JUSTIFICATION & APPROVAL FOR FEDERAL ACQUISITION REGULATION SUBPART 16.5 ACQUISITIONS EXCEPTION TO FAIR OPPORTUNITY

Multiple Award Contract
Orders under Fair Opportunity
Federal Acquisition Regulation (FAR) 16.505(b), Defense FAR Supplement 216.505(b),
Procedures, Guidance, and Information 216.505(b)

Military Interdepartmental Purchase Request Number: N0016725MP00231
Joint Warfighting Cloud Capability (JWCC) Contract Number: HC105023D0003
Task Order (TO) Number: To Be Determined
Procurement Title: Strategic Cloud Platform – Enterprise Mission Integration
Estimated Value: ██████████
Statutory and Regulatory Authority: 10 United States Code (U.S.C.) 3204(a) and FAR
16.505(b)(2)(i)(B)

EXCEPTION TO FAIR OPPORTUNITY
Number: JA25-111

Upon the basis of the following justification, I, as the Head of Contracting Activity, hereby
approve this exception to fair opportunity pursuant to the Statutory Authority of 10 U.S.C.
3204(a) and Regulatory Authority of FAR 16.505(b)(2)(i)(B).

1. REQUESTING AGENCY AND CONTRACTING OFFICE:

Requesting Agency:
U.S. Navy / Cyber Engineering & Digital Transformation Directorate, Naval Sea Systems
Command (NAVSEA) 03
1333 Isaac Hull Ave SE
Washington Navy Yard, DC 20376-0005

Contracting Activity:
Defense Information Systems Agency/Defense Information Technology Contracting
Organization/PS8511
2300 East Drive
Scott Air Force Base, IL 62225-5406

2. NATURE/DESCRIPTION OF ACTION(S):

This action is to issue a firm-fixed-price TO against the JWCC Indefinite Delivery/Indefinite
Quantity Contract for NAVSEA's Strategic Cloud Platform – Enterprise Mission Integration.
This TO will be issued directly to Microsoft Corporation. The anticipated period of performance
(PoP) is for a 1-year base period, plus two 1-year option periods. The total estimated value is
██████████ which will be funded by Working Capital funds.

3. DESCRIPTION OF SUPPLIES/SERVICES:

This requirement is for the lift and shift of an existing NAVSEA cloud environment. The NAVSEA requirement is a fit-for-purpose designated cloud platform that provides access to the Navy and Department of Defense (DoD) programs. The mission of NAVSEA is to continue to collect, store, translate, enrich, and publish critical program data to both external and internal subscribers across the DoD. The objective of transitioning the NAVSEA Impact Level (IL)5 and IL6 cloud effort, including current cloud hosting services for existing infrastructure-as-a-service (IaaS) requirements, is to ensure continued enterprise mission integration operations.

4. SUPPORTING RATIONALE, INCLUDING A DEMONSTRATION THAT THE PROPOSED CONTRACTOR'S UNIQUE QUALIFICATIONS OR THE NATURE OF THE ACQUISITION REQUIRES USE OF AN EXCEPTION TO FAIR OPPORTUNITY:

(a) Exception to Fair Opportunity.

FAR 16.505(b)(2)(i)(B) - Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized.

(b) Description of the Justification.

In order to ensure continued enterprise mission integrations operations, NAVSEA requires use of Azure Data Transfer, Azure Kubernetes Service (AKS), Azure Structured Query Language (SQL) platform-as-a-service (PaaS), Azure Key Vault, Azure Monitor, and ExpressRoute networking provided within the Microsoft environment. Without the use of these services, the NAVSEA Cloud Program mission systems would be unable to provide critical mission capabilities. It is infeasible to modify Microsoft's unique applications to work within another cloud service provider's (CSP) environment. In order for another CSP to host the NAVSEA environment, the Government would need to re-engineer the solution from the ground up. This will require the integration of a new cloud environment, and re-engineering of operational applications that support Defensive Cyber Operations (DCO), which would result in a break in service and inevitable mission failures. Azure Data Transfer is a cloud-based cross domain solution (CDS) that provides scalable and reliable delivery of data from one cloud security domain to another and allows for the cross domaining of data between IL5 and IL6. While other CSPs provide similar CDS, only the Azure Data Transfer service has been verified to handle both the specific data types and the required volume of data associated with current mission owner operations. These workloads include processing and storage of Controlled Unclassified Information (CUI), Classified Navy Non-Propulsion Nuclear Information (NNPI), and real-time data flows in support of mission owners aligned with the Office of the Chief of Naval Operations codes N96, N97, and N98. NAVSEA cloud was designed as a fit-for-purpose environment hosted in Microsoft GovCloud to address these operational, security, and data sovereignty requirements.

The platform holds both an Authority to Operate (ATO) and Authority to Connect, approved under oversight from the Functional Authorizing Official (FAO) and the Navy Authorizing Official (NAO). It is built entirely using Microsoft-native tools and services, including AKS, Azure SQL PaaS, Key Vault Key Management Service (KMS), Azure Monitor, and ExpressRoute networking, which are integrated within the existing cloud architecture and security controls. Introducing a different CSP would require full re-architecture of the environment and re-accreditation of security packages, which would not meet the Government's requirements for interoperability, operational continuity, and compliance within the current NAVSEA environment.

The core of the NAVSEA Cloud Program is Secure Cloud Computing Architecture (SCCA). These SCCA implementations carry full ATOs from the NAO, as well as endorsements for unclassified NNPI processing from NAVSEA 08 - Naval Reactors. NAVSEA Cloud Program SCCA also includes Cybersecurity Service Provider (CSSP) affiliation via Navy Cyber Defense Operations Command sensors, enabling mission owners to focus on building just their applications.

(c) Justification.

(1) Minimum Government requirements.

The cloud service offerings must continue at their current level in order to support the 15 active mission owners in the NAVSEA Cloud. These cloud service offerings include security, cyber, cloud hosting/operations delivered through Azure-native capabilities including AKS, Azure SQL/PostgreSQL PaaS, Key Vault KMS, Azure Policy/Blueprints, Azure Monitor/Log Analytics, and existing ExpressRoute connectivity in the Microsoft IL5 and IL6 environments. In addition, the cloud service offerings must seamlessly integrate into the existing NAVSEA architecture.

(2) Proposed sole source contractor. Microsoft Corporation

(3) Discussion regarding the cause of the sole source situation.

The only CSP capable of performing the transition of NAVSEA Cloud at the required level of quality is Microsoft. Re-architecting, re-engineering, and refactoring of any of the critical cloud service offerings from Microsoft to any other CSP would not meet the Government's need for compatibility. This is because the environment depends on Microsoft-unique services AKS, Azure SQL/PostgreSQL PaaS, Azure Key Vault KMS, Azure Policy/Blueprints, Azure Monitor/Log Analytics, Azure ExpressRoute connectivity, and inherited Risk Management Framework (RMF) controls that cannot be duplicated without significant delay and cost. Refactoring of the current environment from Microsoft to another CSP would cost an estimated ████████████ and delay NAVSEA at least 36 months. In addition, there would be a duplication of costs by having to keep the solution running on one platform while refactoring it on another platform, none of which would meet the Government's minimum need.

The environment also enables mission critical weapon systems testing and evaluation by hosting secure test data pipelines, simulation frameworks, and telemetry analysis tools essential for the development and deployment of next-generation naval combat systems. In addition, NAVSEA Cloud supports digital engineering platforms used by Warfare Centers and system commands to model and modernize Navy platforms. The environment hosts secure workloads at IL5 and IL6, enabling the compliant processing of CUI, classified test data, and Classified NNPI, in accordance with approvals from the FAO and NAO. The current Microsoft environment supports enterprise mission integrations and deployment through native containerized services—such as AKS and Azure Container Registry which are fully integrated and accredited within the Microsoft GovCloud region. These capabilities provide the speed, scalability, and responsiveness required to support afloat and shore-based systems but are specific to Microsoft and cannot be replicated into another CSP's environment without significant redevelopment and re-accreditation. Finally, the current environment underpins operational planning and wargaming systems that enable tactical analysis, scenario-based simulation, and mission rehearsal. Capabilities which are foundational to the performance of 15 mission owners across NAVSEA and directly impact warfighter readiness and execution. Without continued integration within the Microsoft infrastructure, all 15 of these mission owners would be critically affected by any delays in refactoring, reengineering, and rearchitecting.

(4) Demonstration of unique source.

Microsoft possesses the knowledge, skills, capabilities, certification, clearance, and experience required to continue the program without a break or degradation in critical mission services. Microsoft is the only source capable of providing the required transition and sustainment of the NAVSEA Cloud environment without introducing operational risk or mission degradation. The current environment is fully deployed within Microsoft GovCloud using Azure-unique, tightly integrated capabilities including AKS, Azure SQL/PostgreSQL PaaS, Key Vault–based KMS, Azure Policy/Blueprints for inherited RMF controls, Azure Monitor/Log Analytics for DCO, ExpressRoute connectivity, and the evaluated Azure Data Transfer CDS capable of moving the specific classified/unclassified data types and volumes required. These capabilities, along with established RMF/ATO artifacts and CSSP monitoring, represent institutional knowledge, configuration baselines, and security inheritance that other CSPs cannot replicate within the Microsoft cloud infrastructure. No other CSP can assume control of the environment without extensive re-engineering, retraining, and re-accreditation.

(5) Procurement discussion.

Based on outreach to all four JWCC CSPs in April 2025, the only CSP currently capable of meeting the Government's minimum technical and security requirements is Microsoft, using NAVSEA IL2, IL5, and IL6 cloud services to deliver fleet readiness analytics that provide real-time insights into platform availability, maintenance status, and deployment timelines, directly supporting OPNAV N96 and N97 decision-making.

Strategic Cloud Platform – Enterprise Mission Integration

> NAVSEA was collaborating with the current contractor to execute the final option period of the current task order that is set to expire in May 2026. However, there were unforeseen issues that resulted in a change with the current contractor and a modification for two, three-month extensions was put into place which now places the task order expiration on November 11, 2025. In addition, the current task order does not have IL6 capabilities available as required for the NAVSEA Cloud. Further delays would be detrimental to the mission and a new task order award is required soonest for timely transition of all customer workloads.

> (6) Impact.

> Transitioning to another CSP from Microsoft is not feasible based on the inability of any other CSP to seamlessly integrate within the existing architecture. The impact of not procuring through Microsoft would result in NAVSEA being unable to complete a successful and timely transition to JWCC resulting in mission failure. Additionally, it would delay NAVSEA's ability to deliver fleet critical readiness analytics that provide real-time insights into platform availability, maintenance status, and deployment timelines, negatively affecting OPNAV N96 and N97 decision-making for the warfighter.

5. COST/PRICE FAIR AND REASONABLE DETERMINATION:

A determination that the price is fair and reasonable will be based on a comparison of the contractor's proposal to the Independent Government Cost Estimate and the JWCC Catalog pricing, including any discounts, which was previously found to be fair and reasonable and based on the contractor's commercial pricing.

6. MARKET RESEARCH:

Market research for the basic JWCC Contracts was conducted and resulted in a signed market research report on November 9, 2021, that was revalidated and recertified on July 29, 2024. After a survey of the market, it was concluded that use of the JWCC Contract is in the Government's best interest due to technical feasibility and cost to the Government.

NAVSEA conducted market research in April 2025 specific to this requirement by reviewing available capabilities in the JWCC Contracts and it was determined that Microsoft is the only source capable of fulfilling the Government's minimum needs in the manner and timeframe required.

Market research was conducted using several techniques to assess the availability of alternative sources and validate the necessity of acquiring these services from Microsoft under the JWCC Contract including issuance of the *Additional Research to Support Exception to Fair Opportunity* in April 2025 to all four JWCC CSPs.

All four JWCC CSPs, AWS, Microsoft, Google Public Sector (GPS), and Oracle America, provided capability briefs to NAVSEA in April 2025 as a result of the *Additional Research to Support Exception to Fair Opportunity*. While general capabilities were described, AWS, GPS,

and Oracle America confirmed their lack of ability to support the full NAVSEA cloud requirement in its current configuration or timeframe. Only Microsoft confirmed service parity with the current environment and the ability to meet mission needs without introducing unacceptable operational risk.

7. ANY OTHER SUPPORTING FACTS: None.

8. ACTIONS THE AGENCY MAY TAKE TO REMOVE OR OVERCOME BARRIERS THAT LED TO THE EXCEPTION TO FAIR OPPORTUNITY:

   (a) Procurement History:

   Incumbent Contractor: G2OPs
   Contract Number: 47QFLA22D0003
   TO Number: 47QFLA22F0187
   PoP: May 11, 2021 – November 11, 2025
   Competitive Status: Small business set-aside
   Business Size: Woman-Owned Small Business

   (b) To overcome future barriers to competition, future development and enhancement of IaaS components will focus on adopting containerization standards in a way that is not tied to a single CSP. While the current environment leverages Microsoft-native containerized services, future efforts will emphasize portability through open containerization approaches. This evolution should allow more flexibility to shift workloads across CSPs in the future.

   The previous procurement was not based upon an exception to fair opportunity.

Strategic Cloud Platform – Enterprise Mission Integration

TECHNICAL CERTIFICATION: I certify that the supporting data under my cognizance which are included in the J&A are accurate and complete to the best of my

NAME: ███████████████   SIGNATURE: ████████████████

TITLE/AGENCY/ORGANIZATION: ██████████████████

PHONE: █████████

REQUIREMENTS CERTIFICATION: I certify that the supporting data under my cognizance which are included in the J&A are accurate and complete to the best of my knowledge and belief.

NAME: ███████████████   SIGNATURE: ████████████████

TITLE/AGENCY/ORGANIZATION: ████████████████████

PHONE: █████████

CONTRACTING OFFICER CERTIFICATION: I certify that this justification is accurate and complete to the best of my knowledge and belief.

NAME: █████████   SIGNATURE: ████████████████

TITLE/AGENCY/ORGANIZATION: ██████████████████

PHONE: █████████

HEAD OF THE CONTRACTING ACTIVITY APPROVAL: I have reviewed this justification and find it to be accurate and complete to the best of my knowledge and belief. Since this justification does not exceed $100M, this review serves as approval.

NAME: Mr. Douglas Packard   SIGNATURE: ████████████████

TITLE/AGENCY/ORGANIZATION: HCA, DISA/DITCO

PHONE: █████████

ALL QUESTIONS REGARDING THIS JUSTIFICATION ARE TO BE REFERRED TO:
█████████████████████████████████