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.

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

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] 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

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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.