTED] third-party marketplace offerings available at award from [REDACTED] Independent Software Vendors. See AR Tab 371 at 152848. Those offerings included third-party software in unclassified cloud environments—where AWS runs the largest cloud software marketplace in the world—and in classified cloud environments—where AWS is the *only* cloud service provider with an authorization to operate. See AR Tabs 381-384.

Even though these offerings met DoD requirements, DoD incorrectly determined "[REDACTED] [AWS's] marketplace offerings [are] not part of the JEDI Cloud catalog at the time of award." AR Tab 457 at 176402. DoD apparently reached this erroneous conclusion because AWS

[REDACTED]

[REDACTED]. *Id.* DoD incorrectly interpreted this [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] *Id.* at 176403.

DoD's conclusion ignored AWS's explicit explanation of [REDACTED]

[REDACTED]:

[REDACTED]

[REDACTED]

AR Tab 375 at 154075 (emphasis added). In other words, AWS's proposal made clear that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] And, in fact, these marketplace offerings plainly were included in AWS's proposed price catalogs and available to DoD at award. See AR Tabs 380-385.

DoD's contrary interpretation is especially problematic given [REDACTED]

[REDACTED]

[REDACTED]. AWS and DoD discussed how to balance the RFP's requirements for commercial parity and security, after DoD noted that [REDACTED]

[REDACTED] AR Tab 455 at 176356. As the PEB observed, based on these discussions:

[REDACTED]

[REDACTED]

[REDACTED]

AR Tab 455 at 176356 (emphasis added). Thus, the record shows DoD not only [REDACTED]
[REDACTED]
[REDACTED]. *See id.*

Critically, the record does not indicate DoD similarly informed Microsoft that [REDACTED]
[REDACTED]. *See id.* Instead, it
appears DoD simply assumed that [REDACTED]
[REDACTED], stating:

[REDACTED]

AR Tab 457 at 176403.

Thus, in addition to lacking a rational basis for concluding AWS could not provide its proposed third-party marketplace offerings at award, DoD also held unequal and misleading discussions with AWS that skewed the Factor 5 evaluation in Microsoft's favor. DoD's disparate and unreasonable evaluation prejudiced AWS. As the SSDD makes clear, DoD considered Microsoft's [REDACTED] Microsoft was "significantly superior" under Factor 5. AR Tab 459 at 176416. The AR, however, shows [REDACTED] to be a farce. In reality, AWS proposed the superior third-party marketplace. Under a rational evaluation, DoD would have determined AWS was superior to Microsoft, for this aspect of Factor 5.

C. DoD Miscalculated the AWS and Microsoft Proposals in a Host of Other Ways.

DoD committed a litany of additional errors that exacerbated the serious evaluation discrepancies discussed above. First, DoD unreasonably removed previously recognized strengths under Factors 2 and 5 from AWS's final evaluation, even though AWS did not remove those strengths from its proposal, and Microsoft [REDACTED] [REDACTED]. Second, DoD failed to assign AWS several strengths for exceeding the Factor 8 demonstration requirements in ways beneficial to DoD. Third, DoD failed to evaluate AWS's management approach reasonably, arbitrarily reviewing an outdated version of AWS's proposal, misreading AWS's cloud support offering, and failing to appreciate AWS's proven approach to contract performance. Each of these errors further skewed the evaluation in Microsoft's favor.²⁰

²⁰ In addition to the evaluation errors discussed herein, AWS's Complaint highlights additional instances in which DoD either failed to recognize clear strengths in AWS's proposal, or assigned AWS unwarranted weaknesses and risk increases. *See* Compl. ¶¶ 113-14, 120(a)-(d), 136(a)(c), 150(a)-(d). The AR confirms these allegations have merit as well. *See* AR Tab 367 at 152646 (explaining AWS's proposed [REDACTED]); AR Tab 368 at 152797(same); AR Tab 323 at 151160-61 (acknowledging benefits of [REDACTED]); AR Tab 367 at 152648 (showing AWS can apply [REDACTED]); AR Tab 368 at 152789 (showing AWS [REDACTED]); AR Tab 367 at 152656 (showing only [REDACTED]); AR Tab 367 at 152602 (showing AWS's PWS clearly states AWS [REDACTED]); AR Tab 370 at 152842-43 (explaining AWS's proposed [REDACTED]); AR Tab 370 at 152844 (showing AWS [REDACTED]); AR Tab 370 at 152845 (explaining benefits of AWS's [REDACTED]); AR Tab 367 at 152603 (showing AWS proposed [REDACTED]); AR Tab 371 at 152856 (showing AWS proposed over [REDACTED] when the RFP only required three (AR Tab 27 at 615)); AR Tab 371 at 152849 (showing AWS proposed most [REDACTED]); AR Tab 371 at 151846 (showing AWS proposed [REDACTED]).

1. DoD Removed Previously Recognized Strengths Only from AWS's Final Evaluation.

In its apparent attempt to identify differentiators that justified award to Microsoft, DoD failed to recognize actual discriminators that demonstrated AWS's technical superiority. In its February 19, 2019 evaluation of AWS's initial proposal submission for Factor 2, DoD identified several strengths and one risk reduction that DoD inexplicably omitted from its final evaluation, even though AWS did not remove these strengths and risk reductions from its proposal. See AR Tab 441 at 176319 (noting AWS's "IPR [Interim Proposal Revision] is nearly identical to the final proposal revision"). The features earning these strengths and risk reductions included (1) network mapping (*i.e.*, virtual networking) (AR Tab 206 at 57906); (2) cryptographic protections for disk storage and network traffic in hardware (*id.* at 57906-07); (3) marketplace offerings (*id.* at 57924); (4) AWS's CloudFormation service (*id.* at 57924); and (5) AWS's "network design and implementation" (*id.* at 57915).

Similarly, in its January 11, 2019 evaluation of AWS's initial proposal submission for Factor 5, DoD identified three strengths: (1) [REDACTED] [REDACTED] (AR Tab 212 at 58033); (2) [REDACTED] (*id.* at 58035); and (3) AWS's mature marketplace (*id.* at 58035-36). Despite recognizing that AWS's "IPR is nearly identical to the final proposal revision," the TEB inexplicably omitted each of these three strengths in AWS's final evaluation, stripping AWS of key discriminators that should have further established its technical superiority under each factor. Compare AR Tab 323 with AR Tab 447 at 176326; compare AR Tab 326 with AR Tab 450 at 176330. [REDACTED]

Compare AR

Tabs 207, 209, 211, 213, 215 with AR Tabs 329-333, 441-445. Such disparate treatment was highly prejudicial to AWS, given that DoD inexplicably concluded that Microsoft and AWS were equal under Factor 2, and that Microsoft was significantly superior to AWS under Factor 5 [REDACTED] AR Tab 459 at 176415-16.

2. AWS Deserved Several Additional Strengths for Exceeding Demonstration Requirements.

During the second demonstration of its cloud computing solution, AWS exceeded several of the metrics established by DoD to assess the offerors' technical capability, yet DoD failed to assign corresponding strengths to AWS.

Under Scenario 8.1, offerors were required to demonstrate a compute value of 120 seconds and an object storage value of 120 seconds. See AR Tab 307 at 64387; AR Tab 27 at 620. AWS exceeded these requirements by demonstrating [REDACTED], and reporting [REDACTED], but DoD did not credit AWS with a strength. See AR Tab 307 at 64387.

Scenario 8.3 also required offerors to demonstrate successful execution of cloud services using their proposed tactical edge devices. See AR Tab 270 at 63045; see also AR Tab 287 at 64175. AWS executed [REDACTED]. See AR Tab 307 at 64394-97. By contrast, Microsoft [REDACTED]. See AR Tab 308 at 64416. Although DoD listed the number of services AWS demonstrated, it failed to credit AWS's breadth and depth of services, which exceeded the minimum requirements for Scenario 8.3.

Scenario 8.3 required offerors to demonstrate a compute value and an object storage value of 120 seconds or less, and a block storage value of 60 seconds or less. See AR Tab 307 at 64397; AR Tab 27 at 620. During the second demonstration, AWS demonstrated [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]. See AR Tab 307 at 64397. Yet, again, AWS did not receive a strength.

DoD's failure to recognize these strengths prejudiced AWS. Microsoft's demonstration performance is in no way comparable. See *supra* Section I(A)(2). Nonetheless, DoD assigned AWS and Microsoft the same ratings. AR Tab 459 at 176414. Notwithstanding the errors discussed in Section I(A)(2) above, had DoD appropriately recognized these strengths, DoD at least would have determined AWS's demonstrations were qualitatively superior to Microsoft, notwithstanding the arbitrary ratings assigned.

3. DoD Unreasonably Evaluated the Offerors' Management Approaches.

DoD unreasonably determined Microsoft's proposal is technically superior to AWS's under Factor 6. AR Tab 457 at 176403. Factor 6 required DoD to evaluate five areas: (1) program management approach, (2) timely remediation of issues, (3) risk management process, (4) quality assurance surveillance plan, and (5) property management system. See AR Tab 342 at 151496-97. DoD also was to evaluate the degree to which each offeror's proposal reflects an understanding of DoD's requirements in Sections 3 and 5 of the SOO. See *id.* at 151504. DoD failed to perform its evaluation reasonably.

First, DoD evaluated a prior version of AWS's proposal. AWS's FPR (as well as its IPR submission on July 15, 2019) states: [REDACTED]

[REDACTED]
[REDACTED] AR Tab 367 at 152671 (emphasis added); AR Tab 312 at 140330. An

AWS Region is a geographic location where AWS provides multiple, physically separated and isolated Availability Zones, each of which consists of one or more distinct data centers. AR Tab 367 at 152594. [REDACTED]

Nevertheless, the TEB erroneously found that AWS proposed [REDACTED]. AR Tab 327 at 151216. Based on this finding, [REDACTED], the TEB concluded that AWS [REDACTED]. *Id.* In actuality, however, AWS's proposal exceeded the "standard" [REDACTED]. The TEB's conclusion was completely unreasonable.

Second, DoD incorrectly concluded [REDACTED], and then arbitrarily relied on this incorrect conclusion as a discriminator between the offerors. AR Tab 457 at 176403. Specifically, the SSAC stated there was a "notable difference" between AWS and Microsoft because AWS allegedly [REDACTED]. *Id.* Microsoft received [REDACTED]. AR Tab 333 at 151339. AWS's proposal, however, was explicit that [REDACTED]. AR Tab 375 at 154083. DoD, therefore, was incorrect that [REDACTED] was a discriminator, and AWS actually deserved the versus Microsoft strength for this aspect of its proposal.

Third, DoD ignored AWS's proven and tested management approach, which leveraged its extensive experience providing unclassified and classified cloud services and support. AR Tab 372 at 152872. As a result, AWS was able to provide DoD with a proven and tested approach for

[REDACTED]

completing contract requirements on schedule and in accordance with the JEDI Contract's quality and performance metrics. *See id.* [REDACTED]

[REDACTED] DoD inexplicably concluded Microsoft, and not AWS, demonstrated an exceptional approach and understanding of the Management requirements. AR Tab 459 at 176414.

But for DoD's unreasonable evaluation of the offerors' management approaches under Factor 6, AWS would have assigned AWS an Outstanding rating and found AWS to be qualitatively superior to Microsoft for this factor.

II. THE REMAINING INJUNCTIVE FACTORS ALL FAVOR AWS.

When AWS filed its Complaint in this case, AWS did not seek temporary or preliminary injunctive relief because the Government had agreed that, through February 11, 2020, DoD would limit Microsoft's performance to the following initial activities, many of which were not formal requirements and would not require payment under the JEDI Contract: (1) conducting a kickoff event, (2) initializing network connectivity, (3) placing enterprise tools into Microsoft's cloud environment, (4) performing tactical edge device testing, (5) validating cross domain solutions, and (6) conducting provisioning tool integration. *See* Appendix, Exhibit 1, DoD Summary of Preparatory Activities at 1-2.

Despite the Complaint's serious allegations and the evidentiary support for those allegations in the AR, the Government more recently indicated it will direct Microsoft to proceed with the following significant JEDI Contract activities beginning February 12, 2020: (1) "preparatory activities," such as training, support, and advisory services, which DoD proposes to perform pursuant to 15-20 additional task orders issued under CLIN 3 of the JEDI contract; and (2) the "onboarding" of "pilot users," which the Government represents will involve pilot users

placing orders in the JEDI provisioning tool, DoD providing such users an account in JEDI, and the users beginning to use JEDI cloud services (collectively, “Additional Activities”). *See* Appendix, Exhibit 2, DoD Summary of Additional Activities.

The Government has stated DoD is willing to limit Microsoft’s JEDI performance to these Additional Activities until February 29, 2020, and characterizes the activities as both largely preparatory and necessary for national security. *Id.* The Government also claims that unlimited Microsoft performance on JEDI is necessary for national security reasons starting March 1, 2020. *Id.* The Government’s characterization of the Additional Activities, however, is inaccurate and misleading, as is its justification for proceeding with JEDI performance.

Notwithstanding the Government’s representations, DoD’s performance of the JEDI Contract is intended to entrench Microsoft as the JEDI contractor and deny AWS adequate relief if it prevails in its protest.²¹ Indeed, despite its references to national security, DoD has provided no explanation for the alleged urgency of the training, support, and advisory services. *Id.* And, with respect to the onboarding of pilot users, the Government has stated only that “[i]t is critical that some pilot users are onboarded in February, to permit lessons learned in support of validating and optimizing the onboarding process.” *Id.* Accordingly, AWS now asks the Court to grant the immediate injunctive relief necessary to avoid the irreparable harm that DoD’s and Microsoft’s continued contract performance will inevitably cause.

²¹ Although the Government has stated none of these “preparatory activities” would affect the relief available if AWS were to prevail in its protest, the Government likely will still argue in its Motion for Judgment on the Administrative Record that Microsoft’s performance of these “preparatory activities” weighs against granting permanent injunctive relief.

A. Continued Performance of the JEDI Contract Will Result in Immediate and Irreparable Harm to AWS.

Whether AWS will suffer irreparable harm without injunctive relief in this case depends on “whether [AWS] has an adequate remedy in the absence of an injunction.” *NetStar-1 Gov’t Consulting, Inc. v. United States*, 101 Fed. Cl. 511, 530 (2011). AWS does not. As discussed below, the type and severity of harm AWS will suffer without an injunction both warrant immediate injunctive relief.

“[E]conomic harm suffered from the loss of an opportunity to fairly compete for a government contract constitutes, in many if not most cases, irreparable harm.” *HP Enter. Servs., LLC v. United States*, 104 Fed. Cl. 230, 245 n.13 (2012). Furthermore, “the loss of the contract represents not only irreparable injury in terms of lost profit, but also in terms of lost experience working with the government.” *FCN, Inc. v. United States*, 115 Fed. Cl. 335, 385 (2014); *see also Palladian Partners, Inc. v. United States*, 119 Fed. Cl. 417, 458 (2014) (reversed on appeal for unrelated reasons). If a party “cannot perform [the contract], then it will not have any remedy at law to recover the contract rights, benefits, and revenue accruing to [the awardee],” and it will suffer irreparable injury. *See FCN, Inc.*, 115 Fed. Cl. at 384-85; *Heritage of Am., LLC v. United States*, 77 Fed. Cl. 66, 78 (2007). AWS easily meets these legal standards.

In the absence of a temporary restraining order and preliminary injunction, AWS could lose the opportunity to perform the JEDI Contract, earn the revenue and profits resulting from contract performance, ensure its technology is widely used by DoD, and gain additional experience working with the Government. The JEDI Contract is a 10-year program that will transform DoD’s cloud architecture and define enterprise cloud for years to come. The winner of this contract will obtain not only an influx of work across DoD as components migrate their data to the JEDI cloud,

but also a competitive advantage for future cloud contracts across the federal government based on the technology developed and lessons learned.

Indeed, AWS has already begun to feel the impact of the JEDI award, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]. See Appendix, Exhibit 3, Declaration of Jennifer Chronis ¶ 6. Given the serious errors already evident in DoD's evaluation and source selection decision, DoD and Microsoft should not be permitted to perform the JEDI Contract any further until the Court resolves this bid protest.

Microsoft's performance of the Additional Activities on the JEDI Contract, unless enjoined, will also provide Microsoft with an unfair competitive advantage in any recompitation of the JEDI Contract resulting from AWS's protest. See e.g., *Cigna Gov't Servs., LLC v. United States*, 70 Fed. Cl. 100, 102-13 (2006) (finding stay override invalid where allowing awardees to continue performance would confer an "unfair competitive advantage" or "skew the playing field" in the event of a recompete). For example, although the Government has not described the "training, support, and advisory services" activities in detail, such work would undoubtedly give Microsoft access to non-public information that would allow Microsoft (but not AWS) to better tailor any revised proposal submitted in a JEDI recompitation. Appendix, Exhibit 3, Declaration of Jennifer Chronis ¶ 5. Only an injunction imposed by this Court will protect AWS from the irreparable harm to its competitive position, and indeed preserve its opportunity for meaningful relief, as the protest proceeds.

DoD's planned onboarding of pilot users will also affect AWS's existing contracts. Each of the pilot users DoD proposes to onboard [REDACTED] under an existing cloud

computing contract. *See* Appendix, Exhibit 3, Declaration of Jennifer Chronis ¶ 7. The onboarding [REDACTED] to the JEDI Cloud during the course of the protest [REDACTED] before the Court has had an opportunity to review the evidence and resolve AWS's bid protest on the merits. *Id.* Even if AWS ultimately prevails in its protest, [REDACTED] [REDACTED] *Id.* Further, [REDACTED] [REDACTED] [REDACTED] [REDACTED]. *Id.* The Court should issue an injunction to protect AWS from this irreparable harm.

B. The Balance of Hardships Favors Granting Injunctive Relief.

Neither the Agency nor Microsoft will suffer harm from the imposition of an injunction, whereas AWS will suffer irreparable harm if the Court does not grant temporary relief. Pausing contract execution for the brief period necessary to determine the legality of DoD's selection process for this critical defense initiative is the best way to protect national security.

All of DoD's cloud computing needs, including those for the pilot program agencies, are being satisfied today by existing cloud contracts with AWS, Microsoft, and other providers. And a host of existing contract vehicles for cloud computing services are available for the military's immediate and approaching requirements. *See* Appendix, Declaration of Jennifer Chronis ¶ 10. In fact, DoD has at its disposal more than 600 cloud initiatives across the Department. *See* AR Tab 88 at 5933; *see generally* AR Tab 165. Contrary to the Government's insinuations, no DoD command or agency is waiting for the JEDI Contract to fulfill current cloud computing needs. A brief delay in JEDI Contract performance during the pendency of the protest to allow for the

adjudication of serious claims of procurement irregularities will not deprive DoD of the means to satisfy its cloud computing needs. This simple fact weighs heavily against the Government as the Court considers the balance of harms for injunctive relief. *See Palantir USG, Inc. V. U.S.*, 129 Fed. Cl. 218, 293-294 (explaining Government already had functioning data system in place and, although the system could benefit from the updates being procured, it could still be used while injunction was in place).

Moreover, the JEDI Contract's implementation timeline, even in the *absence* of an injunction, will not provide DoD customers with substantive cloud services until well after the completion of the protest litigation. The only services-based delivery milestone within the first 120 days of JEDI Contract award is the delivery of unclassified services—all of which can be provided under existing contract vehicles for cloud computing services. AR Tab 27 at 610; Appendix, Exhibit 3, Declaration of Jennifer Chronis ¶ 10. Moreover, with respect to JEDI-specific classified services, DoD will not obtain these services until at least 180 days *after* conclusion of the post award kickoff event (for Secret services) and 270 days *after* the kickoff event (for Top Secret services). AR Tab 27 at 610. And, in any event, these classified needs also could be addressed through existing cloud contracts. *See id.* Thus, any assertions of harm by the Government are speculative and likely quite minimal. *See Palantir*, 129 Fed. Cl. at 293-294 (finding it unlikely that capabilities would be available and deployable before Army could properly award contract). This is especially true given that, if AWS prevails in the protest and ultimately receives the JEDI award, it can deliver classified services on Day One of contract performance. AR Tab 367 at 152595.

The context and timeline of the RFP and award process itself also demonstrate that the Government's claim of urgency is specious. The Agency's own conduct is the primary source of

delay related to the procurement and DoD had demonstrated a consistent lack of urgency in its administration of the JEDI procurement. DoD's claim of urgency is belied by the record. *See Reilly's Wholesale Produce v. United States*, 73 Fed. Cl. 705, 715-16 (2006) (granting injunctive relief where agency was cause of delay).

DoD first announced the program, and its plan to upgrade and consolidate its cloud infrastructure across the Agency, in September 2017 (more than two years ago). AR Tab 23 at 429. Not until almost a year later (in July 2018) did DoD issue a final RFP. AR Tab 1 at 1. In February 2019, DoD requested a stay of the proceedings so it could investigate potential conflicts of interest in response to Oracle's award protest. *See* Def's Unopposed Mot. to Stay, *Oracle Am., Inc. v. United States*, 144 Fed. Cl. 88 (2019) (No. 1-1880C), ECF No. 60, 62. This stay was not lifted until April 2019, when DoD determined there was no conflict of interest. *See* Order Lifting Stay, *Oracle Am., Inc. v. United States*, 144 Fed. Cl. 88 (2019) (No. 1-1880C), ECF No. 66. To accommodate this voluntary investigation, DoD delayed the start date of the base period of performance from April 2019 to July 2019. *See* AR Tab 301 at 64227.

DoD did not display the urgency it now claims after it closed that investigation. Rather than awarding the contract to allow performance by July 2019, DoD initiated a "review" of the JEDI procurement by Defense Secretary Mark Esper. Before Secretary Esper even commenced his review, he publicly confirmed there was no "hard timeline" for its completion, and certainly did not indicate imminent urgency for national security. *See* Anthony Capaccio, *Esper Has No 'Hard Timeline' for Review of \$10 Billion JEDI Deal* (Sep. 6, 2019), BLOOMBERG, <https://www.bloomberg.com/news/articles/2019-09-06/esper-has-no-hard-timeline-for-review-of-10-billion-jedi-deal>. As a result of the Esper review, which commenced in early August 2019, DoD did not award the JEDI Contract until late October 2019—well over a year after the issuance

of the final RFP and more than two years after DoD first announced the JEDI program.²² See AR Tab 481 at 176973.

Although a temporary restraining order and preliminary injunction may notionally delay the implementation of the JEDI Contract to some degree, that delay is minor compared to DoD's own processes, and, in any event, "only in an exceptional case would [such delay] alone warrant a denial of injunctive relief, or the courts would never grant injunctive relief in bid protests." *Palantir*, 129 Fed. Cl. at 294 (citations omitted).

Finally, the Court should not "blindly accede" to the Government's claim that national security implications make injunctive relief inappropriate in this case. See *GTA Containers, Inc. v. United States*, 103 Fed. Cl. 471, 493 (2012) (finding national security interests did not outweigh harm caused by flawed procurement process); *Bilfinger Berger AG Sede Secondaria Italiana v. United States*, 97 Fed. Cl. 96, 159 (2010) (noting "allegations involving national security must be evaluated with the same analytical rigor as other allegations of potential harm to parties or to the public"). Where, as here, an agency is utilizing, and can continue to utilize, existing contracting vehicles to satisfy its immediate needs, and its own dilatory conduct during the procurement process belies the new-found urgency, the Court need not deny injunctive relief based on claims of speculative harm to national security. See *Palantir*, 129 Fed. Cl. at 294 (finding that although procured updates were "desperately needed," Government could not identify immediate national security consequences in light of existing infrastructure and lengthy implementation period).

²² The Government has caused additional delay by waiting over one month to produce what proved to be an incomplete AR, thereby compelling AWS to move for an order directing the Government to complete the record and delaying the resolution of this protest further.

Invoking the gravity of national security never gives the government a free pass. And it is demonstrably *not* a valid reason to push forward with JEDI performance and cement Microsoft's practical incumbent status given AWS's already compelling demonstration of the obvious flaws in the selection process. National security is best served by a careful evaluation of AWS's protest to ensure DoD chooses the *true* best-value solution for this critical military program.

C. Injunctive Relief Is in the Public Interest.

The Government, as well as the public at large, has "a long-term interest in ensuring that any new contract for the services in question truly represents the best overall value to the government." *NetStar-1*, 98 Fed. Cl. at 735. Because "the public interest in honest, open, and fair competition in the procurement process is compromised whenever an agency abuses its discretion in evaluating a contractor's bid," the public interest also weighs in favor of injunctive relief. *See PGBA, LLC v. United States*, 57 Fed. Cl. 655, 663 (2003); *see also Palantir*, 129 Fed. Cl. at 294; *Cherokee Nation Techs., LLC v. United States*, 116 Fed. Cl. 636, 641 (2014). In this case, the AR, even in its current incomplete state, reveals egregious evaluation errors that have compromised the JEDI source selection process. The public interest weighs heavily in favor of injunctive relief under these exceptional circumstances.

DoD committed a host of egregious errors in the evaluation of the AWS and Microsoft proposals, leading DoD to award the JEDI Contract to Microsoft despite its inferior cloud solution and its defective proposed price. Allowing performance of the JEDI Contract to continue while the Court adjudicates this meritorious protest would undermine the integrity of the procurement system and waste taxpayer dollars. The public interest weighs in favor of injunctive relief to ensure the JEDI procurement is completed in accordance with law and regulation.

The public also has a vested interest in national security, and AWS's cloud solution best serves that interest. *See Palantir*, 129 Fed. Cl. at 294. AWS offers significantly greater cloud security and performance to DoD users than Microsoft. It also offers a proven and tested approach to the effective deployment of cloud infrastructure and platforms, substantially reducing the risk of unsuccessful performance. DoD's selection of an inferior solution does not serve the nation's national security interests, and, in fact, undermines it. And once Microsoft's illegitimate price advantage is eliminated, AWS is also the less expensive solution for the public fisc. The errors in the JEDI procurement are precisely the type of arbitrary and capricious conduct that have the capacity to "destroy the public trust in government contracting." *HP Enter. Servs.*, 104 Fed. Cl. at 246. Accordingly, the Court should grant the requested injunctive relief.

CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, AWS respectfully requests that the Court GRANT its motion for a temporary restraining order and a preliminary injunction.

Dated: January 22, 2020

Respectfully submitted,

By: _____



Kevin P. Mullen
Morrison & Foerster LLP
2000 Pennsylvania Ave., NW
Washington, DC 20006-1888
Telephone: 202.887.1500
Facsimile: 202.887.0763

*Attorney of Record for Plaintiff
Amazon Web Services, Inc.*

Of Counsel:

J. Alex Ward
Daniel E. Chudd
Sandeep N. Nandivada
Caitlin A. Crujido
Alissandra D. Young
Morrison & Foerster LLP
2000 Pennsylvania Ave., NW
Washington, DC 20006-1888

Andrew S. Tulumello
Daniel P. Chung
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 955-8500

Theodore J. Boutrous, Jr.
Richard J. Doren
Eric D. Vandavelde
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
(213) 229-7000