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.	Case No. _____ Judge _____ [redacted] **REDACTED VERSION**

[redacted] **COMPLAINT**

Amazon Web Services, Inc. ("AWS") protests the decision of the U.S. Department of Defense ("DoD") to award the Joint Enterprise Defense Infrastructure ("JEDI") Contract, Solicitation No. HQ0034-18-R-0077 ("RFP"), to Microsoft Corporation ("Microsoft").[1]

Throughout the JEDI procurement process, based on AWS's depth of experience, superior technology, and proven record of success in handling the most sensitive government data, AWS was the consensus frontrunner to aid DoD in this important modernization effort. Yet when the time came to make the award, DoD chose Microsoft. Any meaningful review of that decision reveals egregious errors on nearly every evaluation factor, from ignoring the unique strengths of AWS's proposal, to overlooking clear failures in Microsoft's proposal to meet JEDI's technical

[1] The Defendant has represented that DoD will not proceed with performance of the JEDI Contract beyond initial preparatory activities until at least February 11, 2020. Accordingly, AWS and Defendant have agreed that a temporary restraining order and preliminary injunction are not necessary at this time. AWS reserves the right to move for such immediate injunctive relief if DoD decides to proceed with performance in advance of this Court's resolution of AWS's protest.

[redacted]

requirements, to deviating altogether from DoD's own evaluation criteria to give a false sense of parity between the two offerors. These fundamental errors alone require reversal.

These errors, however, were not merely the result of arbitrary and capricious decision-making. They were the result of improper pressure from President Donald J. Trump, who launched repeated public and behind-the-scenes attacks to steer the JEDI Contract away from AWS to harm his perceived political enemy—Jeffrey P. Bezos, founder and CEO of AWS's parent company, Amazon.com, Inc. ("Amazon"), and owner of the *Washington Post*. DoD's substantial and pervasive errors are hard to understand and impossible to assess separate and apart from the President's repeatedly expressed determination to, in the words of the President himself, "screw Amazon." Basic justice requires reevaluation of proposals and a new award decision. The stakes are high. The question is whether the President of the United States should be allowed to use the budget of DoD to pursue his own personal and political ends.

I. INTRODUCTION

1. On dispassionate review of the technical merits alone, bedrock government procurement principles require overturning the award of the JEDI Contract to Microsoft. In granting that award, DoD committed numerous and compounding prejudicial errors, glossing over wide gaps between AWS's market-segment-leading cloud solution and Microsoft's offering, completely ignoring critical aspects of AWS's technical proposal, and overlooking key failures by Microsoft to comply with the RFP's stated requirements. These errors pervaded nearly every evaluation factor.

2. In a particularly egregious example that is plainly contrary to the factual record, DoD concluded under Factor 3 (Tactical Edge) that [redacted]. DoD

[redacted]

compounded this error by [redacted], while allowing Microsoft—[redacted]—to escape DoD's scrutiny as to Factor 3 entirely. Further exacerbating this fatal error, DoD also failed to recognize the proven benefits of AWS's Snowball Edge device, which is already in active use in the field today (including on the battlefield [redacted]) by numerous DoD organizations, [redacted]

3. Similarly, under Factor 6 (Management and Task Order ("TO") 001), DoD arbitrarily evaluated an outdated, superseded version of AWS's proposal. The full impact of this highly prejudicial error is difficult to calculate. [redacted] The evaluation documents identify numerous other instances where DoD also ignored the plain language of AWS's proposal. When confronted with this fact in AWS's debriefing questions, however, DoD declined to explain its conclusions, stating simply—despite the contrary evidence in the evaluation materials—that DoD evaluated the correct version of AWS's proposal.

4. Moreover, DoD arbitrarily and wrongly concluded that [redacted]

[redacted]

[redacted] DoD also erroneously concluded that [redacted] despite the fact that AWS [redacted] was and still is the only contractor that has a proven approach for managing, developing, and deploying classified and unclassified cloud infrastructure and platforms at the scale contemplated by JEDI.

5. Under Factor 2 (Logical Isolation and Secure Data Transfer), DoD fundamentally misunderstood AWS's cloud solution. In particular, DoD arbitrarily omitted from its final evaluation—without explanation—previously assessed strengths, such as for AWS's virtual networking functionality, cryptographic protections, marketplace offerings, CloudFormation service, and network design and implementation. DoD also deviated from the RFP by failing to meaningfully consider offerors' proposed hypervisors, a foundational security and operational control element and an area where AWS has clearly distinguished itself from Microsoft through its novel Nitro architecture. Further, DoD failed to recognize other beneficial aspects of AWS's proposal [redacted], while also [redacted].

6. Under Factor 4 (Information Security and Access Controls), DoD again deviated from the RFP's criteria by failing to consider offerors' capabilities with respect to isolation, patching, access control configuration, data and resource tagging, and token-based and time-limited federated authentication. Specifically, DoD failed to recognize that AWS's Nitro architecture provides improved information security to DoD users. DoD also overlooked AWS's robust access control capabilities, which include role- and attribute-based access controls, the

[redacted]

ability to tag resources and objects for various functions, and the ability to leverage token-based authentication.

7. Under Factor 5 (Application and Data Hosting and Portability), DoD irrationally concluded that the [redacted] unique third-party marketplace offerings included in AWS's proposal would not be available at the time of award. In fact, AWS's proposal makes clear the contrary is true—[redacted] are available ***at award*** in the unclassified marketplace, with many of these offerings also available at award in the classified marketplace. DoD's unfounded and incorrect conclusion is particularly egregious given that AWS operates the largest cloud software marketplace in the world, and is the ***only*** cloud service provider with a classified cloud software marketplace. DoD also arbitrarily omitted from its final evaluation—again without explanation—previously assessed strengths, [redacted]. And DoD overlooked other strengths (such as AWS's Content Delivery Network Points of Presence, [redacted], its advanced graphics-processing unit and high-memory compute instance types, and its machine learning/artificial intelligence and managed database capabilities) when conducting its final evaluation of AWS's proposal.

8. Under Factor 8 (Demonstration), DoD again deviated from the RFP by failing to consider the extent to which AWS successfully demonstrated its technical approach for Factors 1 through 6. Specifically, DoD failed to acknowledge the numerous instances in which AWS's demonstrated capabilities vastly exceeded performance requirements—while ignoring instances where Microsoft necessarily failed to demonstrate its solution met the technical requirements of the JEDI SOO.

[redacted]

9. In committing the foregoing evaluation errors—and many others—DoD failed to meet its minimum obligation to apply the RFP's stated evaluation criteria reasonably, consistently, and in a fair and equal manner among all offerors. This arbitrary and capricious evaluation created a false parity between the two competitors' technical capabilities, notwithstanding AWS's depth of experience, superior technology, and record of success in handling the most sensitive government data at hyperscale data centers dedicated to serving [redacted] and DoD.

10. Despite the clear factual record establishing AWS's technical superiority over Microsoft—including broad consensus among industry analysts and experts who assessed AWS as the clear frontrunner for the JEDI Contract—DoD did not accurately assess AWS's technical superiority regarding essentially every meaningful aspect of DoD's requirements. As a result, DoD created the illusion that [redacted] Even viewed in isolation from all of the other foregoing defects, however, AWS's more relevant and highly successful experience managing [redacted], combined with DoD's obvious errors when evaluating AWS's proposal under Factor 6, underscore the thin veneer DoD artificially and improperly used to distinguish Microsoft's offering.

11. DoD further compounded its errors through its targeted efforts to drive up AWS's price [redacted]. [redacted]. Under ordinary government contracting principles, these fundamental errors, alone, which combined to skew improperly the best-value determination in Microsoft's favor, require termination of the JEDI Contract and a reevaluation of the proposals.

[redacted]

12. But in this extraordinary case, another, more fundamental defect also demands reevaluation of the award: the intervention of President Trump, Commander in Chief of the U.S. Military and head of the Executive Branch, in the JEDI procurement and award. This intervention destroyed the requisite impartial discharge of the government procurement process, making it impossible for DoD to meet its minimum obligation to apply the RFP's stated evaluation criteria reasonably, consistently, and in a fair and equal manner among all offerors. President Trump's intervention casts the errors discussed above in an even harsher light and puts the very integrity of the government procurement process in question.

13. The government procurement process—through which hundreds of billions of taxpayer dollars are awarded each year to provide essential government services, including to our nation's military—demands objective and even-handed administration based on facts and fair comparisons, not personal animus and undue influence. In this case, the President made it widely known to everyone—including on publicly broadcast television and through his prolific tweets—that DoD should not award the JEDI Contract to AWS. The blatant, inexplicable errors in DoD's award to Microsoft make plain that President Trump's message had its intended and predictable effect.

14. The publicly available record of President Trump's statements and actions demonstrates that he repeatedly attacked and vilified his perceived political enemy—Mr. Bezos, the founder and CEO of AWS's parent company, Amazon, and who separately owns the *Washington Post*—and then intervened in this procurement process to thwart the fair administration of DoD's procurement of technology and services critical to the modernization of the U.S. military.

15. President Trump has made no secret of his personal dislike for Mr. Bezos, Amazon, and the *Washington Post*, or of his express desire to harm them. The seeds of this animus originate with the *Washington Post*'s coverage of him before he even was elected President. That coverage placed Mr. Bezos, Amazon, and the *Washington Post* directly in the crosshairs of President Trump's wrath.

16. For example, in February 2016, then-candidate Trump made this promise during a campaign rally about what would happen to Amazon if he was elected President: "[B]elieve me, if I become president, oh do they have problems. They're going to have such problems." A few months later, he repeated this sentiment, accusing Amazon of "getting away with murder," and "rigg[ing]" the system, and proclaiming that Mr. Bezos uses the *Washington Post* "as a tool for political power against [him]" while declaring "[w]e can't let him get away with it."

17. After he assumed office, President Trump grew "obsessed" with Mr. Bezos and determined to "f*** with him."[2] His new powers expanded his ability to punish Mr. Bezos for the *Washington Post*'s coverage of him.

18. Since the JEDI procurement was announced, the President has reaffirmed his hostility towards Amazon and, as even the public record strongly suggests, has used his office to prevent AWS from winning the JEDI Contract. These efforts range from his own public statements and tweets to pronouncements from the highest levels of power within his Administration. They have been on full display for the whole country to see, including the members of the TEB, the Source Selection Evaluation Board ("SSEB"), the Source Selection Advisory Committee

---

[2] Gabriel Sherman, *"Trump Is Like, 'How Can I F—k With Him?'": Trump's War With Amazon (And The Washington Post) Is Personal*, Vanity Fair (April 2, 2018), https://www.vanityfair.com/news/2018/04/trump-war-with-amazon-and-the-washington-post-is-personal.

("SSAC"), and the Source Selection Authority ("SSA"), all of whom serve under President Trump's command.

19. For example, following months of scathing tweets about Mr. Bezos and Amazon in the summer of 2018 (a time when industry analysts widely reported AWS to be best qualified to win the JEDI Contract), the Commander in Chief directed his then-Secretary of Defense James Mattis to "screw Amazon" out of the contract, as recounted in a book published by Secretary Mattis's former chief speechwriter and Pentagon insider.

20. Similarly, during a press conference held on July 18, 2019, President Trump claimed that he had been getting "tremendous complaints about the contract with the Pentagon and with Amazon," and that he had heard "complaining from different companies, like Microsoft and Oracle and IBM." He then declared that he personally "will be asking [DoD] to look at it very closely to see what's going on." That same day, President Trump's eldest son, Donald Trump, Jr., alleged in a tweet that Mr. Bezos and Amazon had engaged in "shady and potentially corrupt practices," and he ominously predicted that it "may come back to bite them" with respect to JEDI. President Trump doubled down on these statements on July 22, 2019, when he tweeted television coverage decrying the JEDI Contract as the "Bezos bailout." Each of these messages came while DoD was evaluating the JEDI proposals and it would have been virtually impossible for anyone involved in JEDI to ignore them.

21. President Trump's attacks were relentless, and he resorted to increasingly aggressive tactics to carry out his apparent personal goal of preventing Mr. Bezos and AWS from receiving the JEDI Contract. In early August 2019, President Trump—in an unprecedented move—intervened directly in the very final phases of the two-year procurement process. President Trump directed his newly appointed Secretary of Defense, Mark Esper (who replaced Secretary

Mattis after President Trump claimed to have "essentially fired" Mattis following repeated clashes with the President's leadership), to conduct an "independent" examination. President Trump's improper direct intervention, its upending of the procurement, and the President's personal goal of preventing AWS from receiving the JEDI Contract were widely reported at the time: "The White House reportedly directed the Department of Defense to review a $10 billion cloud contract because it would probably go to Amazon."[3]

22. As President Trump's tweets against Mr. Bezos, Amazon, the *Washington Post*, and the JEDI bid process piled up, DoD took numerous actions to systematically remove the advantages of AWS's technological and experiential superiority and artificially level the playing field between AWS and its competitors, including Microsoft.

23. For example, in mid-2018, DoD refused to evaluate past performance—which only AWS possessed with regard to a contract remotely comparable to the size and complexity of JEDI—contrary to the applicable requirements of FAR Subparts 12.206 and 15.304. This was an unusual decision, given the JEDI Contract's significant national security implications and the fact

---

[3] Matt Weinberger, *The White House Reportedly Directed the Department of Defense to Review a $10 Billion Cloud Contract Because It Would Probably Go to Amazon*, Business Insider (Aug. 1, 2019), https://www.businessinsider.my/sec-of-defense-to-look-into-10-billion-jedi-contract-2019-8/; *see also, e.g.*, Rosalie Chen, *President Donald Trump Reportedly Wants to 'Scuttle' the $10 Billion Pentagon Cloud Contract that Amazon and Microsoft are Fighting Over*, Business Insider (July 26, 2019), https://www.businessinsider.com/trump-jedi-cloud-contract-amazon-microsoft-oracle-2019-7; Ari Levy, *Trump Says He's Looking into a Pentagon Cloud Contract for Amazon or Microsoft Because 'We're Getting Tremendous Complaints,'* CNBC (July 18, 2019), https://www.cnbc.com/2019/07/18/trump-says-seriously-looking-into-amazons-pentagon-contract.html; Jim Osman, *Why Amazon Could Be Trumped in Its JEDI Mission*, Forbes (June 7, 2019), https://www.forbes.com/sites/jimosman/2019/06/07/amazon-jedi-trump-microsoft-walmart-oracle-tech/#7b7c359a31f1; Idrees Ali & Nandita Rose, *Pentagon Puts $10 Billion JEDI Contract on Hold After Trump Suggests It Favored Amazon*, Reuters (Aug. 1. 2019), https://www.reuters.com/article/us-amazon-com-jedi/pentagon-puts-10-billion-jedi-contract-on-hold-after-trump-suggests-it-favored-amazon-idUSKCN1UR5UA.

that the FAR explicitly states past performance "should be an important element of every evaluation and contract award for commercial items."

24. Further, in the spring of 2019, DoD required AWS to make various changes to its technical proposal that forced AWS [redacted]. For example, RFP Amendment 0005 in May 2019 required offerors [redacted]—even though DoD's technical evaluators had previously confirmed AWS's proposed solution was "realistic and feasible"—[redacted]. Amendment 0005 also created a new and artificial limitation on technical solutions, without any justification, by requiring offerors to [redacted] in the Price Scenarios. [redacted]—driving up AWS's total evaluated price by [redacted]—a [redacted] increase over AWS's initial total evaluated price. And at the eleventh hour—months after DoD completed its evaluation of AWS's initial proposal, and after the conclusion of all scheduled discussions—DoD changed its interpretation of the RFP's classified infrastructure requirements, effectively rejecting AWS's long-standing plan to utilize existing data centers already certified for classified use and instead requiring AWS to build new dedicated classified infrastructure for DoD. There was no technical basis for this change—which could only impact AWS as the only cloud provider with existing classified infrastructure—and it resulted in an additional [redacted] increase to AWS's total evaluated price. These and other late-breaking DoD-directed changes—all of which arose after DoD's discussions with offerors and focused disproportionately on AWS's unique capabilities—were unnecessary from a technical and overall mission perspective and increased AWS's total

[redacted]

evaluated price [redacted] and arbitrarily leveling the playing field.

25. In addition to these overt changes, DoD evaluators applied a watered-down, "check the box" analysis for many factors—ignoring AWS's numerous technical advantages despite evaluation criteria requiring a comparative analysis in connection with the best value determination—to conclude both offerings were "good enough." Under this approach, the evaluators ignored numerous features that make AWS objectively superior to Microsoft from technical, security, and risk perspectives. These features include AWS's more advanced cloud and security architecture and its demonstrated and accredited ability—unlike any other competitor—to manage Secret and Top Secret classified information, something AWS has been doing [redacted] since 2013.

26. The SSAC further skewed the analysis in favor of Microsoft. The SSEB—which consists of individuals responsible for considering the TEB's input, further evaluating offerors' technical proposals, and providing recommendations to the SSAC—concluded that AWS's core cloud security architecture is "extraordinary" and explicitly recognized the positive impact AWS's technical approach would have on the security of DoD's most critical information. Yet in the midst of the President's campaign against AWS, the SSAC issued a written and comparative analysis that disregarded the SSEB's conclusion entirely. Compounding that gross omission, the SSAC proffered a pretextual reason for disregarding the SSEB's conclusion: [redacted]. It also is inconsistent with previous concerns raised by DoD, and in

[redacted]

particular the Defense Information Systems Agency (DISA), the agency that is responsible for providing information technology (IT) and communications support across DoD. For example, in June of 2019, AWS participated in a technical exchange meeting with representatives from DISA, the DoD's Chief Information Officer's ("CIO") Office (the office responsible for all aspects of the JEDI program), and the U.S. Navy [redacted]. This meeting included a tabletop exercise designed by DISA [redacted]. Further, the SSAC's conclusion that [redacted] unreasonably ignores that AWS's Nitro architecture also reduces the risks associated with each of these issues, as well as insider threats, data exfiltration/theft, and many other infrastructure vulnerabilities.

27. These shifts in the DoD evaluators' assessments of AWS's proposal, including the significance of AWS's security advantages, occurred as President Trump increased the intensity of his public attacks against Mr. Bezos, Amazon/AWS, and the *Washington Post*. Additionally, as discussed in more detail below, there are numerous similar examples in the ultimate award where the SSAC inexplicably disregarded critical evaluation criteria or mischaracterized AWS's offering in order to give the false appearance of technical parity between AWS and Microsoft.

28. Although DoD is afforded significant discretion in evaluating proposals, it is required to wield that discretion within the bounds of the RFP and applicable law and regulation. Indeed, even one prejudicial error in DoD's process would require reevaluation of the JEDI proposals and the issuance of a new award decision. What is most remarkable here is that—consistent with the expressed desires of its Commander in Chief—DoD ***consistently and***

[redacted]

repeatedly made prejudicial errors, at every step along the way, that systematically favored Microsoft and harmed AWS—errors that grew in magnitude at each stage, and that mirrored the increasing tactics from President Trump to thwart the award of the contract to AWS. The most plausible inference from these facts is simply this: under escalating and overt pressure from President Trump, DoD departed from the rules of procurement and complied—consciously or subconsciously—with its Commander in Chief's expressed desire to reject AWS's superior bid. Even if DoD were somehow immune from this presidential pressure—plainly, it is not—the many errors in its evaluation of AWS's proposal alone nonetheless warrant reversal of the award decision and re-evaluation of the proposals.

29. As a result, on October 17, 2019 (after President Trump directed Secretary Esper to "look ... very closely" at the JEDI procurement), DoD set aside the concrete evidence that AWS was the technically superior provider, and instead executed a "Source Selection Decision Document" ("SSDD") that declared Microsoft the awardee of the JEDI Contract.

30. A few days later, on October 22, 2019, with the public unaware that DoD had already awarded the JEDI Contract to Microsoft, Secretary Esper—having already called for his Department to conduct a careful review of the JEDI process—announced that he was recusing himself from the JEDI source selection review in another unprecedented and bizarre attempt to rewrite the factual record and unsully a process tainted by the President's intervention. DoD's stated basis for Secretary Esper's recusal—"his adult son's employment with one of the original contract applicants [i.e., IBM]"—was questionable: not only had Secretary Esper's son been employed by IBM for more than six months before the recusal, but DoD had already eliminated IBM as a contender since April 2019, when it announced that only AWS and Microsoft were the remaining candidates for the JEDI award.

31. On October 25, 2019, to the extreme surprise of the overwhelming majority of industry experts and analysts, DoD announced publicly the decision it had made a week earlier (before Secretary Esper's recusal), that it had awarded the JEDI Contract to Microsoft.

32. At every step in the process, this procurement has been highly unusual. Agencies are prohibited from reinterpreting their evaluation criteria to create false parity among the offerors, ignoring categorical differences between offerors, and making patent errors that mischaracterize one offeror's solution to the benefit of another. In this procurement, however, those highly unusual steps—which alone demand re-evaluation—occurred in a truly extraordinary context: Throughout the final year of the multi-year award process, the President of the United States and Commander in Chief of our military used his power to "screw Amazon" out of the JEDI Contract as part of his highly public personal vendetta against Mr. Bezos, Amazon, and the *Washington Post*. Rarely, if ever, has a President engaged in such a blatant and sustained effort to direct the outcome of a government procurement—let alone because of personal animus and political objectives. Our laws reject this unfair influence and bias into the government procurement process, and this Court should not sanction such behavior or its intended result in this case.

33. Irrespective of any artificial steps the Administration might have taken to sterilize the record, it was impossible to shield DoD from the bias exhibited and undue influence exerted by President Trump and others. That improper and unlawful intervention contributed directly to an arbitrary and capricious award that is contrary to procurement law and contrary to the interests of our national security. As a result, the award must be terminated, and DoD must reevaluate the proposals fairly and free of any direct or indirect improper influence.

II. JURISDICTION

34. This Court has jurisdiction over this post-award protest pursuant to 28 U.S.C. § 1491(b)(1), which provides that the Court of Federal Claims "shall have jurisdiction to render

judgment on an action by an interested party objecting to … a proposed award or the award of a contract or any alleged violation of statute or regulation in connection with a procurement or a proposed procurement. [T]he United States Court of Federal Claims … shall have jurisdiction to entertain such an action without regard to whether suit is instituted before or after the contract is awarded."

35. AWS is an interested party to pursue this protest because it was an actual offeror for the JEDI Contract and, but for DoD's erroneous and flawed evaluation process, including improper influence by President Trump and DoD officials working at his direction, AWS would have received the contract award. *See* 28 U.S.C. § 1491(b)(1).

III. PARTIES

36. Plaintiff is AWS, a subsidiary of Amazon. AWS is the leading provider of scalable cloud computing services to individuals, companies, and governments. AWS is located at 410 Terry Avenue North, Seattle, WA 98109.

37. Defendant is the United States of America, acting by and through DoD.

IV. FACTUAL ALLEGATIONS

A. DoD's Cloud Modernization Initiative

38. The Executive, and specifically DoD, is charged with making the best possible decisions to ensure the safety and security of our nation, and that the taxpayer dollars appropriated by Congress are being responsibly spent free from political influence or ulterior motives. Article I, Section 9, Clause 7 of the U.S. Constitution grants the power of the purse to Congress, which then appropriates funds for the Executive to spend through its inherent power to contract. Article II, Section 1 of the U.S. Constitution "vest[s]" the "executive Power" in the "President of the United States." Congress has defined and bounded the Executive's authority to spend appropriated

funds through a detailed set of procurement laws and regulations to ensure the fair, efficient, and transparent use of public funds. *See, e.g.*, 41 U.S.C. §§ 3101 *et seq.*; 48 C.F.R. §§ 1.000 *et seq.*

39. In an environment fraught with increasingly sophisticated technological threats from our nation's adversaries, it is critical that our military leaders and intelligence community have access to the most advanced technological capabilities to enable them to make mission critical, data-driven decisions. Over the past several years, DoD has sought to modernize its information technology infrastructure to ensure it remains the most capable, nimble, and secure defense institution in the world. As part of this modernization initiative, in September 2017, DoD announced the JEDI program, DoD's plan to upgrade and consolidate its cloud computing infrastructure across the Department, which would enable DoD to employ "emerging technologies to meet warfighter needs" and maintain "our military's technological advantage."[4]

40. "Cloud computing" refers to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is an alternative to traditional "on-premises" information technology resources, which require users to plan, procure, manage, and maintain physical computing resources (i.e., servers). DoD launched its search for a cloud solution that could meet its stringent requirements, including handling complex management of unclassified, Secret, and Top Secret information, and supporting advanced data-analytic capabilities like machine learning and artificial intelligence.[5]

---

[4] *Accelerating Enterprise Cloud Adoption*, Nextgov (Sept. 13, 2017), https://www.nextgov.com/media/gbc/docs/pdfs_edit/090518cloud2ng.pdf.

[5] *Draft DOD JEDI Cloud RFP* (Mar. 7, 2018), https://beta.sam.gov/opp/8e1323cb7a001b0eb3d35b5f8480fd35/view.

41. Over the next several months, DoD invited the public, including industry and technological leaders, to provide input on the JEDI RFP. Through this process, DoD enhanced the industry's understanding of DoD's needs and "afford[ed] industry an opportunity to offer comments or pose questions regarding any element" of the RFP.[6] After reviewing more than 1,500 questions and comments in response to multiple drafts of the RFP, DoD finalized the JEDI RFP on July 26, 2018.[7]

B. The Evaluation Criteria

42. The RFP required DoD to award the JEDI Contract to the offeror whose proposal represents the best value to the Government based on an evaluation of the following nine factors:

Factor 1: Gate Evaluation Criteria
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 6: Management and Task Order ("TO") 001
Factor 7: Small Business Participation Approach
Factor 8: Demonstration
Factor 9: Price

RFP at 93–99.[8]

43. The RFP specified DoD's evaluation would proceed in phases. *Id.* at 92. First, in Phase One, DoD was to evaluate each offeror pursuant to Factor 1, Gate Evaluation Criteria. *Id.* The purpose of the Gate Evaluation Criteria was to, among other things, ensure that the JEDI Cloud: (1) is capable of providing the full scope of services even under surge capacity during a

---

[6] *Id.*

[7] *JEDI Cloud Synopsis/Solicitation* (July 26, 2018), https://beta.sam.gov/opp/7a17a56421e2d84e53c8ee6f7209ef8f/view.

[8] Unless stated otherwise, citations to the RFP refer to the RFP conformed through Amendment 0006.

major conflict or natural disaster event; (2) experiences ongoing innovation and development and capability advancements for the full potential period of performance; (3) provides continuity of services for DoD users around the world; and (4) takes advantage of the critical functionality provided by modern cloud computing providers to generate new systems easily using a combination of Infrastructure as a Service and Platform as a Service offerings as well as offerings provided through the vendor's online marketplace. *Oracle Am., Inc. v. United States*, 144 Fed. Cl. 88, 100–01 (2019). This factor would determine if the offeror was eligible for award. RFP at 92. The RFP provided DoD would not evaluate further any offeror who received a rating of "Unacceptable" under any of the Gate Criteria subfactors. *Id.*

44. Second, for those offerors who cleared Phase One, DoD was to proceed with evaluating proposals under Factors 2–6 and 9. *Id.* at 93. Based on this evaluation, and in connection with Phase Two, DoD was to make a competitive range determination. *Id.* Offerors within the competitive range were to submit for evaluation a Small Business Subcontracting Plan and a proposal volume responsive to Factor 7, and to participate in a cloud solution demonstration under Factor 8. *Id.* Offerors within the competitive range were also to be invited to engage in discussions with DoD. *Id.* The RFP stated DoD would eliminate from the competition any offeror who received a "Marginal" or "Unacceptable" rating for Technical Capability, or a Risk rating of "High," under Factor 8. *Id.*

45. Upon the completion of discussions, DoD was to request an FPR from each offeror remaining in the competition, and then evaluate FPRs under Factors 2–7 and 9 of the RFP. *Id.*

a. When evaluating Factors 2–7, DoD was to consider, in addition to the RFP's specific evaluation criteria, the degree to which each offeror's proposed approach was consistent

with the offeror's proposed Performance Work Statement ("PWS"), which would be referenced in and incorporated into the JEDI Contract. *Id.* at 94.

b. DoD was also to ensure that offerors' proposals reflected an understanding of the Government's requirements in Sections 3 and 5 of the Statement of Objectives ("SOO"), which was also incorporated into the RFP. *Id.* In addition, the RFP stated DoD would "evaluate the degree to which any proposed desired capabilities from Section 4 of the JEDI Cloud SOO provide additional benefit to the Government as defined by the evaluation criteria under the respective Factor." *Id.*

c. The RFP specified the Agency would deem offerors' FPRs to include the already conducted Factor 8 demonstration. *Id.* at 93.

d. Furthermore, Attachment L-2 to the RFP included six Price Scenarios that DoD was to use to evaluate both technical and price factors. *Id.* at 98. When evaluating these Price Scenarios under the non-price factors, DoD was to focus on the degree to which the offeror's technical approach is feasible in light of JEDI requirements. *Id.* at 94–98.

46. The Government 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 92. Factors 2–8, when combined, were more important than Factor 9 (Price). *Id.* However, Factor 9 was to become increasingly important where offerors' proposals were essentially equal in terms of technical capability, or where an offeror's price was so significantly high as to diminish the value of the technical superiority to the Government. *Id.*

47. For Factors 2–6 and 8, DoD was to assign technical and risk adjectival ratings in accordance with the following criteria:

Technical Rating	Description
Outstanding	Proposal meets requirements and indicates an exceptional approach and understanding of the requirements. The proposal contains multiple strengths and no deficiencies.
Good	Proposal meets requirements and indicates a thorough approach and understanding of the requirements. Proposal contains at least one strength and no deficiencies.
Acceptable	Proposal meets requirements and indicates an adequate approach and understanding of the requirements. Proposal has no strengths or deficiencies.
Marginal	Proposal does not clearly meet requirements and has not demonstrated an adequate approach and understanding of the requirements.
Unacceptable	Proposal does not meet requirements and contains one or more deficiencies and is unawardable.

Risk Rating	Description
Low	Proposal may contain weakness(es) which have little potential to cause disruption of schedule, increased cost or degradation of performance. Normal contractor effort and normal Government monitoring will likely be able to overcome any difficulties.
Moderate	Proposal contains a significant weakness or combination of weaknesses which may potentially cause disruption of schedule, increased cost or degradation of performance. Special contractor emphasis and close Government monitoring will likely be able to overcome difficulties.
High	Proposal contains a significant weakness or combination of weaknesses which is likely to cause significant disruption of schedule, increased cost or degradation of performance. Is unlikely to overcome the difficulties, even with special contractor emphasis and close Government monitoring.
Unacceptable	Proposal contains a material failure or a combination of significant weaknesses that increases the risk of unsuccessful performance to an unacceptable level.

Id. at 100–01.

48. The RFP identified different criteria for adjectival ratings under Factor 7:

Adjectival Rating	Description
Outstanding	Proposal indicates an exceptional approach and understanding of the small business objectives.
Good	Proposal indicates a thorough approach and understanding of the small business objectives.
Acceptable	Proposal indicates an adequate approach and understanding of small business objectives.
Marginal	Proposal has not demonstrated an adequate approach and understanding of the small business objectives.
Unacceptable	Proposal does not meet small business objectives.

Id.

Factor 1: Gate Evaluation Criteria

49. The RFP stated DoD would evaluate proposals to determine technical acceptability under each of seven Gate Evaluation Criteria subfactors: (1) Elastic Usage; (2) High Availability and Failover; (3) Commerciality; (4) Offering Independence; (5) Automation; (6) Commercial Cloud Offering Marketplace; and (7) Data. *Id.* at 93–94.

50. DoD determined that both AWS and Microsoft were technically acceptable under these subfactors and therefore included both offerors in its competitive range.

Factor 2: Logical Isolation and Secure Data Transfer

51. Under Factor 2, the RFP required DoD to evaluate each offeror's proposed approach to logical isolation and secure data transfer. *Id.* at 94. "Logical isolation" refers to the mechanisms used to ensure that no cloud user can access the data of any other cloud user without permission. This function is primarily controlled by a "hypervisor"—i.e., a system that controls and secures multiple, disparate cloud user environments running on the same physical machine. In short, Factor 2 evaluates how well the offerors' respective hypervisors function. See RFP at 82–83. The Factor 2 evaluation had two main considerations: (1) offerors' proposed Transfer

Cross Domain Solution; and (2) offerors' proposed logical isolation architecture and implementation, to include the implementation and configuration of the hypervisor. *Id.* at 82, 94.

52. In conducting this evaluation, DoD was to assess:

a. The "quality of the Offeror's proposed approach to achieving secure data transfer using a Transfer Cross Domain Solution that is consistent with the 2018 Raise the Bar Cross Domain Solution Design and Implementation Requirements," and "the degree to which the proposed Transfer Cross Domain Solution will address [the requirements] in Section L, Factor 2(1)(a-h)," *id.* at 94;

b. The "quality of the Offeror's proposed logical isolation architecture and implementation for the classified and unclassified offerings and the degree to which the proposed solution will meet the requirements in Section L, Factor 2(2)(a-h)," *id.*;

c. The "quality of the Offeror's proposed approach to meeting the requirements for classified processing at different classification levels in accordance with section 1.3.2 in Attachment 2 [to the RFP]: Cyber Security Plan," *id.*; and

d. For Price Scenario 3, "the degree to which the technical approach and Unpriced [Basis of Estimate ('BOE')] evidence a technically feasible approach when considering the secure data transfer requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2," and "the degree to which the technical approach and Unpriced BOE for Price Scenario 3 and the Offeror's overall secure data transfer approach under this Factor are consistent across the documents," *id.*

Factor 3: Tactical Edge

53. Under Factor 3, the RFP required DoD to evaluate the tactical edge devices offerors proposed under Section L, Factor 3(1)(a-h), to determine "how well the proposed approach

balances portability against capability to enhance warfighting capacity across the range of military operations in support of national defense." *Id.* at 95. The "tactical edge" refers to operational environments with limited communications connectivity and limited storage availability—e.g., combat zones where military personnel have limited ability to connect to the cloud and must take a portable device with them. In addition, DoD was to evaluate "the degree to which the proposed tactical edge devices address the requirements in Section L, Factor 3(1)(a-g) while also accounting for the practicalities of using the proposed offerings in the tactical edge environment." *Id.* The RFP explained that DoD prefers a solution that more broadly addresses the full range of military operations, rather than a solution that only addresses a subset of military operations. *Id.* It also stated DoD would place "far greater emphasis on existing solutions that meet all of the requirements in Attachment L-1, JEDI Cloud SOO." *Id.*

54. The RFP contained further evaluation criteria depending on whether tactical edge devices fell within Category One (durable, ruggedized, and portable compute and storage) or Category Two (static, modular, rapidly deployable data centers). *Id.* at 84–85, 91, 95. Offerors were required to submit at least one tactical edge device in each category, and were encouraged to propose devices to satisfy the "full range of military operations." *Id.* at 84–85.

a. For Category One devices, DoD was to evaluate the degree to which each offeror's proposed approach addresses the requirements in Section L, Factor 3(2)(a)(i-viii). *Id.* at 95. In addition, for Factor 3(2)(ix), DoD was to evaluate how well the devices balance the power requirements and physical dimensions in delivering capability within the range of military operations to forces deployed in support of a Geographic Combatant Commander or applicable training exercises. *Id.* Further, DoD was to evaluate how well proposed devices balance

portability with capability to enhance warfighting capacity across the range of military operations in support of national defense. *Id.* at 84.

b. For Category Two devices, DoD was to evaluate the degree to which each offeror's proposed approach addresses the requirements in Section L, Factor 3(2)(b)(i). *Id.* at 95. In addition, for Factor 3(2)(b)(ii), DoD was to evaluate how well the proposed approach for Category Two devices balance power requirements and physical dimensions in delivering capability across the range of military operations. *Id.*

c. Unclassified tactical edge devices from Category One had to be in production by January 11, 2019, while unclassified modular data centers from Category Two had to be in production by the first day of the post-award kickoff event. *Id.* The RFP explained DoD would "consider additional tactical edge capabilities that will be in production by January 19, 2020, but with lesser weight than existing solutions that meet the requirements in Attachment L-1, JEDI Cloud SOO." *Id.*

55. Finally, the RFP stated DoD would evaluate Price Scenarios 2, 3, and 5 under Factor 3 as follows:

> [T]he Government will evaluate the degree to which the technical approach and Unpriced BOEs evidence a technically feasible approach when considering the requirements for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenarios 2, 3, and 5, respectively, and the Offeror's overall tactical edge approach are consistent across the documents.

Id.

Factor 4: Information Security and Access Controls

56. Under Factor 4, DoD was to evaluate the quality of an offeror's proposed approach to information security and access controls. *Id.* at 95–96.

57. With regard to the proposed information security approach, the RFP required DoD to evaluate the degree to which the proposed solution met the requirements in Section L, Factor 4(1)(a-h), based on the following criteria:

a. The frequency, accuracy, efficacy, and degree of automation of patching and vulnerability management of hardware, software, and other system components, and the degree to which patching enforcement can be controlled based on vulnerability criticality, *id.* at 95;

b. The quality of supply chain risk management for hardware, software, and other system components, *id.*;

c. The degree to which the physical location and logical isolation of hosted services is discoverable and auditable, *id.*;

d. The degree to which breach identification is automated, and the efficacy of processes for mitigation, isolation, and reporting, *id.*;

e. The degree to which tools and automation can prevent and remediate data spills, including the efficacy of the process for locating and erasing all related data and purging all related media, *id.*;

f. The degree to which the offeror is able to erase data in any environment, *id.*;

g. The degree to which data generated by all intrusion detection technology, network traffic analysis tools, or any other threat detection performed is captured; the efficacy of analysis on the data generated; the degree to which users can control the manner in which notifications are communicated, and the breadth of configuration options for alerts generated by

threat detection systems; and whether the offeror provides the ability to deliver raw logs to the Government for analysis, *id.* at 96; and

h. The efficacy and quality of the process for onboarding new services into the offeror's marketplace in a rapid and secure manner, and the degree to which the offeror is able to add offerings rapidly and securely to the marketplace in the examples provided, *id.*

58. With regard to the proposed access control approach, DoD was to evaluate the degree to which the proposed solution met the requirements in Section L, Factor 4(2)(a-e), based on the following criteria:

a. The range of functionality for creating, applying, and managing technical policies for one workspace and across all JEDI Cloud workspaces, *id.*;

b. The degree of granularity of the permissions available, and the ease of discovery and assignment to roles, *id.*;

c. The efficacy of the capability to tag data objects and resources for billing tracking, access control, and assignment of technical policy, *id.*;

d. The range of capability, ease of implementation, and use of modern standards for federated, token-based, time-limited authentication and role assumptions, *id.*; and

e. The degree to which the offeror has implemented modern standards for any Application Programming Interfaces ("API") and Command Line Interference ("CLI") access and the degree to which these APIs or CLIs, if any, match or exceed the abilities of the offeror's web interfaces for user, account, workspace, identity, and access management, *id.*

Factor 5: Application and Data Hosting and Portability

59. Under Factor 5, DoD was to evaluate each offeror's proposed approach to application and data hosting, as well as its proposed approach to application and data portability. *Id.*

60. The application and data hosting assessment was to focus on "the quality of the Offeror's proposed solution and the degree to which it met the requirements in Section L, Factor 5(1)(a-e)." *Id.*

61. The application and data portability evaluation was to focus on the requirements of Section L, Factor 5(2)(a-b) and the following criteria:

a. Time to execute, time to extraction, ease of use, efficacy of the mechanisms, and format interoperability when exporting all data and object storage and associated schemas for each workspace scenario, *id.*; and

b. Time to execute, time to extraction, ease of use, format interoperability of data when exporting system configurations, including, but not limited to, networking, routing, load balancing, and operating system configuration for each workspace scenario, *id.*

62. The RFP also stated DoD would evaluate Price Scenarios 1, 4, and 6 under Factor 5. *Id.*

a. For Price Scenarios 1 and 6, DoD was to evaluate:

> the degree to which the technical approach and Unpriced BOE evidence a technically feasible approach when considering the application and data hosting requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenario 1 and Price Scenario 6, respectively, and the Offeror's overall application and data hosting approach are consistent across the documents.

Id.

[redacted]

b. For Price Scenario 4, DoD was to evaluate:

> the degree to which the technical approach and Unpriced BOE evidence a technically feasible approach when considering the portability requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenario 4 and the Offeror's overall application and data portability approach under this Factor are consistent across the documents.

Id. at 96–97.

Factor 6: Management and Task Order 001

63. Under Factor 6, the RFP required DoD to evaluate the extent to which each offeror's proposal evidences an effective program management approach to accomplishing the requirements detailed in RFP Section C2 and the TO 001 PWS. *Id.* at 97.

64. This evaluation was to include an assessment of:

a. The likelihood that the approach will achieve effective and timely communication between the offeror and the Cloud Computing Program Office, *id.*;

b. The quality of the offeror's proposed process for timely remediation of issues and the likelihood that issues will be timely remediated, *id.*;

c. The quality of the offeror's proposed risk management process and the likelihood that the proposed process and methods will result in preemptive mitigation for risk areas like tactical edge performance and security, *id.*;

d. The likelihood that the proposed Quality Assurance Surveillance Plan will result in continuously meeting the performance metrics listed in Table 5.1 of the SOO through the life of the contract, *id.*; and

e. The extent to which the proposed property management system, plan, and commercial practices and standards are likely to result in protecting, securing, and reporting the

identified Government Furnished Property in accordance with FAR 52.245-1 and DFARS 252.211-7007, *id.*

Factor 7: Small Business Participation Approach

65. Under Factor 7, the RFP provided DoD would evaluate the extent to which each offeror's proposal complied with the requirements for small business subcontract participation. *Id.*

Factor 8: Demonstration

66. Under Factor 8, DoD was to evaluate "the extent to which the scenarios are successfully demonstrated using the proposed approach for Factors 1 through 6." *Id.* DoD was to provide 24-hour notice of the specific scenarios to be demonstrated for evaluation purposes. *Id.* at 87. DoD scheduled the first demonstration for April 23, 2019. However, because of Government-caused errors in the first demonstration—including providing defective instructions—DoD scheduled a second demonstration for May 9, 2019. DoD stated the second demonstration would "be given more weight in light of it reflecting each Offeror's ability to best showcase their offerings." *Id.* at 97.

Factor 9: Price

67. Under Factor 9, the RFP required DoD to evaluate proposed prices in accordance with FAR Subpart 12.209. *Id.*

68. DoD was to evaluate offerors' Price Volumes for accuracy and completeness, including verifying that figures are correctly calculated and that proposed prices, and any applicable discounts, premiums, or fees, are accurate across the entire Price Volume. *Id.* at 98.

69. For each of the six price scenarios, offerors were to submit a Priced and Unpriced BOE, and a price build-up for each of the price scenarios. *Id.* at 88. The RFP stated DoD was to

[redacted]

evaluate the Unpriced BOEs for each price scenario under Factors 2 through 5, as specified above, rather than under Factor 9. *Id.* at 98.

70. For TO 001, DoD was to determine if each offeror's price is fair and reasonable, complete, and accurate. *Id.*

71. The RFP provided the following Table M-1 to indicate how DoD would calculate a proposal's total evaluated price:

Price Component	Units	Unit Price	Total Price
Price Scenario 1 Total Proposed Price			As proposed
Price Scenario 2 Total Proposed			As proposed
Price Scenario 3 Total Proposed			As proposed
Price Scenario 4 Total Proposed			As proposed
Price Scenario 5 Total Proposed			As proposed
Price Scenario 6 Total Proposed			As proposed
Portability Plan, CLIN 0005	4 units (assuming 2 units are ordered per year for the Base Ordering Period for purposes of TEP only)	As proposed	4 Units X Unit Price = Total Price
Portability Plan, CLIN 1005	6 units (assuming 2 units are ordered per year for the Option 1 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Plan, CLIN 2005	6 units (assuming 2 units are ordered per year for the Option 2 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Plan, CLIN 3005	4 units (assuming 2 units are ordered per year for the Option	As proposed	4 Units X Unit Price = Total Price

[redacted]

	3 Ordering Period for purposes of TEP only)		
Portability Test, CLIN 0006	4 units (assuming 2 units are ordered per year for the Base Ordering Period for purposes of TEP only)	As proposed	4 Units X Unit Price = Total Price
Portability Test, CLIN 1006	6 units (assuming 2 units are ordered per year for the Option 1 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Test, CLIN 2006	6 units (assuming 2 units are ordered per year for the Option 2 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Test, CLIN 3006	4 units (assuming 2 units are ordered per year for the Option 3 Ordering Period for purposes of TEP only)	As proposed	4 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 0007	24 units (assuming all months are ordered for purposes of TEP only)	As proposed	24 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 1007	36 units (assuming all months are ordered for purposes of TEP only)	As proposed	36 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 2007	36 units (assuming all months are ordered for purposes of TEP only)	As proposed	36 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 3007	24 units (assuming all months are ordered for purposes of TEP only)	As proposed	24 Units X Unit Price = Total Price
TEP			**Summation of all Total Prices**

Id. at 98–99.

C. AWS's Superior Cloud Computing Services Made It Uniquely Qualified to Meet the Needs of the JEDI Program

72. AWS is a leading provider of cloud-computing services, with a proven record of success in fulfilling the most complex and demanding specifications, including hosting classified

[redacted]

government workloads. Hundreds of thousands of the world's leading companies, governments, and institutions in 190 countries use AWS to manage their computing infrastructure and technology needs, so that they can instead focus their resources and efforts on their core missions.

73. AWS's superiority is readily apparent from a fair consideration of the factors identified by the Government. At a high level, the product-related factors can be grouped into three categories: technical and security capabilities (Factors 2, 4, 5), ability to deploy in war zones (Factor 3), and proven ability to make the product actually work (Factors 6, 8).

i. Technical and Security (Factors 2, 4, 5)

74. On the technical and security factors, AWS's technology is objectively superior to that of its competitors, including Microsoft. AWS extended its technological superiority in 2017, when it released its Nitro architecture. Nitro, the culmination of years of research and development, represents a fundamental improvement in the design of "hypervisors"—systems that control and secure multiple, disparate cloud user environments running on the same physical machine—and other core technologies that allow AWS to create, manage, and secure scalable virtual machines within cloud environments. Nitro's technological advantages underlie AWS's JEDI offering, providing DoD a faster, more efficient, and, most importantly, more secure computing environment.

75. No competitor—including Microsoft—has core technology that matches Nitro, as evident by the fact that all other cloud solutions available to DoD use traditional software-based hypervisors that are general-purpose in nature and contain multiple design tradeoffs to benefit general use over security. This is further illustrated in the National Institute of Standards and Technology National Vulnerability Database, which has documented numerous Common Vulnerabilities and Exposures entries for Microsoft's Hyper-V hypervisor over the last three

[redacted]

years.[9] Thus, no competitor—including Microsoft—can match AWS's security, speed, and efficiency metrics.

76. ***Security:*** AWS developed its Nitro architecture from the ground up to substantially mitigate multiple classes of security vulnerabilities that exist in software-based hypervisors, such as Microsoft's Hyper-V.

a. Unlike Microsoft's general-purpose, software-based Hyper-V hypervisor, Nitro is hardware-based and dedicated to strictly performing defined operations necessary for providing secure cloud computing resources. Nitro's design significantly reduces the number of "attack surfaces," i.e., exploitable components, when compared to general-purpose, software-based approaches. For example, Microsoft's Hyper-V is controlled by a software hypervisor and a Windows Server Operating System. The numerous features and capabilities of the Windows Server Operation System create attack surfaces that simply do not exist in Nitro—any of which could potentially be exploited, impacting the security of all Microsoft customer environments controlled by the hypervisor.

b. Additionally, while Microsoft's Hyper-V and other general-purpose, software-based hypervisors have terminals and/or user-interfaces that allow administrator access with the highest possible permissions, Nitro eliminates the possibility of AWS access to customer cloud environments by removing an administrator's ability to interact directly with those environments, thereby significantly reducing the risk related to insider threats. *See, e.g.*, AWS FPR, Volume III, Tab D at 9. This attack vector—which is eliminated by Nitro—is particularly

---

[9] *National Vulnerability Database*, Nat'l Inst. Of Stds. & Tech., https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=hyper-v&search_type=all.

[redacted]

dangerous to our national security, and it was the source of multiple prominent security breaches, including the Manning and Snowden data breaches.

c. Unlike Microsoft's Hyper-V, which uses APIs to perform numerous functions beyond those strictly necessary to operate cloud infrastructure, AWS's Nitro architecture uses a very limited set of APIs designed exclusively to provide secure isolation. Limiting APIs in this manner provides two additional, substantial security benefits that general-purpose, software-based hypervisors lack. First, Nitro can only execute functions that are necessary to run the infrastructure; this significantly reduces the number of possible attack surfaces. Second, by limiting the number of APIs, Nitro is able to effectively audit, log, and immutably store every single interaction. This means that Nitro has a complete and verifiable "audit trail" of all actions that occur within AWS's environment, allowing AWS to effectively and actively monitor for, and react to, abnormal behaviors. This level of security cannot be matched by general-purpose, software-based hypervisors, such as Microsoft's Hyper-V.

77. Nitro's ability to prevent "hypervisor breakout attacks" also sets it apart from general-purpose, software-based hypervisors, such as Microsoft's Hyper-V. Hypervisor breakout attacks are the most catastrophic attacks possible against a cloud platform. If successful, a perpetrator could gain complete access to the information, data, and applications contained in all user environments controlled by the hypervisor, with no or very limited ability for the compromised user to know a breach even occurred.[10] A successful hypervisor breakout attack

---

[10] Of note, in 2017, Microsoft reported two remote code execution vulnerabilities when its Hyper-V solution failed to "properly validate inputs from an authenticated user on a guest operating system." *See* CVE-2017-007 / Hyper-V Remote Code Execution Vulnerability, Microsoft (Mar. 14, 2017), https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0075; CVE-2017-0109 / Hyper-V Remote Code Execution Vulnerability (Mar. 14, 2017), https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0109.

would be devastating to customers, like DoD, who need absolute security on their cloud platform. AWS's Nitro architecture is the first and only cloud architecture available to DoD that is capable of effectively preventing such attacks due to its reliance on hardware, rather than software. When shown AWS's Nitro technology, the SSEB described it as "extraordinary." SSEB Report at 4.

78. ***Stability and Scalability with No Downtime:*** AWS's unique Nitro architecture improved how infrastructure components are updated and maintained in cloud data centers.

a. All technology systems require software patching and updates to address security vulnerabilities, release new features, and modernize capabilities. Patches and updates frequently require system reboots for the changes to take effect. Individuals experience this process regularly when updating the operating system on their phone or installing software updates on their personal computer.

b. Because Microsoft's cloud infrastructure is based on general-purpose software, when Microsoft installs updates or patches, it must reboot its impacted infrastructure before the updates can take effect. During a reboot, just like operations on a smart phone or personal computer, any customer workloads that are running on that infrastructure will be interrupted or terminated. Because installing patches and updates can disrupt customer workloads for several minutes while the reboot occurs, it can be very difficult for cloud service providers to

---

As Microsoft noted, this vulnerability could allow an attacker to "run a special crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code," including on the host operating system. *Id.* As Microsoft's virtualization market share increases, so too will the likelihood of additional hacks and vulnerabilities. *See* Dan Levtov, Hypervisor Market Share – ControlUp Perspective, ControlUp (Nov. 29, 2018), https://www.controlup.com/hypervisor-market-share-controlup-perspective/.

update the entirety of their infrastructure quickly. This leaves the unpatched portions of the infrastructure vulnerable to security breaches.

c. Nitro significantly mitigates these issues. The Nitro software can be updated in milliseconds without disruption to customer workloads. The process is complete before the user is even aware the update began. In a war zone, the difference between the process to update Nitro and the process to update Microsoft's Hyper-V could have life and death impacts. Additionally, AWS can perform updates to Nitro across its entire infrastructure in rapid succession—and much faster than required by the RFP—allowing AWS to roll out critical patches in near real time, effectively eliminating the vulnerabilities and security risks created by unpatched infrastructure.

ii. Ability to Deploy in War Zones (Factor 3)

79. Here again, AWS's technology is superior. Prior to JEDI, AWS already offered two devices—the "Snowball" and "Snowball Edge"—which weigh under 50 pounds each and can be taken into rugged environments and war zones. Indeed, these devices currently are in use at the tactical edge by government customers, including DoD. For example, DoD organizations—[redacted]—have Snowball Edge devices in the field today [redacted] hosting cloud-native applications and providing compute, storage, and analytics capabilities.

80. [redacted]

[redacted]

[redacted], [redacted].

iii. Ability to Deliver a Workable, Real-World Solution (Factors 6 and 8)

81. The best metric for knowing whether a company can provide a real-world solution is to see if the company already has done so successfully under similar conditions while meeting similar requirements. AWS has. For well over a decade, the Government has entrusted AWS with its most sensitive and mission-critical cloud computing needs. Since 2013, AWS has partnered with [redacted] to provide cloud services—an initiative that [redacted] called "the best decision we've ever made." According to [redacted], AWS's cloud solution "is pretty close" to "invincible."[11] AWS is uniquely qualified when it comes to working with government agencies to ensure a seamless, secure, and reliable cloud that can support their operational and security needs.

82. AWS further demonstrated its ability to execute at its second demonstration.[12] There, AWS flawlessly executed a variety of tasks assigned by DoD, including [redacted]

83. It was no surprise then that industry analysts and experts widely regarded AWS as the best choice for the JEDI Contract, referring to AWS as the "runaway favorite,"[13] "in a league

---

[11] [redacted]: *Private Cloud "The Best Decision We've Ever Made*," FCW (June 14, 2017), [redacted]

[12] AWS performed a second demonstration to address errors by the Government during the first demonstration.

[13] Rosalie Chan, *As Bidding Closes, Amazon's Cloud is the Favorite to Win a $10 Billion Defense Deal. Here's Why Everybody Else is So Mad About it*, Business Insider (Oct. 12, 2018), https://www.businessinsider.com/heres-why-amazon-is-heavily-favored-to-win-the-10-billion-jedi-contract-2018-10.

[redacted]

of its own,"[14] and the "lone frontrunner."[15] DoD's evaluation, however, was riddled with errors and, as a result, culminated in an award to Microsoft, despite Microsoft's inferior cloud offering. The most plausible explanation for these otherwise inexplicable errors lies with President Trump's persistent efforts to influence the JEDI procurement and ensure that AWS did not win.

D. President Trump's Interference with the JEDI Procurement Process

84. President Trump's animosity toward Mr. Bezos, Amazon, and the *Washington Post* is well known, and it originates at least in part from his dissatisfaction with the *Washington Post*'s coverage of him from before he assumed office. Since at least 2015, President Trump has lashed out against that coverage, and over time he has extended his attacks to Mr. Bezos, Amazon, and the *Washington Post*, often conflating the three as one. He has called the *Washington Post* a "lobbyist weapon"[16] and "tax shelter"[17] for Mr. Bezos and Amazon. He has attacked Mr. Bezos for "own[ing] [the *Washington Post*] for purposes of keeping taxes down at his no profit company, [A]mazon,"[18] and called the *Washington Post* a "scam" to "sav[e]" Amazon from "crumbl[ing] like a paper bag."[19] During a February 2016 campaign speech, then-candidate Trump threatened,

---

[14] Eric Jhonsa, *Amazon's Cloud Is Still in a League of Its Own (Sorry, Microsoft and Google)*, TheStreet (Apr. 9, 2018), https://www.thestreet.com/investing/stocks/amazon-cloud-is-in-a-league-of-its-own-14548667.

[15] Frank Konkel, *Is Amazon The Lone Frontrunner For A $10 Billion Pentagon Cloud Contract*, Nextgov (Mar. 28, 2018), https://www.nextgov.com/emerging-tech/2018/03/amazon-lone-frontrunner-10-billion-pentagon-cloud-contract/147035/.

[16] Donald J. Trump (@realDonaldTrump), Twitter (July 24, 2017, 7:36 PM), https://twitter.com/realDonaldTrump/status/889675644396867584.

[17] Donald J. Trump (@realDonaldTrump), Twitter (Dec. 7, 2015, 7:18 AM), https://twitter.com/realdonaldtrump/status/673884271954776064.

[18] Donald J. Trump (@realDonaldTrump), Twitter (Dec. 7, 2015, 7:08 AM), https://twitter.com/realdonaldtrump/status/673881733415178240.

[19] Donald J. Trump (@realDonaldTrump), Twitter (Dec. 7, 2015, 7:22 AM), https://twitter.com/realDonaldTrump/status/673885376742825984.

"If I become President, oh [does Amazon] have problems. They're going to have such problems."[20] And in an interview with Sean Hannity on May 13, 2016, then-candidate Trump asserted that Mr. Bezos bought the *Washington Post* "as a tool for political power against me and against other people" and to "try and stop antitrust" (i.e., to try to stop the administration from breaking up his "monopoly").[21] The attacks escalated in frequency and intensity once President Trump ascended to the White House.

85. Since assuming office, President Trump has used his office to step up his attacks against Amazon, the *Washington Post*, and Mr. Bezos. As evidence that the three are one and the same in his mind, President Trump has frequently referred to the "Amazon Washington Post" as a single entity, and he has frequently hurled invective against Amazon whenever the *Washington Post* publishes articles that he believes slight him or his Administration.[22] President Trump has also repeatedly claimed the *Washington Post* is selling "fake news,"[23] and he has called it an "[e]nemy of the [p]eople[.]"[24]

---

[20] CNBC Now (@CNBCnow), Twitter (Feb. 26, 2019), https://twitter.com/CNBCnow/status/703296870521528320.

[21] Jonathan Chait, *Trump Is 'Obsessed' With Amazon Because He Wants to Crush the Washington Post*, N.Y. Magazine, (Mar. 28, 2018), http://nymag.com/intelligencer/2018/03/trump-obsessed-with-amazon-wants-to-crush-washington-post.html; Donald J. Trump (@realDonaldTrump), Twitter (July 24, 2017, 7:36 PM), https://twitter.com/realDonaldTrump/status/889675644396867584.

[22] Donald J. Trump (@realDonaldTrump), Twitter (June 28, 2017, 6:06 AM), https://twitter.com/realdonaldtrump/status/880049704620494848; Donald J. Trump (@realDonaldTrump), Twitter (July 23, 2017, 4:57 PM), https://twitter.com/realDonaldTrump/status/889273320574783489; Donald J. Trump (@realDonaldTrump), Twitter (July 24, 2017, 7:23 PM), https://twitter.com/realDonaldTrump/status/889672374458646528.

[23] Donald J. Trump (@realDonaldTrump), Twitter (June 28, 2017, 6:06 AM), https://twitter.com/realDonaldTrump/status/880049704620494848.

[24] Donald J. Trump (@realDonaldTrump), Twitter (Mar. 4, 2019, 6:04 PM), https://twitter.com/realdonaldtrump/status/1102751706444636160; Donald J. Trump (@realDonaldTrump),

86. The President has also falsely blamed Amazon for the economic woes of others. For example, in August 2017, he tweeted: "Amazon is doing great damage to tax paying retailers. Towns, cities and states throughout the U.S. are being hurt—many jobs being lost!"[25] He has claimed Amazon is taking advantage of the U.S. taxpayer by not paying higher rates to the U.S. Postal Service,[26] and accused Amazon of not running a "level playing field" with other retailers.[27] He summed up his "concerns" thusly: "Unlike others, they pay little or no taxes to state & local governments, use our Postal System as their Delivery Boy (causing tremendous loss to the U.S.), and are putting many thousands of retailers out of business[.]"[28]

87. When DoD announced the JEDI Contract RFP in late 2017 and early 2018, President Trump ratchetted up his rhetoric against Amazon, attacks publicly reported to have been further fueled by encouragement from Amazon's critics and competitors. For example, just weeks after the JEDI Contract proposal was announced, the *New York Post*—known to be one of

---

Twitter (Mar. 4, 2019, 6:10 PM), https://twitter.com/realdonaldtrump/status/1102753238451929088.

[25] Donald J. Trump (@realDonaldTrump), Twitter (Aug. 16, 2017, 3:12 AM), https://twitter.com/realDonaldTrump/status/897763049226084352.

[26] Donald J. Trump (@realDonaldTrump), Twitter (Apr. 3, 2018, 6:55 AM), https://twitter.com/realdonaldtrump/status/981168344924536832; Donald J. Trump (@realDonaldTrump), Twitter (Dec. 29, 2017, 5:04 AM), https://twitter.com/realDonaldTrump/status/946728546633953285.

[27] Donald J. Trump (@realDonaldTrump), Twitter (Apr. 2, 2018, 6:35 AM), https://twitter.com/i/web/status/980800783313702918; Edward Helmore, *What is the Donald Trump v Jeff Bezos Feud Really About?*, The Guardian (Apr. 7, 2018), https://www.theguardian.com/us-news/2018/apr/07/trump-bezos-feud-amazon-washington-post-taxes-usps; Marc Fisher, *Why Trump Went After Bezos: Two Billionaires Across a Cultural Divide*, Wash. Post (Apr. 5, 2018), https://www.washingtonpost.com/politics/why-trump-went-after-bezos-two-billionaires-across-a-cultural-divide/2018/04/05/22bb94c2-3763-11e8-acd5-35eac230e514_story.html.

[28] Donald J. Trump (@realDonaldTrump), Twitter (Mar. 29, 2018, 4:57 AM), https://twitter.com/realdonaldtrump/status/979326715272065024.

President Trump's favorite newspapers—published a photo of Mr. Bezos with the headline: "President Trump: Your Defense Department is set to award a no-bid, ten-year contract for all its IT infrastructure to Administration-enemy Jeff Bezos' Amazon." The page further stated: "Thank you for the $100 billion handout. The cash will really help my many efforts to oppose your Administration's policies," and it was (fictitiously) signed: "Your pal, Jeff, Owner, Amazon & The Washington Post [*sic*]."[29]

88. Oracle co-CEO Safra Catz—who served on President Trump's transition team and has met with him repeatedly—held a private dinner with President Trump on April 2, 2018, during which she advocated against AWS in the JEDI procurement process.[30]

89. In the days after he had dinner with Ms. Catz, President Trump began to complain in tweets about Amazon's "costing the United States Post Office massive amounts of money for being their Delivery Boy" (Apr. 3, 2018)[31] and called the *Washington Post* "Amazon's 'chief lobbyist'" (Apr. 5, 2018).[32]

90. Around this same time, President Trump's advisors reported that he had grown "obsessed" with Mr. Bezos and was asking how he could "f*** with him."[33] So President Trump's

---

[29] Troy K. Schneider, *Tabloid Ad Tries to Focus Trump on DOD's JEDI Cloud Contract*, FCW (Mar. 28, 2018), https://fcw.com/articles/2018/03/28/amazon-jedi-trump-ad.aspx.

[30] Jennifer Jacobs, *Oracle's Safra Catz Raises Amazon Contract Fight With Trump*, Bloomberg (Apr. 5, 2018), https://www.bloomberg.com/news/articles/2018-04-04/oracle-s-catz-is-said-to-raise-amazon-contract-fight-with-trump.

[31] Donald J. Trump (@realDonaldTrump), Twitter (Apr. 3, 2018, 6:55 AM), https://twitter.com/realdonaldtrump/status/981168344924536832.

[32] Donald J. Trump (@realDonaldTrump), Twitter (Apr. 5, 2018, 6:10 AM), https://twitter.com/realdonaldtrump/status/981881669593559040.

[33] Gabriel Sherman, *"Trump Is Like, 'How Can I F—k With Him?'": Trump's War With Amazon (And The Washington Post) Is Personal*, Vanity Fair (April 2, 2018),

advisors encouraged the President to "cancel" the "pending multi-billion contract" between Amazon and the Pentagon.[34]

91. As the JEDI procurement process continued, President Trump's anti-Amazon rhetoric grew more strident, and his directives more overt and clear, both publicly and behind the scenes. In the summer of 2018, President Trump ordered then-Secretary James Mattis to "screw Amazon" out of the JEDI Contract opportunity.[35] Contrary to that order, Secretary Mattis demurred, later explaining to his team that he wanted the process to be "done by the book, both legally and ethically."[36] Less than half a year later, Secretary Mattis left his post as Secretary of Defense, with the President claiming that he had fired him,[37] another in an ongoing series of exits from the Trump Administration for individuals who have refused to unquestioningly follow all of the President's directives.

92. Competitors of AWS, including Oracle and IBM, also tried to derail the JEDI evaluation process. Oracle and IBM challenged AWS's eligibility to submit a bid for the JEDI Contract before the Government Accountability Office, alleging AWS should be barred because of an organizational conflict of interest. The GAO denied the protest, finding no evidence of an organizational conflict of interest that would disqualify AWS from pursuing the JEDI Contract.

---

https://www.vanityfair.com/news/2018/04/trump-war-with-amazon-and-the-washington-post-is-personal.

[34] *Id.*

[35] Guy M. Snodgrass, *Holding the Line: Inside Trump's Pentagon with Secretary Mattis* 309 (2019).

[36] *Id.*

[37] Maggie Haberman, *Trump Says Mattis Resignation Was 'Essentially' a Firing, Escalating His New Front Against Military Critics*, N.Y. Times (Jan. 2, 2019), https://www.nytimes.com/2019/01/02/us/politics/trump-mattis-defense-secretary-generals.html.

Oracle further submitted a pre-award bid protest to this Court, which considered—and ultimately rejected—Oracle's arguments on July 12, also concluding that alleged conflicts of interest did not impact the procurement process. *See Oracle Am., Inc. v. United States*, 143 Fed. Cl. 341 (2019).[38]

93. Less than a week after Oracle's efforts to derail the JEDI procurement failed in this Court, Senator Marco Rubio—whose political campaign received support from Oracle founder Larry Ellison,[39] and whose former chief of staff was an Oracle lobbyist[40]—implored President Trump to "delay awarding [the] cloud computing contract to @amazon."[41] Similarly, Representative Steve Womack urged President Trump to devote his "personal attention" to

---

[38] In addition, Oracle's lobbying efforts included a one-page flow chart, titled "A Conspiracy to Create a Ten Year DoD Cloud Monopoly," which was reportedly shown to President Trump. The chart propagated a conspiracy narrative that Amazon was politically connected with several high-level former Pentagon officials, and it created a false impression of "corruption and conflicted interests" through the use of images of dollar signs, arrows, and a heart. This false narrative has been debunked, both by this Court and DoD—yet its circulation to President Trump is troubling and further evidence of his bias against AWS. *See* Michael Warren et al., *Exclusive: Inside the Effort to Turn Trump Against Amazon's Bid for a $10 Billion Contract*, CNN (July 27, 2019), https://www.cnn.com/2019/07/26/politics/oracle-trump-amazon-defense-contract-conspiracy/index.html; Tom McKay, *Oracle Document Claiming an Amazon 'Conspiracy' to Win Military Contract Makes It to Trump's Desk*, Gizmodo (July 27, 2019), https://gizmodo.com/oracle-document-claiming-an-amazon-conspiracy-to-win-mi-1836760675.

[39] Tarini Parti, *Oracle's Larry Ellison to Host Fundraiser for Rubio*, Politico (May 13, 2015), https://www.politico.com/story/2015/05/larry-ellison-marco-rubio-fundraiser-117895.

[40] Lee Fang, *Exclusive: Senator Marco Rubio's Chief of Staff Maintains Financial Ties To Lobbying Firm*, Republic Report (June 4, 2012), https://www.republicreport.org/2012/marco-rubio-lobbyist/.

[41] Marco Rubio (@marcorubio), Twitter (July 19, 2019, 4:16 AM), https://twitter.com/marcorubio/status/1152175409863319552.

intervene in the JEDI procurement process, and Senator Ron Johnson asked then-Acting Secretary of Defense Mark Esper to delay the JEDI award.[42]

94. President Trump subsequently escalated his intervention, jettisoning any appearance of impartiality by making clear to DoD (and to the world) that he did not want AWS to get the JEDI Contract.

95. During a July 18, 2019, press conference, President Trump said he was looking "very seriously" into the JEDI procurement process (which he mistakenly referred to as "The Amazon" process) and that he would "be asking [DoD] to look at it very closely" because of "tremendous complaints about the contract with the Pentagon and with Amazon."[43]

96. Following this statement, the President's son, Donald Trump, Jr., began to refer to Mr. Bezos as "No Bid Bezos" (apparently insinuating that the JEDI Contract would be a sole-source award to AWS) on Twitter (echoing the ad published in the *New York Post* in March 2018), and proclaimed that "the shady and potentially corrupt practices from @amazon and No Bid Bezos may come back to bite them."[44] This tweet also reflects the Administration's attempts at misinformation: the suggestion that this was a "no bid" sole source award is of course false.

---

[42] Ben Brody & Naomi Mix, *Lawmakers Press Trump, Pentagon Over $10 Billion JEDI Cloud Deal*, Bloomberg (July 8, 2019), https://www.bloomberg.com/news/articles/2019-07-08/lawmakers-press-trump-pentagon-over-10-billion-jedi-cloud-deal.

[43] Scott Shane & Karen Weise, *Trump Says He May Intervene in Huge Pentagon Contract Sought by Amazon*, N.Y. Times (July 18, 2019), https://www.nytimes.com/2019/07/18/us/politics/trump-amazon-defense-department-contract.html; Aaron Gregg & Jay Green, *Trump Says Pentagon's $10 Billion Cloud Contract Should Be Investigated. Again.*, Wash. Post (July 18, 2019), https://www.washingtonpost.com/business/2019/07/18/trump-says-pentagons-billion-cloud-contract-should-be-investigated-again/.

[44] Donald Trump Jr. (@DonaldJTrumpJr), Twitter (July 18, 2019, 10:24 AM), https://twitter.com/DonaldJTrumpJr/status/1151905489472630785.

97. On July 22, 2019, President Trump tweeted a video from a Fox News segment calling the JEDI Contract the "Bezos Bailout,"[45] and unleashed yet another series of attacks on the "Amazon Washington Post."[46]

98. These escalations occurred as DoD was completing its final evaluations of AWS's and Microsoft's proposals, and shortly before DoD reached an award decision.

E. Competitive Range Determination, Discussions, Evaluations

99. AWS's initial proposal had a total evaluated price [redacted]. SSDD at 5. To achieve this value for DoD, AWS proposed, among other things, to leverage its existing classified cloud infrastructure, [redacted] and DoD, enabling AWS to provide substantial cost savings for DoD while also delivering proven and tested infrastructure capable of handling the nation's most sensitive information. AWS Initial Proposal, Volume III, Tab A at 5. AWS's proposal also highlighted its unique Nitro architecture—a purpose-built, hardware-based virtualization tool that provides superior security and performance. AWS Initial Proposal, Volume III, Tab B at 7–9. Thus, AWS proposed the best technology available at the lowest price possible.

100. DoD's evaluation of AWS's initial proposal, reflected in evaluation reports that DoD provided to AWS on April 10, 2019, did not indicate any concern about AWS's use of existing classified infrastructure to perform the JEDI Contract. *See generally* TEB Initial

---

[45] Donald J. Trump (@realDonaldTrump), Twitter (July 22, 2019, 4:20 PM), https://twitter.com/realdonaldtrump/status/1153444627573280768.

[46] Donald J. Trump (@realDonaldTrump), Twitter (July 22, 2019, 5:31 AM), https://twitter.com/realdonaldtrump/status/1153281479184658433; Donald J. Trump (@realDonaldTrump), Twitter (July 22, 2019, 5:31 AM), https://twitter.com/realDonaldTrump/status/1153281480073908224.

[redacted]

Evaluation. It also recognized the substantial benefits of AWS's Nitro architecture. *See, e.g.*, TEB Factor 2 Initial Evaluation at 9.

101. After evaluating initial proposals received in response to the JEDI RFP, on April 10, 2019, DoD narrowed the competitive range for the JEDI Contract to AWS and Microsoft. That same day, the Agency opened discussions with both offerors.

102. During discussions in May 2019, however, DoD required AWS to revise its technical and pricing approaches to keep pace with late-breaking changes to DoD's requirements. For example, without technical justification, DoD amended the RFP to require the storage of data in the Price Scenarios in a highly accessible form despite the fact AWS had already proposed a compliant solution using services that provided [redacted] to meet customer needs in a realistic, effective, and efficient manner. RFP Amend. 0005. This change created an artificial limitation on AWS's proposed technical solution, [redacted], i.e., a [redacted] increase from AWS's initial total evaluated price. Similarly, even though DoD's technical evaluators confirmed that AWS's proposed solution was "realistic and feasible," TEB Factor 2 Initial Evaluation at 32, DoD amended the RFP [redacted] in the Price Scenarios, RFP Amend. 0005. This change resulted in an increase of [redacted] in AWS's total evaluated price. Finally, at the eleventh hour—months after DoD completed its evaluation of AWS's initial proposal, and after the conclusion of all scheduled discussions—DoD changed its interpretation of the RFP's classified infrastructure requirements, requiring AWS to build dedicated classified infrastructure for DoD, thereby preventing AWS from leveraging its existing classified infrastructure (which is currently in use in support of both [redacted]

[redacted]

[redacted] and DoD) and increasing AWS's total evaluated price [redacted]. RFP Amend. 0005.

103. On May 13, 2019, the Government requested Interim Proposal Revisions ("IPR"). AWS submitted its first IPR on June 12, 2019. On July 3, 2019, DoD informed AWS that it intended to hold discussions related to AWS's IPR on a rolling basis. Through this process, AWS submitted its second (and final) IPR incrementally, submitting various updates to its proposal on July 15, 2019, July 25, 2019, July 30, 2019, and August 9, 2019.

104. DoD evaluated AWS's final IPR under the non-price factors (in order of importance) as follows:

[redacted]

See FPR Re-Affirmations (indicating the entire technical evaluation remains unchanged and hereby is reaffirmed).

[redacted]

105. AWS's total evaluated price for its final IPR [redacted], approximately [redacted].

106. Based on the offerors' IPRs, DoD engaged in further discussions with the offerors and, on August 28, 2019, requested FPRs from AWS and Microsoft.

107. DoD's FPR evaluation was as follows:

Offeror Name	**Factor 2: Adjectival Rating**	**Factor 2: Risk Rating**
AWS	[redacted]	
Microsoft	Good	Moderate
	Factor 3: Adjectival Rating	**Factor 3: Risk Rating**
AWS	[redacted]	
Microsoft	Good	Low
	Factor 4: Adjectival Rating	**Factor 4: Risk Rating**
AWS	[redacted]	
Microsoft	Outstanding	Low
	Factor 5: Adjectival Rating	**Factor 5: Risk Rating**
AWS	[redacted]	
Microsoft	Good	Low
	Factor 8: Adjectival Rating	**Factor 8: Risk Rating**
AWS	[redacted]	
Microsoft	Good	Low
	Factor 6: Adjectival Rating	**Factor 6: Risk Rating**
AWS	[redacted]	
Microsoft	Outstanding	Low
	Factor 7: Adjectival Rating	**Factor 7: Risk Rating**
AWS	[redacted]	
Microsoft	Good	N/A

SSDD at 5–6.

[redacted]

108. Microsoft's FPR had a total evaluated price of $678,517,417.38. *Id.* at 6. AWS's FPR had [redacted]

109. DoD's technical and price assessments supporting the final FPR evaluation for each Factor described above were fundamentally flawed for the following reasons:

FACTOR 2

110. DoD made at least three critical errors to reach its erroneous determination that [redacted] under Factor 2, Logical Isolation and Secure Data Transfer. SSDD at 8. In particular, DoD committed three errors in its evaluation of AWS's and Microsoft's proposals: (1) it arbitrarily removed previously assessed strengths from its final evaluation and failed to recognize others; (2) it deviated from the RFP's stated evaluation criteria; and (3) [redacted].

DoD Arbitrarily Removed Previously Assessed Strengths and Failed to Recognize Others

111. In its February 19, 2019, evaluation of AWS's initial proposal submission for Factor 2, DoD identified several strengths and one risk reduction. Yet, in its final evaluation, DoD inexplicably omitted these strengths and risks reductions, even though AWS did not remove these strengths and risk reductions from its proposal. The strengths and risk reductions initially identified and later wrongly removed included the following:

a. The TEB found that AWS's "virtual networking functionality in the 2nd (and 3rd) generation design is a strength as it provides a stronger baseline of network isolation than the industry norms, thus reducing the likelihood of inappropriate mixing of tenant traffic and thus decreasing the risk of contract non-performance." TEB Factor 2 Initial Evaluation at 8. The TEB assigned an additional strength because AWS's Nitro architecture "implements cryptographic protections for disk storage and network traffic in hardware, thus substantially increasing the

[redacted]

barrier for an attacker and decreasing the security risk." *Id.* at 9. Neither of these strengths, however, is reflected in the TEB's final evaluation. *See generally* TEB Factor 2 IPR Report. Given AWS did not change its solution for network isolation, disk storage, or network traffic, the TEB's unexplained omission of the previously assessed strengths from the final evaluation was unreasonable. *See id.*

b. The TEB assigned AWS a strength for highlighting the way in which its [redacted] *Id.* at 26. In its FPR, AWS continued to emphasize the flexibility of its marketplace offerings, noting AWS's extensive experience working with the Government in its existing classified cloud infrastructure to curate AWS marketplace titles, share security scan results, and create private marketplace offerings. *See* AWS FPR, Volume III, Tab B at 17. The TEB therefore had no basis to omit this previously assessed strength from the final evaluation. *See generally* TEB Factor 2 IPR Report.

c. The TEB assessed AWS a strength for its CloudFormation service, which the TEB found "strengthens the proposed solution by providing the Government with the ability to rapidly deploy reusable secure network architectures in common scenarios without network security experts performing redundant work." TEB Factor 2 Initial Evaluation at 26. The TEB had no basis to omit this previously assessed strength from the final evaluation, given that CloudFormation remained a JEDI Cloud Service in AWS's FPR. *See generally* TEB Factor 2 IPR Report; *see* AWS FPR, Volume III, Tab B at 19.

d. The TEB assessed AWS a reduction in contract non-performance risk because the "Offeror indicates that the network design and implementation have been reviewed, audited, and accredited at the Secret and Top Secret levels which eases JEDI Cloud adoption and

[redacted]

decreases the risk of contract non-performance." *Id.* at 17. AWS's FPR also indicated that AWS's network design and implementation had been reviewed and accredited at the Secret and Top Secret levels. AWS FPR, Volume III, Tab B at 11. Accordingly, the TEB had no basis to omit this previously assessed risk reduction from the final evaluation. *See generally* TEB Factor 2 IPR Report.

112. AWS did not revise its proposal in any way that would justify the TEB's complete omission of the above strengths from the final evaluation. *See* FPR Factor 2 Re-Affirmation at 1 ("The IPR is nearly identical to the final proposal revision (FPR) submitted by AWS.").

113. In addition, DoD failed to assign AWS a strength for its [redacted]. The RFP required offerors to propose a cross-domain solution to achieve secure data transfer and stated DoD would evaluate "the degree to which the proposed Transfer Cross Domain Solution will address [the requirements] in Section L, Factor 2(a)(a-h)." RFP at 82, 94. AWS's [redacted] service is an ***existing***, [redacted] service that has been available to customers in AWS's Top Secret and Secret regions since June 2017 and which has advanced and proven capabilities that exceed the RFP's requirements. *See* AWS FPR, Volume III, Tab A at 56; AWS FPR, Volume III, Tab B at 40. DoD, however, ignored this aspect of AWS's proposal, despite the fact that this existing and proven solution substantially reduces performance risk. *See generally* TEB Factor 2 IPR Report.

114. Moreover, DoD failed to assign AWS strengths for using [redacted] to trigger additional processing when a file is transferred, and using [redacted] to provide machine learning interfaces for tactical edge devices. The RFP required each offeror to "provide a detailed description of the technical approach to Price Scenario 3(c) with a focus on how that information evidences the Offeror's secure data transfer approach." RFP at 83. When evaluating AWS's

[redacted]

proposal against this requirement, the TEB found that AWS's reliance on [redacted] "is an effective method of initializing further analytics at the Secret level, while [redacted] provides machine learning interface on the tactical edge device prior to replication." TEB Factor 2 IPR Report at 40–41. Yet, it inexplicably failed to assign strengths for this effective approach. *See id.*

115. DoD's failure to recognize the above aspects of AWS's proposal arbitrarily deflated AWS's evaluation rating under Factor 2.

DoD Deviated from the RFP's Evaluation Criteria

116. Factor 2 required DoD to evaluate offerors' proposed logical isolation architecture and implementation for unclassified and classified offerings, including "the implementation and configuration of the ***hypervisor***." RFP at 82 (emphasis added). In particular, the RFP required DoD to assess:

- How the virtualization system, or hypervisor, manages using a management console;
- How the management console communicates with its client hypervisors over a network connection that is operating at the highest security level supported by the virtualization systems;
- How communications between the management console and its client hypervisors are encrypted using standards-based security protocols (e.g., TLS, IPSec) using Federal Information Processing Standards ("FIPS")-certified cryptography;
- How the hypervisor and management console shall log security and change-related events to both local and remote log repositories;
- How the management console interface on the hypervisor is protected;
- How boundary protections and isolation between tenants is provided (e.g., virtual firewalls, virtual switches); and
- How physical and virtual intrusion detection and prevention systems shall be used to protect the hypervisor and tenants.

Id. at 82–83.

[redacted]

117. Section 2.7 of the SOO, which describes one of JEDI's "primary objectives," requires offerors to provide "[s]ecurity that enables enhanced cyber defenses from the root level of systems through the application layer and down to the data layer with improved capabilities including ... resiliency against persistent adversary threat." SOO at 3.

118. The security of the hypervisors thus represents the most critical component of an offeror's proposed approach for logical isolation.

119. When making its source selection decision, DoD failed to evaluate AWS's proposal in accordance with these criteria. DoD failed to recognize that AWS's Nitro architecture—an innovative hardware-based hypervisor—enables AWS to deliver security to DoD users that far exceeds the RFP's requirements, as well as Microsoft's capabilities.

a. Nitro is AWS's proprietary hypervisor that uses purpose-built hardware, firmware, and software modules to virtualize network and storage resources for DoD users. AWS FPR, Volume III, Tab B at 6.

b. Nitro is a substantial step forward in hypervisor technology. Traditional hypervisors, such as Microsoft's Hyper-V, bifurcate a computing environment into trusted and untrusted elements. Trusted elements represent the space only accessible to the cloud administrator (such as Microsoft) from which the cloud administrator provisions compute resources to users. Untrusted elements represent the space occupied by users (such as DoD) performing compute functions. A major risk in the traditional hypervisor structure is that a malicious actor in an untrusted element will "breakout" and gain access to the trusted elements—from which the malicious actor could potentially gain access to, and control over, all untrusted elements/user environments within the system.

c. AWS's Nitro architecture practically eliminates the risk of these "hypervisor breakout attacks" by hosting the trusted elements on dedicated hardware that is separate and distinct from the untrusted elements in which users operate. *See, e.g.*, *id.* at 38. This partition is a significant defense to hypervisor breakouts because it significantly mitigates the ability of a malicious actor to access trusted elements even if they breakout of an untrusted element. *Id.*

d. The TEB demonstrated its initial understanding of AWS's Nitro architecture and the advanced security capabilities it offers. It noted that the "Nitro design approach to achieving greater assurance of logical separation is to devote a significant portion of critical functionality to dedicated hardware rather than on hardware shared with tenant processing." TEB Factor 2 IPR Report at 9–10. It also noted that this "physical separation limits the attack surface exposed to tenants." *Id.* at 10. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

e. The SSEB recognized that AWS's "approach to logical isolation at the hypervisor level ... represents an ***extraordinary*** approach to the Government's requirements in this area." SSEB Report at 4 (emphasis added). Noting that "[s]eparation of tenants (customers) within the cloud infrastructure is one of the ***key security challenges*** facing cloud providers and a ***critical security requirement*** of the RFP," the SSEB found that the "AWS solution goes ***beyond the industry-standard approach*** and further logically isolates tenants within the shared physical infrastructure." *Id.* at 5 (emphases added). The SSEB further stated that AWS's solution "reduces the risk of cyber compromise and represents a ***significant security benefit*** to the Government." *Id.* (emphasis added).

f. The SSAC agreed with both the TEB's and the SSEB's findings that Nitro offers a superior approach to infrastructure security. It "recogniz[ed] the value in providing hardware-backed logical isolation of tenants, and a rigid interface for AWS administrator interaction with virtual workloads" and "agree[d] with the SSEB's assertion that AWS's hardware enforced separation of the control plane ***reduces the risk of cyber compromise.***" SSAC Report at 5–6 (emphasis added). It also found that "the AWS hardware-backed approach ***significantly decreases the likelihood of a hypervisor breakout attack.***" *Id.* at 6 (emphasis added).

g. Nevertheless, the SSAC decided the Nitro architecture [redacted] *Id.* The first statement is simply false, and both of these justifications are inconsistent with the evaluation criteria. Moreover, the justifications are

[redacted]

inconsistent with concerns previously raised by DISA, [redacted] when meeting with the members of DoD CIO's Office and AWS in June 2019.

h. In addition to substantially mitigating [redacted]—which the TEB correctly recognized as significant—Nitro mitigates or eliminates the risks associated with the very types of cyberattacks cited by the SSAC, as well as insider threats, data exfiltration/theft, and many other infrastructure vulnerabilities. *See, e.g.*, AWS FPR, Volume III, Tab D at 9. Unlike Microsoft's general-purpose, software-based Hyper-V hypervisor, Nitro eliminates all direct human access by administrators to customer cloud environments, thereby removing the risks related to "bad administrator hygiene" and insider threats. *See* TEB Factor 2 IPR Report at 11. Moreover, AWS uses advanced system audits and checks to ensure the security and integrity of the Nitro boot process and interface prior to the deployment of software. *See, e.g.*, AWS FPR, Volume III, Tab D at 6. This approach prevents the deployment of "poorly written" or "misconfigured software" to the most critical component of the cloud infrastructure. *See id.* Nitro also allows for patching in milliseconds—which far exceeds the RFP's requirement for patching within eight hours of a vulnerability notification—and without any disruption to customer workloads. AWS FPR, Volume III, Tab D at 2–4. This allows AWS to perform updates to Nitro across its entire infrastructure in rapid succession—ensuring critical patches can be deployed in near real time to effectively eliminate the vulnerabilities and security risks inherent in unpatched infrastructure. *Id.* Finally, Nitro is purpose-built to operate AWS's cloud infrastructure using only a limited set of APIs designed exclusively for that purpose. By limiting the number of APIs, Nitro is able to effectively audit, log, and immutably store every single interaction, allowing for reliable active monitoring. *See, e.g.*, AWS FPR, Volume III, Tab B at 19. The security benefits of Nitro are best described by the TEB: "[Nitro] substantially reduces the possible attack surface exposed

[redacted]

to any potential malicious actor, even one who has managed to 'break out' of a tenant VM." TEB Factor 2 IPR Report at 10.

i. [redacted] AWS's Nitro architecture substantially mitigates the risks of hypervisor breakout attacks. The TEB and SSEB recognized this threat and assigned AWS strengths on this basis. *Id.* at 1, 9–11; SSEB Report at 4–5. The SSAC, however, erroneously [redacted]. SSAC Report at 6. This reasoning ignores [redacted] are often preceded by user error within individual customer environments and are significantly more catastrophic when successful. It also ignores the fact that Factor 2 of the RFP focused on hypervisor security and attacks. RFP at 82–83. The SSAC's justification [redacted] had the effect of creating false parity between AWS's Nitro architecture and Microsoft's Hyper-V solution.

j. Based on these clear errors and omissions, the SSAC improperly downgraded AWS's "extraordinary approach to the Government's requirements in this area." SSEB Report at 4. The Source Selection Authority explicitly adopted the SSAC's reasoning, stating she "consider[ed] and adopt[ed] all of the SSAC report" (SSDD at 7) and that [redacted] for Factor 2 (*id.* at 8). The SSA's conclusion improperly ignored the significant benefits of the AWS Nitro architecture and deviated from the RFP's stated evaluation criteria. But for this inexplicable departure from the TEB's and the SSEB's evaluation

[redacted]

judgments and the RFP's evaluation criteria, [redacted].

[redacted]

120. Finally, DoD assessed AWS [redacted] based on DoD's misunderstanding of AWS's proposal, further skewing the Agency's evaluation [redacted] and rendering DoD's evaluation *per se* unreasonable.

a. [redacted]

[redacted]. [redacted]

b. [redacted]

[redacted]

[redacted]

c. [redacted]

d. [redacted],

121. [redacted].

[redacted]

FACTOR 3

122. DoD erroneously determined [redacted] under Factor 3, Tactical Edge. SSDD at 8. Specifically, DoD incorrectly determined that [redacted], engaged in disparate treatment, applied an unstated evaluation criterion [redacted], and overlooked a deserved strength.

123. Factor 3 required offerors to propose at least one tactical edge device in each of two tactical device categories, and encouraged offerors to propose additional devices to satisfy the "full range of military operations," including dismounted operations. RFP at 84–85. Category 1 devices included durable, ruggedized, and portable compute and storage devices. *Id.* at 84. Category 2 devices included static, modular, rapidly deployable data centers. *Id.* at 85.

124. When evaluating proposals, DoD arbitrarily minimized the technical gap between AWS's robust and currently deployed tactical edge offering and Microsoft's lesser solution. In reality, Microsoft's Factor 3 proposal did not meet the minimum requirements of the RFP and should have been un-awardable. *See* SSAC Report at 6.

[redacted]

125. [redacted]

a. First, as AWS explained in its proposal, the Snowball Edge device "is human portable and does not require heavy equipment to move." AWS FPR, Volume III, Tab C

[redacted]

at 5. [redacted]

b. [redacted] The TEB found the Snowball Edge devices "are able to be ***lifted by a single person, making them portable***, with limitations." TEB Factor 3 IPR Report at 3 (emphasis added). [redacted]

c. In light of AWS's unequivocal statements [redacted], it was arbitrary and capricious for DoD to conclude that AWS [redacted]. This is especially so given the SSAC explicitly recognized that [redacted] SSAC Report at 6. As previously noted, the SSA explicitly adopted the SSAC's reasoning, stating she "consider[ed] and

[redacted]

adopt[ed] all of the SSAC report." (SSDD at 7.) Therefore, the SSA's source selection decision relied upon and incorporated the errors made by the SSAC.

DoD Engaged in Disparate Treatment

126. [redacted]. TEB Factor 3 IPR Report at 3, 6, 7–8.

a. [redacted]

[47] [redacted]

[redacted]

128. At a minimum, , it should have assigned Microsoft a ***deficiency*** and determined it ineligible for award

DoD Applied an Unstated Evaluation Criterion and Overlooked a Deserved Strength

129. ,

a.

b. .

[redacted]. [redacted]

130. Separately, DoD also failed to recognize that AWS's Snowball Edge has already been accredited for Impact Level 6 and is deployed operationally ***today*** with [redacted] and DoD Combatant Commands in war zones, [redacted]. *See* AWS FPR, Volume III, Tab C at 1–3. This means the risk associated with AWS's Snowball Edge devices is virtually zero. AWS deserved significant credit for this aspect of its proposal.

131. Under a rational evaluation, DoD would have credited AWS appropriately for its [redacted], [redacted] But for these evaluation errors, AWS [redacted].

FACTOR 4

132. DoD erroneously determined [redacted] under Factor 4, Information Security and Access Controls. SSDD at 8. In particular, it deviated from the RFP's evaluation criteria by failing to credit AWS for its substantial information security and access control capabilities.

[redacted]

133. Factor 4 required DoD to evaluate offerors' approaches to information security by assessing (i) the degree to which the physical location and logical isolation of hosted services is discoverable and auditable; (ii) the degree to which breach identification is automated and the efficacy of processes for mitigation, isolation, and reporting; (iii) the frequency, accuracy, efficacy, and degree of automation of patching and vulnerability management of hardware, software, and other system components; and (iv) the degree to which patching enforcement can be controlled based on vulnerability criticality. RFP at 85, 95–96.

134. When evaluating AWS's proposal, DoD failed to recognize several key features that AWS's Nitro architecture provided to ensure the highest level of information security.

a. As discussed above, AWS proposed its purpose-built Nitro architecture to provide DoD with the most secure hypervisor available. Nitro achieves a level of isolation that is unique from all other cloud service providers. AWS FPR, Volume III, Tab D at 1. 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. The provisioning process includes a strong technical control that overwrites ***all*** firmware on host hardware, eliminating the possibility that compromised hardware could ever be used as part of the cloud services. Further, not only does Nitro prevent firmware updates by "normal" software driven means, but the host hardware is continually scanned to ensure the firmware remains unchanged. *Id.* at 6. This automated control exceeds the industry standard, which relies on humans to verify the integrity of certain (but not all) host firmware.

b. Moreover, the Nitro architecture provides substantial security benefits for supply chain integrity. Because Nitro is purpose-built to operate hosts within the AWS cloud, [redacted] that ensures the integrity of firmware accessing the cloud. When a

[redacted]

host accesses a virtual machine, Nitro holds the system [redacted]. *Id.* This process occurs at ***every*** reboot of the host system. *Id.*

c. AWS's Nitro architecture also offers enhanced patching capabilities that allow AWS to resolve vulnerabilities rapidly ***without disruption*** to DoD functions. *Id.* at 4. The SOO required the JEDI contractor to be able to apply patches and updates to underlying infrastructure and cloud services within eight hours of notification. SOO at 14. Nitro allows for patching in ***milliseconds*** and without any disruption to customer workloads. AWS FPR, Volume III, Tab D at 2–4. This allows AWS to perform updates to Nitro across its entire infrastructure in rapid succession—ensuring critical patches can be deployed in near real time to effectively eliminate the vulnerabilities and security risks inherent in unpatched infrastructure. *Id.*

d. Finally, the Nitro architecture 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. *Id.* at 9. As the U.S. Government has seen with Private Bradley (now Chelsea) Manning and Edward Snowden, malicious insiders are responsible for significant breaches and stolen data that harm national security. Nitro substantially reduces the risk of such occurrences.

135. Factor 4 also required DoD to assess each offeror's proposed approach for (i) "[h]ighly granular attribute and role-based access control configuration, and the ability to assign permissions to roles IAW technical policies"; (ii) "[o]bject and resource access control management, including data and resource tagging"; and (iii) "[t]oken-based and time-limited federated authentication allowing a user to assume a role within the cloud environment at all classification levels." RFP at 85.

[redacted]

136. As with its information security evaluation, however, DoD failed to recognize AWS's significant access control capabilities and their clear superiority to Microsoft's offerings.

a. In its proposal, AWS explained [redacted].

i. [redacted]

b. AWS's proposal also explained how AWS could leverage its data and resource tagging capabilities [redacted]

[redacted]

c. [redacted]

137. Although DoD determined [redacted] to information security and access controls, neither the TEB nor the SSEB credited AWS for the substantial benefits discussed above, [redacted]. *See generally* TEB Factor 2 IPR Report; SSEB Report. [redacted]. *See generally* SSAC Report.

138. DoD's failure in this regard is all the more significant given that Microsoft's access control capabilities are significantly less comprehensive than AWS's and, more importantly, do not satisfy the RFP's requirements. According to Microsoft's online technical documentation and reputable industry reports, Microsoft does not have the capability to tag resources and users for access control policies. Microsoft therefore lacks the capability to perform "[o]bject and resource access control management, including data and resource tagging." *See* RFP at 85.

139. Had DoD recognized the substantial information security and access control benefits that the AWS solution offered, and similarly acknowledged the significant deficiencies in Microsoft's proposed approach, it could not have [redacted]

[redacted]

[redacted]. [redacted] [redacted]

[redacted].

FACTOR 5

140. DoD erroneously determined [redacted] under Factor 5, Application and Data Hosting and Portability. SSDD at 7. In particular, DoD misevaluated AWS's proposed third-party marketplace offerings and overlooked strengths in AWS's proposal, including those the Agency explicitly recognized during its initial evaluation of AWS's proposal.

DoD Misevaluated AWS's Third-Party Marketplace Offerings

141. Factor 5 required DoD to evaluate each offeror's proposed approach to application and data hosting and application and data portability. RFP at 96. In this regard, the SOO required offerors to "[p]rovide the ability to rapidly and securely deploy CSP and third-party platform and software service offerings from an online marketplace with baseline template configurations." SOO at 10.

142. In response to this requirement, AWS's proposal included [redacted] third-party marketplace offerings available at the time of award from over [redacted]. *See* AWS FPR, Volume III, Tab E at 3. AWS's 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 including [redacted]—where AWS not only has a marketplace, but is the ***only*** cloud service provider with an authorization to operate. AWS listed each of these offerings in its JEDI price catalog related to CLINs x001 and x002. AWS FPR, Volume VI, Tab C.

[redacted]

143. Nevertheless, when considering AWS's proposal, DoD erroneously determined [redacted] SSAC Report at 7–8.

144. DoD apparently reached this incorrect conclusion based on [redacted] *Id.* DoD incorrectly interpreted [redacted] *Id.* at 8.

145. DoD's conclusion, however, ignores AWS's explicit explanation of the [redacted] which states:

[redacted]

146. In other words, AWS's proposal made clear that [redacted] And, in fact, these Marketplace offerings plainly were included in AWS's proposed price catalogs and available to DoD at award. *See* AWS FPR, Volume VI, Tab C.

[redacted]

147. DoD's contrary interpretation is especially problematic given AWS only included the information [redacted] to comply with DoD's instructions during oral discussions. During oral discussions, AWS and DoD discussed how to balance the RFP's requirements for commercial parity and security. [redacted].

148. [redacted]—this is equally true whether the underlying cloud provider is AWS or Microsoft. Thus, consistent with DoD's instructions, AWS [redacted] a requirement which would be nonsensical with regard to third-party marketplace offerings. AWS FPR, Volume VI, Tab A at 5. This is especially so given the RFP required offerors to include at least 90% of their free marketplace offerings—which are even less likely to comply with all of the RFP's security requirements—as part of their JEDI solution. SOO at 10.

149. DoD therefore did not have a rational basis for concluding AWS could not provide its proposed third-party marketplace offerings at the time of award.

[redacted]

DoD Overlooked Strengths in AWS's Proposal, Including Those Previously Recognized

150. In its strained attempts to identify differentiators that justified award to Microsoft, DoD failed to recognize ***actual*** discriminators that demonstrated AWS's technical superiority. For example:

a. AWS [redacted] Content Delivery Network Points of Presence. AWS FPR, Volume III, Tab A at 13. These Points of Presence allow AWS to bring cloud-hosted content closer to DoD users around the world, thereby allowing for quicker download and access. In addition, they enable DoD users to upload content to the cloud faster.

b. AWS proposed [redacted], AWS FPR, Volume III, Tab E at 11, ensuring service availability and reliability on a scale not even contemplated by the RFP, [redacted].

c. AWS offered the most advanced graphics processing units and high-memory compute instance types available in the commercial marketplace, including: General Purpose, Memory Optimized, Storage Optimized, Computer and Network Optimized, and Higher Performance Computer Acceleration. AWS FPR, Volume III, Tab E at 4. In particular, to support DoD's diverse mission needs, AWS proposed [redacted]

[redacted]

[redacted]

Id. These technologies are critical for next generation machine learning and artificial intelligence applications.

d. AWS proposed [redacted] It supports integration with existing on-premises workloads, cloud-native applications, and hybrid implementations to run on premises and scale in the cloud. *Id.*

e. AWS's proposed portability plan provides detailed instructions on how to move data between AWS cloud environments and other hosting environments. [redacted] The proposed migration plans were comprehensive and

[redacted]

[redacted], as required by the RFP and the DoD's Enterprise Cloud Strategy. *Id.* at 1, 13, 16. AWS's superior understanding of DoD's desire to be able to move data between on-premises hosting environments, other cloud providers, and the tactical edge dramatically lowers the risk of contract non-performance and give's DoD control of its data.

f. AWS proposed robust Relational Database Services ("RDS") that far exceed the SOO's requirement that offerors propose a "managed database and noSQL services at the scale and speed to meet mission requirements, including both object storage options and managed databases." SOO at 8. Specifically, AWS proposed [redacted] These offerings provide multi-availability zone replication and resiliency as well as cross-region replication options. *See id.* Moreover, [redacted] provides the ability to analyze data at the exabyte level, which is greater than the petabyte scale DoD required. *Id.* at 75.

g. DoD unreasonably failed to recognize the above features and assign corresponding strengths to AWS's proposal.

151. In addition, in its January 11, 2019, evaluation of AWS's initial proposal submission for Factor 5, DoD identified several strengths that DoD inexplicably excluded from the final IPR evaluation conducted in August 2019, which DoD affirmed and incorporated in its September 2019 evaluation of AWS's FPR. These strengths and risk reductions in AWS's initial proposal included the following:

[redacted]

a. The TEB assessed AWS a strength because [redacted] The TEB provided no explanation for its failure to assess a similar strength in the final evaluation. *See generally* TEB Factor 5 IPR Report.

b. The TEB assessed AWS a strength because AWS proposed [redacted] can also be used to store configurations and provision infrastructure," which allows for "flexibility based on user preference and can be used to launch and manage Offeror services." TEB Factor 5 Initial Evaluation at 6. In particular, the TEB noted [redacted] "allows for the Offerors services to rapidly be provision[ed] using [redacted]." *Id.* AWS also discussed [redacted] in its FPR, but the TEB failed to carry forward the previously assessed strength. *See* AWS FPR, Volume III, Tab E at 5–6; *see generally* TEB Factor 5 IPR Report.

c. The TEB assessed AWS a strength for its proposed use of a "mature marketplace," which "allows for the sharing of pre-built and pre-approved configurations." TEB Factor 5 Initial Evaluation at 6. The TEB found that this feature "further decreases the amount of time needed to configure databases" and "significantly increases the speed and rapid nature of database deployments." *Id.* Furthermore, the TEB noted that the marketplace offers "third party services which enables the rapid procurement and deployment of third party services that will integrate with the Offeror's services." *Id.* Even though AWS discussed its mature marketplace in

[redacted]

its FPR, the TEB inexplicably abandoned the previously assessed strength. *See* AWS FPR, Volume III, Tab E at 2–3; *see generally* TEB Factor 5 IPR Report.

d. AWS did not revise its IPR in any way that would justify DoD's omission of the above strengths in the final evaluation. FPR Factor 5 Re-Affirmation at 1 ("The IPR is nearly identical to the final proposal revision (FPR) submitted by AWS.").

152. But for the evaluation errors described above, AWS would have received [redacted]

FACTOR 6

153. DoD erroneously determined that [redacted] under Factor 6, Management and TO 001. SSDD at 7. In particular, DoD (1) unreasonably evaluated a prior, superseded version of AWS's proposal; (2) incorrectly concluded AWS [redacted]; and (3) ignored AWS's proven and tested management approach, [redacted], where AWS operates hyperscale data center clusters at both the Top Secret and Secret levels.

DoD Improperly Evaluated a Prior Version of AWS's Proposal

154. The SOO required offerors to propose unclassified services in ***three*** physical data centers within 30 days of contract award. SOO at 9.

155. AWS's FPR (as well as its IPR submission on July 15, 2019) states: [redacted]

[redacted]

[redacted] 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. *Id.* at 4. [redacted]

156. Nevertheless, the TEB erroneously found that AWS had proposed [redacted] Based on this finding, [redacted], the TEB concluded that [redacted] *Id.* In actuality, AWS's proposal exceeded the "standard" [redacted]

157. The TEB's conclusion suggests the TEB not only ignored the AWS Region structure described in AWS's proposal, but also evaluated a prior version of AWS's proposal. Specifically, earlier versions of AWS's proposal indicated it would only provide [redacted]. However, beginning with AWS's IPR submitted on July 15, 2019, through its FPR, AWS clearly proposed [redacted]

158. Under a rational evaluation, DoD would have evaluated AWS's FPR, recognized that AWS proposed to substantially exceed the SOO's requirement for three unclassified data centers, [redacted]

[redacted]

DoD Incorrectly Determined AWS [redacted]

159. DoD's evaluation also was erroneous because it incorrectly concluded [redacted], and then treated this arbitrary conclusion as [redacted] in the Factor 6 evaluation. SSAC Report at 8.

160. The SSAC Report states that AWS offered [redacted]. Both of these statements are demonstrably false.

a. [redacted], AWS's proposal states:

[redacted]

b. [redacted]

161. [redacted]

DoD Unreasonably Discounted AWS's Proven Management Approach

162. Finally, DoD inexplicably concluded [redacted],

163. 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

[redacted]

plan, and (5) property management system. *See* RFP at 97. Additionally, as part of the evaluation for Factors 2–7, DoD was to evaluate the degree to which the proposal reflects an understanding of the Government's requirements in Sections 3 and 5 of the SOO. *See id.* at 94.

164. AWS's program management approach leveraged its extensive experience as [redacted], which is the only contract remotely comparable to the size and complexity of the JEDI Contract, to demonstrate its capabilities in each of the five areas noted above. *See, e.g.*, AWS FPR, Volume III, Tab F at 1. As a result, AWS offered DoD a ***proven and tested*** approach for completing contract requirements on schedule and in accordance with the JEDI Contract's quality and performance metrics—including the ability to operate securely, scaleably, and successfully at the Secret and Top Secret levels. *See id.*

165. In stark contrast, Microsoft, which has never performed a cloud infrastructure contract similar to JEDI, necessarily proposed a program management approach that is ***theoretical and unproven***.

166. Yet, when evaluating proposals, DoD bizarrely concluded [redacted] under Factor 6. SSDD at 6, 8. This evaluation judgment was arbitrary and capricious, especially given DoD did not even acknowledge [redacted] when evaluating [redacted]. *See generally* TEB Factor 6 IPR Report; SSEB Report at 25–26; SSAC Report at 8. [redacted] has characterized the AWS cloud as the "best decision we've ever made,"[48] and has stated that it "has transformed

[48] [redacted]: *Private Cloud "The Best Decision We've Ever Made,"* FCW (June 14, 2017), [redacted].

[redacted]

our ability to build new capabilities and has transformed our ability to solve seemingly impossible intelligence problems," it is unfathomable DoD would overlook this aspect of AWS's offering.[49]

167. [redacted].

FACTOR 8

168. [redacted] SSDD at 6. Specifically, DoD overlooked objective evidence showing that AWS's cloud solution demonstration far exceeded the Agency's stated requirements.

169. Factor 8 required offerors to demonstrate their JEDI cloud solutions using their proposed approaches for Factors 1 through 6 in different demonstration scenarios. *See* RFP at 97. DoD was to evaluate "the extent to which the scenarios are successfully demonstrated using the proposed approach for Factors 1 through 6." *Id.* DoD informed the offerors of the demonstration date and the four scenarios that would be performed 24 hours in advance of the demonstration activity day. *See id.* at 87.

170. DoD initially planned only one demonstration activity. However, because of numerous Government-caused failures in the first demonstration activity on April 23, 2019, DoD notified AWS that it would hold a second demonstration activity and amended the RFP accordingly. The amended RFP required DoD to give more weight to the second demonstration

---

[49] Amanda Ziadeh, [redacted] *Finds Security, AI Opportunities in Cloud*, Government CIO Media & Research (June 20, 2018), [redacted]

[redacted]

activity "in light of it reflecting each offerors ability to best showcase their offerings." *Id.* at 97. The second demonstration activity occurred on May 9, 2019. Both demonstrations involved the following four scenarios:

a. Scenario 8.1 – Test Suite: The Government was to run a set of automated tests using offeror-provided code on both the public, commercial cloud environment, and the offeror's proposed portable tactical edge device, interacting with the existing and publicly available API. A successful implementation would programmatically create, destroy, and interact with remote resources as required by each test case. *See* First Demonstration Procedures at 2–3; *see also* Second Demonstration Procedures at 3–5.

b. Scenario 8.2 – Scaling Application: The offeror was required to demonstrate the creation and configuration of an automatically scaling pool of virtual machines through its Graphical User Interface. It was then required to deploy a simple application to the pool, with incoming traffic evenly distributed amongst the virtual machines in the pool. A successful implementation would result in a dynamically created pool of compute resources to respond to incoming requests from a client. As the client increased the number of incoming requests, the number of compute nodes was to seamlessly increase as the number of incoming requests exceed the predefined maximum requests per node. As the test client reduced usage, the shutdown of excess nodes was to be seamless. *See* First Demonstration Procedures at 3–4; *see also* Second Demonstration Procedures at 5–7.

c. Scenario 8.3 – Tactical Edge Device Testing: Offerors' proposed portable tactical edge devices were to undergo basic tests surrounding their durability and interface with the cloud environment in both connected and disconnected mode. These tests were to focus on the ability of the device to process and stream data. A successful implementation would allow the

application to save data to the offeror's tactical edge device despite network disconnect/reconnect, being physically dropped, and being exposed to environmental factors, while opportunistically syncing that data to the offeror's cloud environment. The test suites in Scenario 8.1 were to run against the proposed portable tactical edge device. *See* First Demonstration Procedures at 4; *see also* Second Demonstration Procedures at 7–10.

d. Scenario 8.4 – Security Demo: Offerors were to set and modify users, roles, and Access Control Lists, both through the standard user interface, as well as through the API. Offerors also were required to display the capability to tag files appropriately, add or modify a policy to restrict access based upon tags, and automatically add tags to new objects created. A successful implementation for this scenario would demonstrate that the security controls and user Access Control Lists work as expected and audit logs are generated in the course of any access, security, and API events during the exercise, both through the Graphical User Interface and interactively through a command line interface. *See* First Demonstration Procedures at 4–5; *see also* Second Demonstration Procedures at 10–13.

171. [redacted] DoD failed to evaluate ***the extent*** to which AWS successfully demonstrated its technical approach for Factors 1 through 6, as required by the RFP. *See* RFP at 97.

a. Under Scenario 8.1, offerors were required to demonstrate a compute value of 120 seconds. SOO at 14 (Table 5.1); TEB Factor 8 Evaluation at 5. AWS far exceeded this requirement by demonstrating [redacted]. TEB Factor 8 Evaluation at 5. Similarly, offerors were required to demonstrate an object storage value of 120 seconds. SOO at 14 (Table 5.1). AWS far exceeded this requirement

[redacted]

by reporting [redacted]. TEB Factor 8 Evaluation at 5.

b. Under Scenario 8.3, offerors were required to demonstrate successful execution of cloud services. *See* Second Demonstration Procedures at 8. During both demonstrations, AWS clearly demonstrated this capability, [redacted] Although the TEB noted this point, it failed to credit AWS's breadth and depth of services, which exceeded the minimum requirement for Scenario 8.3. Scenario 8.3 also 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. SOO at 14 (Table 5.1); TEB Factor 8 Evaluation at 15. During the second demonstration, AWS demonstrated [redacted]. *See* TEB Factor 8 Evaluation at 15. AWS also demonstrated [redacted]. *See id.* Finally, AWS demonstrated a block storage value [redacted]. *See id.*

c. Under Scenario 8.4, DoD required offerors to create Windows 10 virtual machine instances using the default configuration, with remote access available. *See* Second Demonstration Procedures at 13. AWS demonstrated the use of [redacted] to access remotely the Windows Virtual Machine created during the demonstration without "using direct access to a running remote access daemon," which the TEB acknowledged as a Strength. TEB Factor 8 Evaluation at 19. However, the TEB failed to acknowledge AWS's ability to leverage [redacted]

[redacted]

[redacted] to connect remotely with Windows virtual machines even with no network connectivity to the enclave. *See id.* In addition, Scenario 8.4 required offerors to demonstrate a capability to revoke a session that was currently in progress. *See* Second Demonstration Procedures at 12. AWS not only demonstrated this capability, but also the ability to revoke all active sessions for an identity ***immediately***, which the TEB ignored. *See* TEB Factor 8 Evaluation at 16–19.

172. [redacted].

173. [redacted]

F. At the Eleventh Hour, the Government Changed Course Under Pressure from President Trump

174. While DoD evaluators were preparing the IPR Reports for the various evaluation factors described above, President Trump, senior DoD appointees, and others continued to exert their influence on DoD's source selection process, resulting in abrupt irregularities in the final stages of the procurement process.

175. As late as the end of July 2019—despite the very public comments by the Commander in Chief and others questioning the procurement process, *see supra* ¶¶ 91–97—DoD maintained that it was planning to announce its final award decision in August 2019.[50]

---

[50] Aaron Gregg, *Pentagon issues forceful rebuke of Oracle as debate over a massive federal contract turns caustic*, Wash. Post (July 30, 2019),

[redacted]

176. However, a few days later, on August 1, 2019, DoD abruptly reversed course when newly appointed Secretary of Defense Mark Esper (who was sworn in just one week earlier to replace Secretary Mattis) announced that he had ordered a re-review of the JEDI RFP process, and that DoD's award decision would be placed on hold until he completed his examination. He explained that he was taking a "hard look" at JEDI because "I've heard from folks in the administration, so I owe, as the new guy coming in, a fresh look at it, study it, make sure I understand all the different factors."[51] This reversal came shortly after Senators Rubio and Johnson sent letters to Secretary Esper urging him to postpone the award of the JEDI Contract.[52] The next day, Secretary Esper was even more explicit about the role of the Commander in Chief, stating that he "heard from people from the White House" and that JEDI "deserves an honest, thorough look."[53]

177. Once the JEDI Contract award was under examination, Donald Trump, Jr., tweeted several times, bluntly, that AWS would not be awarded the JEDI Contract upon completion of the

---

https://www.washingtonpost.com/business/2019/07/30/pentagon-issues-forceful-rebuke-oracle-debate-over-massive-federal-contract-turns-caustic/.

[51] Aaron Gregg, *After Trump cites Amazon concerns, Pentagon reexamines $10 billion JEDI cloud contract process*, Wash. Post (Aug. 1, 2019), https://www.washingtonpost.com/business/2019/08/01/after-trump-cites-amazon-concerns-pentagon-re-examines-billion-jedi-cloud-contract-process/; *see also* Frank Konkel, *JEDI Contract on Hold for Defense Secretary Review*, Nextgov (Aug. 1, 2019) https://www.nextgov.com/it-modernization/2019/08/jedi-contract-hold-defense-secretary-review/158887/.

[52] Letter from Senator Marco Rubio to Honorable Mark Esper, Secretary of Defense (July 25, 2019), https://www.rubio.senate.gov/public/_cache/files/04fdc9b6-34d1-4725-97e5-8d5faa5e055e/E069C0B453AD2BA467894E98889B3D62.19.07.25-senator-rubio-ltr-to-secdef-re-jedi-cloud.pdf; Letter from Senator Ron Johnson to Honorable Mark Esper, Secretary of Defense (June 24, 2019), https://www.hsgac.senate.gov/imo/media/doc/2019-06-24%20RHJ%20to%20DOD%20re%20OIG%20Investigation%20-%20JEDI.pdf.

[53] *Secretary of Defense Esper Media Engagement En Route to Sydney, Australia* (Aug. 2, 2019), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1925072/secretary-of-defense-esper-media-engagement-en-route-to-sydney-australia/.

re-review process, stating that "[e]ven the democrats aren't buying the BS coming from Bezos Inc."[54] and confirming that it "[s]ounds like the corrupt #BezosBailout is in trouble."[55] Around the same time, CNN reported that President Trump wanted to "scuttle" the process.[56]

178. Secretary Esper's appointment as Secretary of Defense in the summer of 2019 marked an important turning point in DoD's analyses of the evaluation factors. For instance, TEB's initial evaluations of AWS from early 2019 readily acknowledged significant strengths in AWS's proposal, particularly for Factors 2 and 5. But in TEB's subsequent evaluation reports of AWS's IPR in August 2019—amidst President Trump's escalating attacks on Mr. Bezos, Amazon, and the *Washington Post* and following President Trump's and Secretary Esper's calls for an examination into the JEDI evaluation process—those previously identified strengths were noticeably absent, without any explanation for their omission. The substance of these evaluations was re-affirmed in September 2019. Factor 2 FPR Re-Affirmation; Factor 5 FPR Re-Affirmation. Thus, the SSEB, SSAC, and ultimately the SSA, relied on these IPR Reports in reaching their decision to award the JEDI Contract to Microsoft.

179. This abrupt change in course reflects the culmination of President Trump's improper interference and express direction to officials responsible for overseeing the award of the JEDI Contract—which began with President Trump's claimed firing of former Secretary Mattis in

---

[54] Donald Trump Jr. (@DonaldJTrumpJr) Twitter (Aug. 6, 2019, 4:58 PM), https://twitter.com/donaldjtrumpjr/status/1158890185226149893.

[55] Donald Trump Jr. (@DonaldJTrumpJr) Twitter (Aug. 13, 2019, 6:57 AM), https://twitter.com/donaldjtrumpjr/status/1161275522103595008.

[56] Michael Warren, *Exclusive: Inside the effort to turn Trump against Amazon's bid for a $10 billion contract* (July 27, 2019), https://www.cnn.com/2019/07/26/politics/oracle-trump-amazon-defense-contract-conspiracy/index.html?no-st=1564177550.

January 2019, and his replacement of DoD key leadership with individuals, like Secretary Esper, who were uniquely susceptible to pressure from the Commander in Chief.

180. Both Secretary Esper and the senior DoD political appointees overseeing the JEDI Contract procurement were specifically selected by the President and their nominations and appointments were dependent on his continued goodwill (widely reported to change frequently).

181. Dana Deasy, DoD's CIO, was in charge of all aspects of the JEDI program, including the procurement process and the Cloud Computing Program Office, starting in June 2018. Mr. Deasy served in that position for nearly a year until President Trump formally nominated Mr. Deasy for his position in June 2019.[57] Soon after, while Mr. Deasy's nomination was pending, the President began to call publicly for an investigation into the JEDI procurement process.

182. Given President Trump's public comments and his record of dismissing political appointees with whom he disagrees, Secretary Esper and Mr. Deasy undoubtedly understood that they served at the pleasure of a President who had made clear that he did not want AWS to win the JEDI Contract, and they had personal incentives to ensure that the President's command was carried out. Indeed, the President's direct control over the continued employment and potential promotion of these and other high-level decision makers—both in the military and in civilian service—would have been readily apparent to them, as would the risks of going against the President's stated wishes.

183. In addition, the very nature of DoD acquisitions and the structure and makeup of the Washington Headquarters Services Acquisition Directorate made it more likely that the

---

[57] Congress made the position of DoD CIO a Senate-confirmed post beginning in January 2019, via the 2018 National Defense Authorization Act.

President, as Commander in Chief, had an outsized influence on the SSA. The Washington Headquarters Service exists to serve the procurement needs of the Office of the Secretary of Defense, which leads the executive department most directly under the control of the President as Commander in Chief, whose desires generally become priority mission objectives for DoD. Any bias stemming from the President, whether expressed publicly or privately, would have been understood by, and would have inherently impacted, these political appointees, who, in turn, supervised the contracting officer, managed the SSAC, and imparted the President's bias to the SSAC.

184. The SSA and members of the SSAC were thus subject to the President's influence on multiple fronts. There were the public statements of the President, their Commander in Chief, detailed above. There also was the certainty that any recommendation they made would be subject to scrutiny from the highest levels and that their choice would be much more likely to meet with approval if it pleased their superiors. No matter how much the SSA and the members of the SSAC may have tried to discharge their duties impartially, or DoD attempted to shield the decision-makers from their Commander in Chief's directives, no amount of compartmentalization, segregation, or anonymization could have isolated the decision-makers from the clear and unmistakable conflict of interest that stemmed from the very highest levels of power in DoD and that were made known to all. As recent events demonstrate, the President is perfectly willing to go after those with whom he disagrees, even within his own Administration. That dynamic cannot have been lost on the JEDI award decision-makers.

G. Contract Award and Debriefing

185. The SSEB issued its Executive Summary Report on September 27, 2019, the Price Evaluation Board issued its final Report on September 29, 2019, and the SSAC made its source selection recommendation to the SSA on October 3, 2019.

186. On October 17, the SSA signed the SSDD, "determin[ing] that Microsoft's proposal represents the best value to the Government" and selecting "Microsoft Corporation[] for award of the Joint Enterprise Defense Infrastructure Cloud contact." SSDD at 9. DoD had privately made its award decision, but the public would wait over a week to learn of the Government's miscarriage of the procurement process.

187. Before DoD's flawed award decision was publicized, on October 22, 2019, Secretary Esper announced unexpectedly that he was recusing himself due to a personal conflict of interest arising out of his son's employment with IBM.[58] By this time, however, Secretary Esper's son had been employed with IBM for more than six months[59]—and in fact DoD had already eliminated IBM's proposal for the JEDI Contract since as early as April 2019, when DoD announced that AWS and Microsoft were the only remaining candidates for the award.[60]

188. On October 25, 2019, DoD announced that the JEDI Contract had been awarded to Microsoft, to the shock of industry analysts and experts—and indeed, even to Microsoft itself, which was not prepared to issue a statement until the following day.[61] The SSA's decision

---

[58] *Statement From Chief Pentagon Spokesperson Jonathan Rath Hoffman on DOD Cloud Update*, Dep't of Defense (Oct. 22, 2019), https://www.defense.gov/Newsroom/Releases/Release/Article/1995650/statement-from-chief-pentagon-spokesperson-jonathan-rath-hoffman-on-dod-cloud-u/.

[59] Aaron Gregg, *Defense Secretary Mark Esper Recuses Himself from Massive Pentagon Contract, Citing Son's Employment*, Wash. Post (Oct. 22, 2019), https://www.washingtonpost.com/business/2019/10/22/defense-secretary-mark-esper-recuses-himself-pentagon-cloud-review-citing-sons-employment/.

[60] Karen Weise, *Amazon and Microsoft Are 2 Finalists for $10 Billion Pentagon Contract*, N.Y. Times (Apr. 10, 2019), https://www.nytimes.com/2019/04/10/technology/amazon-microsoft-jedi-pentagon.html.

[61] Emily Birnbaum, *Amazon Poised to Escalate Pentagon "War Cloud" Fight*, The Hill (Oct. 29, 2016), https://thehill.com/policy/technology/467827-amazon-poised-to-escalate-pentagon-war-cloud-fight.

indicated Microsoft's proposal presented the best value to the Government [redacted]. SSDD at 9. In particular, the SSA found that although [redacted]. *Id.* at 7–8. Moreover, under Factor 9, Price, the SSA noted that Microsoft's total evaluated price was [redacted] *Id.* at 9. Accordingly, the SSA selected Microsoft for award of the JEDI Contract.

189. Despite the significance of the JEDI procurement—which has been years in the making and has a potential ceiling of $10 billion—on the same day DoD announced its award decision, DoD provided AWS a written debriefing detailing the evaluation results and advised AWS that it had two business days to submit written questions based on the debriefing, foreclosing the opportunity for AWS to request and receive an in-person debriefing. As a result, AWS was forced to abide by DoD's instruction to submit written debriefing questions in short order.

190. On October 29, 2019, AWS timely submitted 265 detailed written debriefing questions, as allowed by 10 U.S.C. § 2305(b)(5)(B)(vii), (C), in the hope that DoD would provide in writing what it refused to provide in person. AWS's debriefing questions sought a more detailed explanation for how DoD reached its unexpected decision to award the JEDI Contract to Microsoft.[62]

---

62 [redacted]

[redacted]

191. In violation of applicable procurement regulations, DoD failed to provide "reasonable responses to relevant questions about whether source selection procedures contained in the solicitation, applicable regulation, and other applicable authorities were followed." *See* 48 C.F.R. § 15.506(d). In fact, DoD did not provide a substantive response to a single one of the 265 questions that AWS timely submitted, leaving AWS in the dark about DoD's explanations for the substantive issues for which AWS raised concern in the debriefing questions. Instead, DoD subjectively determined which of AWS's questions were "relevant" and then blithely stated that "[a]ll 265 questions were reviewed and reasonable responses are provided herein for relevant questions, in accordance with FAR 15.506." What followed, however, was anything but reasonable, with DoD providing broad, overarching responses that generically referenced the Agency's evaluation reports, and utterly failed to provide a single substantive response.

CLAIMS FOR RELIEF

COUNT ONE
(Failure to Evaluate AWS Proposal in Accordance with Solicitation)

192. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

193. Government officials are required to conduct procurements in a manner consistent will the terms of the RFP and applicable law and regulations. Failure to do so is, by definition, arbitrary and capricious. Evaluation judgments that are unsupported in the administrative record

[redacted]

[redacted]

are arbitrary and capricious and cannot form the basis of a valid award decision. 5 U.S.C. § 706(2)(A).

194. DoD determined [redacted] a superficial evaluation that deviated from the RFP's stated criteria for obtaining a cutting-edge and market-leading cloud solution.

195. The RFP's SOO clearly outlined DoD's desire for a modern cloud solution capable of scaling alongside increasing threats to the warfighter:

> To maintain our military advantage, DoD requires an extensible and secure cloud environment that spans the homeland to the global tactical edge, as well as the ability to rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance. These foundational infrastructure and platform technologies are needed for DoD to capitalize on modern software, keep pace with commercial innovation, and make use of artificial intelligence and machine learning capabilities at scale.

SOO at 1.

196. Moreover, in its report to Congress on the JEDI procurement, DoD acknowledged that:

> Battlefield advantage is driven by who has access to the best information that can be analyzed to inform decision making at the point and time of need. This advantage cannot be achieved at scale in the absence of an enterprise approach to adopting cloud technology. The 2018 National Defense Strategy (NDS) makes clear that ***the DoD needs a more lethal, resilient, and innovative Joint Force to preserve peace through strength and prevail in conflict when necessary***. The NDS therefore prioritizes investments in cyber security, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Rapidly providing the DoD access to underlying foundational technologies, like cloud computing and data storage, on a global scale is critical to national defense and preparing the DoD to fight and win wars.

Combined Congressional Report to Congress at 4 (emphasis added).

[redacted]

197. AWS's cloud solution exceeded the high bar set by DoD for JEDI. AWS offered advanced cloud capabilities that Microsoft could not match. These capabilities included AWS's leading Nitro architecture—AWS's purpose-built, hardware-based virtualization tool that provides exceptional security and performance for DoD users. Moreover, [redacted], AWS offered a proven approach for developing and deploying cloud infrastructure and platforms at scale, which drastically reduces the risk of unsuccessful performance of the JEDI procurement. AWS's tactical edge computing devices are already being used on the battlefield by DoD. No other offeror—including Microsoft—has remotely similar capabilities or experience.

198. Despite AWS's more advanced technology—which is widely recognized in the industry as market-leading—DoD somehow concluded [redacted]. As detailed above, this determination was arbitrary and capricious, contrary to the RFP, and without basis in the evaluation record. Under a rational evaluation, [redacted], and DoD would have awarded the JEDI Contract to AWS.

COUNT TWO
(Failure to Evaluate Microsoft Proposal in Accordance with Solicitation)

199. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

200. DoD also evaluated Microsoft unreasonably, repeatedly deviating from the RFP's evaluation criteria in order to indicate falsely that Microsoft's cloud solution is in the same league as AWS's market-leading solution. *See* 5 U.S.C. § 706(2)(A).

201. Under Factor 2, DoD deviated from the RFP's stated criteria for hypervisor security and performance by failing to recognize that Microsoft's Hyper-V solution does not provide

[redacted]

sufficient security for DoD's sensitive operations. As discussed above, unlike AWS's revolutionary and proprietary Nitro hypervisor, Microsoft's Hyper-V is ***not*** purpose-built, ***not*** hardware-based, and ***not*** invulnerable to hypervisor breakout attacks. DoD acknowledged as much when finding that AWS's Nitro solution is "extraordinary," "beyond the industry-standard approach," and deserving of "special note." TEB Factor 2 IPR Report at 1; SSEB Report at 4–5. [redacted]

202. Under Factor 3, DoD again deviated from the evaluation criteria and engaged in disparate treatment. [redacted] But rather than finding Microsoft un-awardable based on this deficiency, DoD allowed Microsoft to proceed unscathed. [redacted]

203. Under Factor 4, DoD arbitrarily concluded that [redacted] with respect to information security and access controls. A critical component of information security for the JEDI Contract is the security of offerors' proposed hypervisors. RFP at 82–83. As noted above, Microsoft's Hyper-V solution lags behind AWS's Nitro in terms of security, as shown by the fact that the National Institute of Standards and Technology National Vulnerability Database has documented numerous Common Vulnerabilities and Exposures entries

[redacted]

for Hyper-V over the last three years. Moreover, given Microsoft's Hyper-V is ***not*** purpose-built, ***not*** hardware-based, and ***not*** invulnerable to hypervisor breakout attacks, it certainly is not as secure as AWS's Nitro hypervisor. Furthermore, as both Microsoft's online technical documentation and reputable industry reports indicate, Microsoft does not have the capability to tag resources and users for access control policies.[63] Microsoft's access control capabilities therefore fail to satisfy the RFP's requirements.

204. Under Factor 5, DoD erroneously concluded— [redacted]. The SSAC Report reveals that this determination was based solely on DoD's mistaken conclusion that [redacted] SSAC Report at 7–8. As discussed above, however, this is patently untrue. In reality, Microsoft's offering is inferior to AWS's in material ways. For example, AWS's proposal [redacted] *See* AWS FPR, Volume III, Tab E at 3. These 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 not only has a marketplace, but is ***the only cloud service provider with an authorization to operate.***

205. Under Factor 6, DoD arbitrarily determined [redacted] Microsoft,

---

[63] *National Vulnerability Database*, Nat'l Inst. of Stds. & Tech., https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=hyper-v&search_type=all.

[redacted]

however, does not have experience working with [redacted] or DoD Combatant Commands, operating classified cloud environments, or hosting classified data at the scale contemplated by JEDI. In fact, AWS is the ***only*** offeror with such experience, having performed the [redacted]. AWS therefore has industry-leading cloud capabilities. Indeed, AWS's performance [redacted] was one of the primary drivers of industry concerns that DoD designed the JEDI Contract specifically for AWS, because the industry believed AWS, [redacted], was ahead of the rest of the industry with respect to hosting classified data. DoD could not have reasonably concluded that Microsoft, which lacks experience operating classified cloud environments and hosting classified data, proposed a more effective performance approach than AWS.

206. Finally, under Factor 8, DoD erroneously concluded that [redacted]. That is impossible. For example, the Factor 8 demonstration instructions for Scenario 8.3 required offerors to perform tests on their ***portable*** tactical edge devices related to their durability and interface with the cloud environment in both connected and disconnected mode. *See* Second Demonstration Procedures at 7–10. [redacted] Microsoft therefore could not have demonstrated the required testing. Similarly, the Factor 8 demonstration instructions for Scenario 8.4 explicitly required offerors to demonstrate, among other things, access-based controls for tagging. Second Demonstration Procedures at 12. As noted above, however, both Microsoft's online technical documentation and reputable industry reports indicate Microsoft does not have the capability to tag resources and

[redacted]

users for access control policies. Microsoft could not have demonstrated what it affirmatively lacks the capability to do, and it therefore deserved a lower rating under Factor 8.

207. The above examples of the Agency's erroneous and disparate evaluation merely scratch the surface of the unexplainable evaluation errors in the record. There are numerous other unsupported evaluation judgments that improperly skewed the best value source selection decision in Microsoft's favor.

208. [redacted]

209. AWS was prejudiced by DoD's failure to evaluate Microsoft's proposal in accordance with the RFP. Had DoD evaluated Microsoft's proposal in accordance with the terms of the solicitation, it would have determined that AWS's proposal demonstrated the best value to the Government and awarded the contract to AWS.

COUNT THREE
(Wrongful Deprivation of Competitive Advantage)

210. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

211. Throughout the JEDI procurement process, DoD—without any technical justification—took affirmative steps to deprive AWS of its competitive advantage over Microsoft and level the playing field so that DoD could justify its award to a technically inferior competitor.

[redacted]

212. These affirmative steps included not evaluating past performance, prohibiting AWS from leveraging its existing classified infrastructure for the JEDI Contract, and precluding AWS from relying on [redacted] and [redacted] under the Price Scenarios. *See* RFP Amend. 0005.

213. DoD's directed changes resulted in a [redacted].

214. But for DoD's arbitrary and capricious conduct, AWS [redacted] and would have received the JEDI Contract. *See* 5 U.S.C. § 706(2)(A).

COUNT FOUR
(Irrational Best Value Decision)

215. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

216. DoD's best value source selection decision is fundamentally flawed because of the numerous prejudicial errors described above and evident in DoD's evaluation materials. *See* 5 U.S.C. § 706(2)(A).

217. These prejudicial errors resulted in DoD arbitrarily concluding that [redacted]

218. But for DoD's erroneous and unsupported evaluation judgments, DoD would have concluded that [redacted],

[redacted]

[redacted]

COUNT FIVE
(Bias and Bad Faith)

219. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

220. President Trump's bias against AWS improperly influenced DoD officials responsible for the JEDI solicitation, undermined the procurement process, resulted in an unreasonable evaluation, and unfairly deprived AWS of the JEDI award. DoD engaged in arbitrary, capricious, and unlawful conduct through its biased, bad-faith decision making in its proposal evaluations and award decision. *See* 5 U.S.C. § 706(2)(A).

221. The SSA and SSAC's abilities to rationally evaluate the proposals and to award the JEDI Contract were tainted by President Trump's repeated statements against Amazon at key decision points during the proposal evaluation process. This Court and its predecessor have found bad faith where there is a conspiracy to "get rid of" an offeror; where the Government's course of conduct was "designedly oppressive" as to a particular competitor; and where the Government's actions are "motivated alone by malice." Although Government officials are presumed to act in good faith, the President's public campaign against Amazon, coupled with DoD's suspect last-minute efforts to "review" the JEDI proposal and Secretary Esper's subsequent, post-award decision to recuse himself from that review, is sufficient to rebut that presumption.

222. As discussed above, DoD's ever-increasing hostility toward AWS (and favoritism towards AWS's only remaining competitor, Microsoft) is evidenced throughout the selection process, and in particular, in how DoD changed, reinterpreted, or ignored the original RFP requirements, minimized, on technical and risk grounds, the factors on which AWS was

[redacted]

objectively superior to make it appear as though [redacted], and conjured post-hoc requirements or simply mischaracterized AWS's offerings to make it appear as though [redacted] in certain regards.

223. Amazon was prejudiced by DoD's biased and bad faith actions.

COUNT SIX
(Violation of Procurement Law and Regulation)

224. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

225. DoD's evaluation of AWS's proposal and award decision violated numerous procurement statutes and regulations, including (1) statutory and regulatory conflict of interest provisions; (2) regulatory requirements to treat offerors impartially; and (3) regulatory requirements to evaluate proposals exclusively against stated evaluation criteria, as discussed below.

226. The Administration created a conflict of interest by demonstrating through repeated conduct that Executive Branch employees who do not follow President Trump's directives are at risk of losing their jobs. Secretary Mattis was but one in a series of dismissals by the Trump Administration of individuals who refused to do the President's bidding. The fact that the decision makers knew that their continued employment likely depended on selecting Microsoft created a conflict. *See, e.g.*, 18 U.S.C. § 208 (prohibiting executive branch employees, among others, from participating personally and substantially as a Government officer in a contract in which they have a financial interest); 5 C.F.R. § 2635.403(c) (employee of executive branch barred from participating personally and substantially in decision in which, to his knowledge, he has a financial interest).

[redacted]

227. In violation of 48 C.F.R. § 3.101-1, DoD failed to give fair consideration to AWS and to treat it impartially.

228. In violation of 48 C.F.R. § 15.305, DoD applied an unstated evaluation criteria to its review of AWS's proposal—the unstated criteria that, per President Trump's directive, AWS not be awarded the JEDI Contract.

229. Amazon was prejudiced by DoD's numerous violations of procurement law.

COUNT SEVEN
(Breach of Implied Contract of Good Faith and Fair Dealing)

230. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

231. As a bidder on the JEDI procurement, AWS had an implied contract of good faith and fair dealing with DoD.

232. DoD breached the implied contract to consider all bids fairly and honestly by conducting the procurement in an arbitrary, capricious, and irrational manner.

233. President Trump induced DoD to conduct the procurement in a manner that breached the implied contract of good faith and fair dealing between the Government and AWS.

234. Amazon was prejudiced by DoD's breach of the implied contract of good faith and fair dealing.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully asks this Court to enter judgment in its favor and against Defendant and to:

A. Declare that DoD's rejection of AWS's proposal and award to Microsoft is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

B. Enjoin DoD and Microsoft from commencing performance on the JEDI Contract pending reevaluation and a new award decision;

C. Direct DoD to reevaluate proposals or, in the alternative, reopen discussions with Microsoft and AWS, solicit and reevaluate revised proposals, and make a new best value decision;

D. Award to Amazon its attorney's fees and costs in pursuing this action, and/or its proposal costs; and

E. Grant such other relief as the Court deems appropriate.

Dated: November 22, 2019 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
Sandeep N. Nandivada
Caitlin A. Crujido
Alissandra D. Young
MORRISON & FOERSTER LLP
2000 Pennsylvania Ave., NW
Washington, DC 20006-1888

Theodore B. Olson
F. Joseph Warin
Andrew S. Tulumello
Daniel P. Chung
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Ave., NW
Washington, D.C. 20036-5306

Theodore J. Boutrous, Jr.
Richard J. Doren
Eric D. Vandevelde
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Ave.
Los Angeles, CA 90071-3197