DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES PERFORMANCE WORK STATEMENT (PWS)

Table of Contents

List of Tables

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

1. General

1.1 Background

The Department of Navy (DON) is increasing the use of commercial cloud services to maintain its technological advantage, better secure DON applications, and reduce costs. The commercial cloud services sought by the DON include, but are not limited to, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) Cloud Service Offerings (CSOs), cloud computing, information technology services, and professional support services. Commercial cloud professional support services may include in-depth technical analysis of the current environment, cloud migration support, change management, and training. It is the intent of the DON that the scope of this PWS is sufficiently broad and flexible to satisfy requirements that may change over the period of performance and be fully comprehensive so as to embrace the full complement of services that relate to commercial cloud services.

1.2 Scope of Work

The scope of this requirement includes delivery of commercial cloud services by Cloud Service Providers (CSPs) that are Federal Risk and Authorization Management Program (FedRAMP) approved and DoD Provisionally Authorized (PA) with a DON emphasis on aligning with NIST Special Publication 500-291, encompassing IaaS, PaaS, SaaS, and other commercially available CSOs as aligned with either the IaaS, PaaS, or SaaS service delivery model in accordance with the Cloud Computing Security Requirements Guide, at information Impact Levels (IL) 2, 4, and 5, as defined in the NIST Special Publication 800-145. In addition, the Contractor shall provide related services that enable mission owner transition to and operation in the commercial cloud environment.

The DON requires engineering support to analyze Cloud requirements and to develop and implement recommended solutions. The types of services and solutions required include the following Task Areas: Network Normalization, Identity and Access Management, Enterprise Services, Cloud Computing, Storage Services, Secure File Transfer Services, Virtual Machine Services, Database Hosting Services, Web Hosting Services, Hosting Optimization, Development and Test Hosting Services, Training and Professional Services. Cloud service delivery may necessitate Contractor provision of commercial off-the-shelf software and maintenance thereof, and COTS IT new equipment. These services will enable the DON to transition from current hosting environments to the Commercial Cloud.

The commercial cloud services will be provided as commercial catalog or market price list offerings that keep pace with technology and meet DON commercial cloud service requirements. The Contractor shall provide for new technologies and refresh their offerings under the Agreement in accordance with the Contractor's commercial business practices, as DON cloud requirements change, and in accordance with this Agreement, over the full period of performance.

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Services within the scope of the Agreement may be modified or added in accordance with FedRAMP and DoD PA approved CSPs, CSOs, and service items available on the Agreement Holder's GSA Schedule Contract(s) and BPA.

Decentralized ordering against this BPA is authorized by DON Ordering Contracting Officers and organizations supporting DON requirements where authorized by Navy Cloud Brokers (NCBs). Government contractors supporting DON may also be authorized to use the Agreement, where authorized by a Navy Cloud Broker, solely for the purpose of fulfilling a DON requirement. Service delivery shall fulfill CONUS, Outlying Areas and OCONUS commercial cloud requirements within scope of this Agreement and the Agreement Holder's GSA Schedule Contract(s).

NOTE: Work will not be performed in Afghanistan.

1.3 Definitions

(a) "DON" is the Department of the Navy at the seat of government; the headquarters, US Marine Corps; the entire operating forces of the United States Navy and of the US Marine Corps, including the Reserve Components of such forces; all field activities, headquarters, forces, bases, installations, activities, and functions under the control or supervision of the Secretary of the Navy; and the US Coast Guard when operating as a part of the Navy pursuant to law.

(b) The term "Contractor" in this PWS means the total Contractor organization or a separate entity of it, such as an affiliate, division, or plant that performs its own purchasing. References to the "Contractor" include any supplier, distributor, vendor, or firm that furnishes supplies or services to or for the prime Contractor or another subcontractor or teaming partner.

(c) The term "Customer" refers to the cloud service consumer, Government activity within the DON for whom the individual task order is being issued, or Contractors supporting the DON that are required to use this contract as a Government Source of Supply, when authorized by PEO-EIS and the Ordering Contracting Officer.

(d) A "Cloud Service Provider" (CSP) is an entity that offers one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third party facilities such as data centers, carrier hotels / collocation facilities, and Internet Exchange Points (IXPs)). CSPs offering SaaS may leverage one or more third party Cloud Service Offerings (CSOs) (i.e., for IaaS or PaaS) to build out a capability or offering.

(e) A "Cloud Service Offering" (CSO) is the actual IaaS, PaaS, and SaaS solution available from a CSP.

(f) Currently, there are four (4) deployment models as defined below:

1. "Private cloud" – The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned,

managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

2. "Community cloud" – The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
3. "Public cloud" – The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or Government organization, or some combination of them. It exists on the premises of the cloud provider.
4. "Hybrid cloud" – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

(g) "Continuous United States (CONUS)" means the 48 contiguous States and the District of Columbia.

(h) "Outlying Areas" means—

1. *Commonwealths*
a. Puerto Rico
b. The Northern Mariana Islands
2. *Territories*
a. American Samoa
b. Guam
c. U.S. Virgin Islands and
3. *Minor outlying islands*
a. Baker Island
b. Howland Island
c. Jarvis Island
d. Johnson Atoll
e. Kingman Reef
f. Midway Islands
g. Navassa Island
h. Palmyra Atoll
i. Wake Atoll

1.4 Applicable Documents

The Contractor shall adhere to the following documentation, or any revisions/updates thereto, incorporated into this Agreement or a task order issued pursuant to this Agreement. If a revision or update is perceived to create price, schedule, or technical changes to the Agreement, the Contractor shall notify the Procuring Contracting Officer (PCO) of the impacts of the change in accordance with the Changes clause of the Agreement. Contractor implementation of the change shall follow PCO instructions. Other documents required for execution of task orders issued under the Agreement will be detailed in individual task orders.

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Table 1-1: Applicable Documents

Document/Title/Website	Title
Defense Information Systems Agency, the Security Technical Implementation Guide (STIG): https://iase.disa.mil/stigs/Pages/index.aspx	Security Technical Implementation Guides (STIGs) (Current as of date of Agreement award, unless revised at the Task Order level)
DoDM 8530.01 http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf	Defense Cyber Operations – Internal Defensive Measures dated 25 July 2017
DISA Cloud Connection Process Guide (CCPG): https://www.disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf	DoD Cloud Connection Process Guide v2, March 2017
International Traffic and Arms Regulation (ITAR): https://www.pmddtc.state.gov/regulations_laws/itar.html	Official International Traffic and Arms Regulation (ITAR) Annual Edition, as of 6 September 2017
DoD Information System Certification and Accreditation Reciprocity: http://www.doncio.navy.mil/uploads/0727CYR27494.pdf	Memorandum for DoD Information System Certification and Accreditation Reciprocity, 23 July 2009
Office of Personnel Management (OPM) Federal Investigations Notice 10-06: https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2010/fin-10-06.pdf	OPM Position Designation System 2010 guides agencies in determining the proper level of investigation and screening required based on an assessment of risk and national security sensitivity.
RMF Process Guide v1.0	US Fleet Cyber Command (FCC) / Space and Naval Warfare (SPAWAR) Command Navy Authorization Official and Security Control Assessor Risk Management Framework Process Guide V1.0, 31 August 2015
36 CFR 1194 July 1, 2011	Implementing section 508 of the Rehabilitation Act of 1973; Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996"
CJCSI 6510.01F	Information Assurance (IA) and Computer Network Defense (CND), July 2015

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Document/Title/Website	Title
CNSS No. 6 https://www.hsdl.org/?view&did=487788	National Policy on Certification and Accreditation of National Security Systems, October 2005
CNSSI 1253	Security Categorization and Control Selection for National Security Systems, 27 March 2014
CNSSI 1253F	Security Overlays Template, 01 June 2013
CNSSI 4009	Committee on National Security Systems (CNSS) Glossary, 6 April 2015
COMNAVNETWARCOM Communications Tasking Order (CTO) 11-16	Secure Configuration Compliance Validation Initiative and Vulnerability Remediation Asset Manager (VRAM) Requirements
CYBERCOM CTO 10-84	USB Flash Media/Thumb Drive Devices are Prohibited in DoD, 2010
DoD 5205.02-M http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520502m.pdf	DoD Manual Operations Security Manual, 03 November 2008
DoD 5220.22-M http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf	DoD Manual- National Industrial Security Program Operating Manual (NISPOM), 28 February 2006; incorporating change 2, 18 May 2016
DoD 8570.01-M http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf	DoD 8570.01-M Information Assurance Workforce Improvement Program, Dated 19 December 2005, Incorporating Change 4, 11/10/2015
DoD Cloud Computing SRG https://iasecontent.disa.mil/cloud/SRG/index.html	DoD Cloud Computing Security Requirements Guide Version 1, Release 3 (SRG), 6 March 2017 (this version applies to contracted work unless otherwise authorized by the PCO, or OCO for individual task orders).
DoD Directive (DoDD) 8000.01 http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf	Management of the Department of Defense Information Enterprise (DoDIE) July 27, 2017
DoD Instruction 5000.02 https://www.acq.osd.mil/fo/docs/500002p.pdf	Operation of the Defense Acquisition System, 07 January 2015
DoD Instruction 5015.02	DoD Records Management Directive,

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Document/Title/Website	Title
	August 17, 2017
DoD Instruction 5200.02 http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520002_2014.pdf	DoD Personnel Security Program, Change 1, September 2014
DoD Manual (DoDM) 5200.01 Vol 3 http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001_vol3.pdf	Information Security Program: Protection of Classified Information, Volume 3, March 2013
DoD Manual (DoDM) 5200.01 Vol 4 http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001_vol4.pdf	Information Security Program: Controlled Unclassified Information, Volume 4, 24 Feb 2012
DoD O 8530.1-M	Computer Network Defense (CND) Service Provider Certification and Accreditation Process, 17 December, 2003
DoDD 5205.02E	DoD Directive Operations Security (OPSEC) Program, 20 June 2012
DoDD 5210.50	Unauthorized Disclosure of Classified Information to the Public, 27 October 2014
DoDD 5220.22	DoD Directive- National Industrial Security Program, 27 September 2004
DoDD 5230.29	Security and Policy Review of DoD Information for Public Release, 13 August 2014
DoDI 5230.24	Department of Defense Instruction Distribution Statements on Technical Documents, 23 August 2012
DoDD 5530.3	DoD Directive 5530.3, International Agreements, June 11, 1987 as amended
DoDD 8140.01	DoD Directive 8140.01, Cyberspace Workforce Management, 11 August 2015
DoDI 8500.01	Cybersecurity, 14 March 2014
DoDI 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014, as amended 24 May 2016
DoDI 8520.03	Department of Defense Instruction Identity Authentication for Information Systems, 13

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Document/Title/Website	Title
	May 2011
DoDI 8520.2	Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011
DODI 8530.01	Cybersecurity Activities Support to DoD Information Network Operations , March 7, 3026 and Change 1 25 July 2017 and all policies cited therein
DoD O-8530.1-M	Department of Defense Computer Network Defense (CND) Service Provider Certification Accreditation Program, dated 17 Dec 2003
DoDI 8551.01	Ports, Protocols, and Services Management (PPSM), 28 May 2014
DoDD 8570.1	DoD Directive 8570.1, Information Assurance Certification Requirements, 10 November 2015
DoDI 8582.01	Security of Unclassified DoD Information on Non-DoD Information Systems, 06 June 2012
DoDM 5200.2	DoD MANUAL 5200.02 PROCEDURES FOR THE DoD PERSONNEL SECURITY PROGRAM (PSP), April 2017
DON CIO Brokerage Policy	Navy Commercial Cloud Brokerage Policy Memo from DON Deputy CIO (Navy), 19 December 2017
DON DCIO	Navy Cloud First Policy, 01 February 2017
DON CIO Memo	Memo on the acquisition and use of Commercial Cloud Computing Services, 15 May 2015
DTM-08-003	Next Generation Common Access Card (CAC) Implementation Guidance, 01 December 2008
Executive Order 13526	Classified National Security Information, 29 December 2009
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, February 2004
FIPS 200	Minimum Security Requirements for

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Document/Title/Website	Title
	Federal Information and Information Systems, March 2006
FIPS 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors, September 2013
FISMA 2002	The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014
HSPD 12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004
CNSSP NATIONAL POLICY #11	Committee on National Security Systems National Policy Governing the Acquisition of IA and IA-Enabled IT, June 2003
FIPS 140-2	Security Requirements for Cryptographic Modules, 03 Dec 2002
NIST SP 500-292	Cloud Computing Reference Architecture, September 2011
NIST SP 800-88 Revision 1	Guidelines for Media Sanitization, Rev 1, 17 Dec 2014
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment, September 2008
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
NIST SP 800-137 Revision 1	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
NIST SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing, December 2011
NIST SP 800-145	The NIST Definition of Cloud Computing, September 2011
NIST SP 800-146	Cloud Computing Synopsis & Recommendations, May 2012
NIST SP 800-160	Systems Security Engineering: An

Document/Title/Website	Title
	Integrated Approach to Building Trustworthy Resilient Systems, 03 Jan 2018
NIST SP 800-171 Revision 1	Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015, Revision 1 December 2016; updated 20 February 2018
NIST SP 800-30 Revision 1	Guide for Conducting Risk Assessments, September 2012
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems, Nov 2010
NIST SP 800-37 Revision 1	Guide for Applying the Risk Management Framework to Federal Information Systems, 10 Jun 2014
NIST SP 800-39	Managing Information Security Risk, March 2011
NIST SP 800-41, Rev1	Guidelines and Best Practices for DMZ/Firewall, September 2009
NIST SP 800-146	Cloud Computing Synopsis and Recommendations, May 2012
NIST SP 800-53 Revision 5	Security and Privacy Controls for Federal Information Systems and Organizations, 15 Aug 2017
NIST SP 800-59	Guideline for Identifying an Information System as a National Security System, August 2003
NIST SP 800-60 Volume 1 Revision 1	Guide to Mapping Types of Information and Information Systems to Security Categories, August 2008
NIST SP 800-60 Volume 2 Revision 1	Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
NIST SP 800-61 Revision 2	Computer Security Incident Handling Guide, August 2012
NIST SP 800-66, Revision 1	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Document/Title/Website	Title
NIST SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006
NIST SP 800-88, Revision 1	Guidelines for Media Sanitization, December 2014
NIST SP 800-Series	National Institute of Standards and Technology Special Publications 800 Computer Security Policies, Procedures, and Guidelines
NIST SP 800-47	Security Guide for Interconnecting Information Technology Systems, September 2002
NIST SP 800-18, Rev1	Guide for Developing Security Plans for Federal Information Systems, February 2006
OMB Circular A-130	Office of Management and Budget "Management of Federal Information Resources" and Appendix III, "Security of Federal Automated Information Systems", 27 Jul 2016
OMB Memorandum M-04-04	E-Authentication Guidance for Federal Agencies, 16 December 2003
OPNAVINST N9210.3	Safeguarding of Naval Nuclear Propulsion Information (NNPI), 07 Jun 2010
SECNAV Manual M-5510.30	DON Personnel Security Program, June 2006
SECNAVINST 5239.19	DON Computer Network Incident Response and Reporting Requirements, 18 March 2008
SECNAV M-5239.2	Cyberspace Information Technology And Cybersecurity Workforce Management And Qualification Manual, June 2016
SECNAVINST 5239.20A	DON Cyberspace IT and Cybersecurity
SECNAVINST 5239.3B	Department of the Navy Information Assurance Policy, 17 June 2009
SECNAVINST 5510.30B	DON Personnel Security Program (PSP) Instruction, 06 October 2006
SPAWAR INST 3432.1	SPAWAR OPSEC Policy, 2 Feb 2005

1.5 Certification and Accreditation Requirements

Any CSP performing contracted cloud services shall possess a DoD PA(s) for any required CSOs (IaaS, PaaS, and SaaS) at IL 2, 4 and 5, in accordance with DFARS 239.7602-1 General.

1.6 Quality Assurance

The Government will evaluate the Contractor's performance of the task orders issued under this Agreement in accordance with the Quality Assurance Surveillance Plan (attached to the task order), using methods standard in the commercial industry to validate performance has been in accordance with the Agreement performance standards. Annual Performance Evaluation Reporting using the Government-wide Contractor Performance Assessment (CPARS) Reporting Tool shall be performed, as required by FAR 42.15, and as supplemented at the individual task order level.

1.7 Hours of Operation

The Contractor is responsible for conducting business during the hours required on each individual task order.

1.8 Special Provisions

When recommending or purchasing commercial software products, hardware, and related services supporting DON programs and projects, the Contractor shall recommend or procure items from approved sources in accordance with the latest DON and DoD policies.

> ***DON Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program:*** *Pursuant to DON Memorandum – Mandatory use of DON Enterprise Licensing Agreement (ELA) dated 22 Feb 2012, Contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DON ELAs, and, if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DON ELA program, Contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and Government-wide SmartBUY program (see DoD memorandum dated 22 December 2005).*

The Contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Purchases from DON ESL, DoD ESI, and SmartBUY Agreements are for the sole purpose of supporting DON requirements in the Contractor's cloud environment and may not be used for any other purpose.

The listing of commercial software available from DoD ESI and DON ESL sources can be viewed on the website at http://www.esi.mil/.

The listing of commercial software available from SmartBUY sources can be viewed on the website at http://www.gsa.gov/portal/content/105119.

1.9 Government Facilities

No Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided unless detailed in individual task orders.

1.9.1 Government Property and Information

Where Government Property is authorized on a task order, the Contractor shall establish and maintain property management procedures as approved by the Government Property Administrator (PA). Authorization of Government furnished items and services will be provided at the discretion of the Ordering Contracting Officer. Provision of GFI needed to perform work and authorized access will be addressed at the individual TO level.

As defined in FAR Part 45.107 (a)(1)(iii), Government Furnished Property (GFP) is property that will be identified at the task order level. The Contractor shall use Government property in accordance with FAR clauses 52.245-1, and the terms contracted. The Contractor shall implement a Government-approved Property Management Plan to ensure effective and efficient stewardship of Government property when GFP is authorized on the task order.

1.10 Security Requirements

Contractor personnel performing work under this Agreement shall have the appropriate security clearance as specified in each individual task order at time of the proposal submission and shall maintain the level of security required for the life of the task order. Security requirements shall be as specified in the DD Form 254, Department of Defense Contract Security Classification Specification, associated with the task order. All Contractor personnel with access to unclassified information systems, including e-mail, shall have a favorable National Agency Check (NAC).

1.10.1 Visitor Group Security Agreement

The Contractor may be required to sign a Contractor Visitor Group Security Agreement to protect classified information involved in performance under individual task orders. The task order will outline responsibilities in the following areas: Contractor security supervision; Standard Practice Procedures; access, accountability, storage, and transmission of classified material; marking requirements; security education; personnel security clearances; reports; security checks; security guidance; emergency protection; protection of Government resources; DD Forms 254; periodic security reviews; and other responsibilities, as required.

1.10.2 Physical Security

The Contractor shall be responsible for safeguarding all Government equipment, information, and property provided for Contractor use.

1.10.3 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities require Contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The Contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD 5220.22-M (NISPOM) not later than one (1) week prior to visit – timeframes may vary at each facility/ installation.

(b) Depending on the facility/installation regulations, Contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement.

(c) All Contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government and shall report any known or suspected security violations to the Security Department at that location.

1.11 Cybersecurity

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

1.11.1 Cyber Incident Reporting

The Contractor shall comply with all contracted cyber incident response and reporting requirements. Prior to initiating any cyber incident emailed communications or reporting, the Contractor shall obtain instruction from Fleet Cyber Command. Cyber incident response and reporting requirements originate from the following agencies and referenced publications and include, but are not limited to, the following:

- CJCSM 6510-01B Cyber Incident Handling Program
- Cloud Service Provider (CSP) Incident Response Plan (IRP) including amendments and updates issued by 10th Fleet/Fleet Cyber Command or other Government source as approved under this Order
- DoD Cloud Computing Security Requirements Guide
- DoD Cyber Crime Center (DC3) for handling malicious software handling per DFARS 252.204-7012
- DIB-CS required DIB Net reporting detailed in DFARS 252.239-7010
- Federal Information Security Modernization Act of 2002 as amended by Federal Information Security Modernization Act of 2014
- NIST SP 800-61 Computer Incident Handling Guide
- NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- PGI 204-7303-3 Cyber incident and compromise reporting
- PGI 204.7303-4 DoD damage assessment activities
- SECNAVINST 5239.19 DON Computer Network Incident Response and Reporting Requirements

- US-CERT Federal Incident Notification Guidelines

However, in accordance with DFARS 252.204-7012, requirements of other applicable U.S. Government statutory or regulatory requirements, clauses, and terms of this contract are still authoritative and shall be met. IRP amendments / updates approved by 10 Fleet/Fleet Cyber Command or other Government sources may be incorporated into the task order in accordance with the contracted Change process.

The DON Cybersecurity Lead will provide information of DON and DoD notifications such as Computer Tasking Orders CTOs, Operation Orders (OPORDS), Warning Orders (WARORDs), etc. to the Contractor to enable their compliance with the Navy ATO. The Contractor shall report status to the DON Cybersecurity Lead on required notifications for compliance. The Government Cybersecurity Lead will be responsible for managing the Navy's approval process for the Contractor to obtain Navy ATO at the task order level if required and to act as the Contractor's sponsor through the process.

Submission of, and update(s) to, the CSP's Incident Response Plan (IRP) shall comply with requirements of the CSP's DoD Provisional Authorization to Operate and Navy Assessment Office certification. The CSP's IRP shall be updated, and the update maintained current, to reflect the points of contact and requirements of this Agreement and task orders issued thereunder. A copy of the update shall be provided to the respective task order OCO.

The DON Cybersecurity Lead will provide guidance and coordinate with the Contractor's Cybersecurity Lead for information needed to respond to DON and DoD cyber security information requests. The Contractor is required to have a dedicated Cybersecurity Lead to interface with the Government Cybersecurity Lead, ACO, PCO and OCO. Instructions or guidance perceived by the Contractor to be a Change to the task order shall be identified to and authorized by the OCO prior to implementation, in accordance with the contracted Change process.

1.11.2 Cyber IT and Cybersecurity Personnel

(a) The Cyberspace workforce elements addressed include Contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, Contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed Contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract/task order during the course of the performance period.

(b) The Contractor shall identify, track and report cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel.

(c) Contractor personnel that access DON IT shall follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR).

(d) Contractor personnel with privileged access are required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

1.11.3 Integration, Configuration or Installation of Hardware and Software

The Contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements, as specified under DoDI 8500.01. The Contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dated 12 February 2016. Use of blacklisted software is specifically prohibited. Procurement and installation of software governed by the DON Enterprise License Agreements (ELAs) – for example, Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

1.11.4 Cyber Security Training

All Contractor employees shall complete the DoD Cyber Awareness Challenge Training (formerly Information Assurance Awareness Training) before issuance of network access, and annually thereafter. In accordance with DoDD 8570.01, all Contractor personnel supporting Cybersecurity functions shall complete appropriate training within specified timelines and attain and maintain the required Information Technology (IT) and cybersecurity training certifications. The Contractor shall be responsible for verifying applicable personnel receive all required training. The Contractor's designated Security Officer shall track the following information: security clearance information; dates possessing Common Access Cards; issued and expired dates for badges; cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; Cybersecurity Workforce certifications; etc. For classified work, the Contractor shall educate employees on the procedures for the handling and protection of classified material and documents, and other security measures, as described in the task order PWS and in accordance with DoD 5220.22-M.

1.11.5 Disclosure of Information

Disclosure of any information shall be handled in accordance with DFARS clause 252.204-7000.

1.11.6 Handling of Personally Identifiable Information (PII)

When a Contractor is authorized access to Personally Identifiable Information (PII), the Contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act (FAR clauses 52.224-1 and 52.224-2). The Contractor shall safeguard PII from theft, loss, and compromise. The Contractor shall transmit and dispose of PII

in accordance with the latest DON policies. The Contractor shall not store any Government PII on their personal computers. The Contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to Contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the Contractor shall immediately notify the Contracting Officer and COR. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred because of having to notify personnel.

1.12 OPSEC

1.12.1 Local and Internal OPSEC Requirements will be provided in the individual TO

Contractor personnel shall adhere to the OPSEC program policies and practices as cited in the local site OPSEC procedures, to be provided at the task order level. The local site refers to the Contractor's place of performance. The Contractor shall develop their own internal OPSEC program specific to the contract/task order and based on the local site's OPSEC procedures. At a minimum, the Contractor's program shall identify the current Government OPSEC Officer/Coordinator and requirements the local OPSEC procedures.

1.12.2 OPSEC Training

Contractor shall track and ensure Contractor personnel performing contracted work receive initial and annual OPSEC Awareness training. Training may be provided by the Government or the Contractor's OPSEC Manager. Contractor training shall, at a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the contract/task order, and review OPSEC requirements if working at Government facilities. The Contractor shall ensure any training materials developed by the Contractor shall be reviewed by the Government OPSEC Officer, who will ensure it is consistent with DON OPSEC policies. OPSEC training requirements are applicable for Contractor personnel during their entire term supporting the contracted work and shall include workplace requirements applicable to the Contractor or authorized under an individual TO.

1.12.3 OPSEC Program

Contractor shall participate in OPSEC program briefings and working meetings. The Contractor shall complete any required OPSEC survey or data calls within the timeframe specified.

1.12.3.1 Data Handling and User Controls

The Contractor shall handle all data received or generated under this Agreement as For Official Use Only (FOUO) material, in accordance with DoDI 5200.01 and NIST SP 800.171. The Contractor shall handle all classified information received or generated pursuant to the task order DD Form 254 and shall be in compliance with all applicable PWS references and other applicable Government policies and procedures cited herein and in the individual task order.

1.12.3.2 Effective Use of Controls

The Contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD-approved anti-virus software prior to delivery to the Government. The Contractor shall utilize appropriate controls (i.e., firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the Contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication, and non-repudiation. The Contractor shall ensure provisions are in place that will safeguard all aspects of information operations pertaining to this Agreement in compliance with all applicable PWS references. The Contractor shall ensure Data-at-Rest is required on all portable electronic devices used for transfer of data from DON to contractor or CSP facilities including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation.

1.12.4 Anti-Terrorism (AT) Training

All Contractor employees requiring access to DoD installations, facilities, and controlled access areas shall complete AT Level I Awareness training, as required, at the task order level. The Contractor shall submit certificates of completion for each affected Contractor employee to the Task Order COR within 5 calendar days after completion of training by all employees.

1.12.5 Access and General Protection/Security Policy and Procedures

The Contractor shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services, or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DoD, DON, and/or local policy. In addition to the changes otherwise authorized by the "Changes" clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

1.13 Post Award Conference and Periodic Progress Meetings

The Contractor agrees to attend any post award conference convened by the contracting activity in accordance with FAR Subpart 42.5, "Post-Award Orientation." The Contracting Officer, Contracting Officers Representative (COR), and other DON personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings, the Contracting Officer will apprise the Contractor of how the DON views the Contractor's performance, and the Contractor will apprise the DON of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the DON. Meetings pertaining to task order performance will be conducted by the Ordering Contracting Officer on the individual task order level.

1.14 Badges

1.14.1 Corporate Identification

Contractor personnel shall wear and clearly display an identification badge with their full name and corporate affiliation at all times while performing DON-site duties and while at TDY

locations on official business. They must also ensure that all documents or reports produced by Contractor are suitably marked as Contractor products or that Contractor's participation is appropriately disclosed.

1.14.2 Common Access Card (CAC)

Contractor personnel may be required to obtain a CAC, which will provide physical access to facilities or installations in addition to allowing access to the Non-secure Internet Protocol (IP) Router Network (NIPRnet). Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The Contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, Contractor personnel shall be able to meet all of the following security requirements prior to work being performed. Pursuant to DoD Manual (DoDM-1000.13-M-V1), issuance of a CAC is based on the following four criteria:

1. Eligibility for a CAC – To be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the Government on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
2. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS) (formerly Contractor Verification System (CVS)).
3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoD Manual 5200.02 (April 2017) – At a minimum, this requires the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a National Agency Check with Inquiries (NACI) investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. Contractor personnel shall contact the local site's Security Office (to be identified at the task order level) to obtain the latest CAC requirements and procedures.
4. Verification of a claimed identity – All Contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

1.14.3 Contractors That Do Not Require CAC

If the Contractor requires access to a DoD facility or installation, the Contractor shall comply with adjudication standards and procedures using the National Crime Information Center

Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB), and applicable installation, facility and area commander installation/facility access, local security policies, and procedures (provided by Government representative).

1.15 Other Direct Costs

The Other Direct Costs (ODC) category provides an estimate for Travels and an estimate for Materials in terms of the types such as hardware, software, equipment, bonding and quantity required for the Contractor to perform the work expected to be accomplished.

a. **Other Direct Costs for Travels (ODC Travels FFP CLIN 0007, Optional CLINs 1007, 2007, 3007, and 4007)**

Task order-related travel pricing (i.e., temporary duty (TDY) to include travel, lodging and meals) (Firm Fixed Price (FFP)) may be required, and will be specified in the individual task order. All travel requirements (including plans, agenda, itinerary, dates and price) shall be pre-approved by the DON prior to conducting contracted travel (subject to local policy procedures detailed in the task order).

b. **Other Direct Costs for Travels (ODC Travels ODC Travels T&M CLIN 0008, Optional CLINs 1008, 2008, 3008, 4008)**

Task order-related travel costs (i.e., temporary duty (TDY) to include travel, lodging and meals) (Cost Reimbursable ODCs supporting Time-and-Material task orders) may be required, and will be specified in the individual task order. All travel requirements (including plans, agenda, itinerary, dates and NTE cost) shall be shall be pre-approved by the DON prior to conducting contracted travel (subject to local policy procedures detailed in the task order). Travel costs shall be billed in accordance with the regulatory implementation of Public Law 99-234 and FAR 31.205-46, Travel Costs (subject to local policy & procedures). The Contractor will be authorized travel expenses consistent with the substantive provisions of the Federal Travel Regulation (FTR) and the Limitation of Funds specified in this Agreement/task order. All travel costs require prior Government approval/authorization by and notification to the COR. If any travel arrangements cause additional costs to the task order that exceed those previously authorized, written approval by the Ordering Contracting Officer is required, prior to undertaking such travel.

c. **Other Direct Costs for Related Materials (Hardware (SIN 132-8) and non-DOD ESI Software and Software Maintenance under SINs 132-32/33/34) (ODC Materials FFP CLIN 0009, Optional CLINS 1009, 2009, 3009, 4009)**

ODCs for Related Materials consist of IT Solution Equipment, non-DOD ESI IT Solution Software, Incidentals, and Other ODCs necessary in support of an overall task order such that the items are not the primary purpose of the work ordered, but are an integral part of the total solution offered. ODCs under these CLINS are contracted on a FFP basis. Thus, purchases made under the Government Sources of Supply authority are not acquired under the CLIN. The Contractor shall include a detailed description of all proposed ODCs for Materials in individual task order proposals. The cost of general purpose items required for the conduct of

the Contractor's normal business operations will not be considered an allowable ODC in the performance of this Agreement or task orders issued thereunder.

d. **Other Direct Costs for Related Materials (Hardware (SIN 132-8) and non-DOD ESI Software and Software Maintenance under SINs 132-32/33/34 and Items Acquired from Government Sources of Supply) (ODC Materials T&M CLIN 0010, Optional CLINS 1010, 2010, 3010, 4010)**

ODCs for Related Materials consist of IT Solution Equipment, non-DOD ESI IT Solution Software, Incidentals, and Other ODCs from Government Sources of Supply necessary in support of an overall task order such that the items are not the primary purpose of the work ordered, but are an integral part of the total solution offered. They are reimbursable at cost under the Time and Materials CLIN. Purchases from Government Sources of Supply will be reimbursed at cost not-to-exceed the amount reflected in the Supplier's Government contract. The Contractor shall include a detailed description of all proposed ODCs for Materials in individual task order proposals. The cost of general purpose items required for the conduct of the Contractor's normal business operations will not be considered an allowable ODC in the performance of this Agreement or task orders issued thereunder.

1.16 Quality Controls

The Contractor shall perform all quality control inspections necessary in the performance as identified by the individual task orders. The Government reserves the right to, at a minimum, inspect or request data samples to assure that the Contractor provided services, documents, material, data, artifacts, logs and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

1.17 Electronic Format

At a minimum, the Contractor shall provide deliverables electronically by email; hard copies are only required if requested by the Government. To ensure information compatibility, the Contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, etc., are provided in a format approved by the receiving Government representative. The Contractor shall provide all data in an editable format

1.18 Information

1.18.1 Electronic Communication

The Contractor shall be capable of Public Key Infrastructure client-side authentication to DoD private web servers. Unless otherwise specified, all key personnel on contract shall be accessible by email through individual accounts during all working hours. Key personnel, if required, will be specified at the task order level.

1.18.2 Information Security

Pursuant to DoDM 5200.01, the Contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information systems. The Contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear

expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the Contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

1.18.3 Safeguards

The Contractor shall:

(a) Protect Government information.
(b) Comply with DFARS clause 252.204-7012.
(c) Not process DoD information on public computers or computers that do not have access control.
(d) Protect information by at least one physical or electronic barrier when not under direct individual control.
(e) Sanitize media before external release or disposal.
(f) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DoD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage."
(g) Ensure all solutions meet FIPS 140-2 compliance requirements.
(h) Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.
(i) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment.
(j) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.
(k) Do not post DoD information to website pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).
(l) Provide protection against computer network intrusions and data exfiltration, minimally including the following:
(m) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
(n) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.
(o) Prompt application of security-relevant software patches, service packs, and hot fixes.

(p) As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).
(q) Report loss or unauthorized disclosure of information in accordance with the Agreement.

1.18.4 Compliance

Pursuant to DoDM 5200.01, the Contractor shall include in its quality processes procedures that are compliant with information security requirements.

1.19 Industrial Funding Fee (IFF) (CLIN 0014; Optional CLIN 1014, 2014, 3014, 4014)

The IFF is a quarterly contract management fee which must be paid back to GSA by the Contractor. The IFF equals 0.75% of sales made and it supports the GSA branch that negotiates all GSA Schedules.

The Contractor remits the IFF back to the GSA on either a quarterly or monthly basis (in accordance with the Contractor's Schedule 70 contract). The fees are based on actual sales for the quarter or month. The IFF is 0.75% of the unit price of each line item, service or labor category. Regardless of task order type, the Agreement holder and TO Contractor must include the IFF in their proposed pricing.

2. Specific Requirements/Tasks

The Contractor shall offer the following types of service offerings in accordance with FedRAMP and DoD PA approved CSPs, CSOs, and service items available on the Agreement Holder's GSA Schedule:

2.1 Infrastructure as a Service (IaaS) – Reference SIN 132-40 (CLIN 0001, Optional CLINs 1001, 2001, 3001, 4001)

IaaS is the capability provided to the consumer for provisioning processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The Contractor shall deliver IaaS services as specified in the task order.

2.2 Platform as a Service (PaaS) – Reference SIN 132-40 (CLIN 0002, Optional CLINs 1002, 2002, 3002, 4002)

PaaS is the capability provided to the consumer for deployment of consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider into the cloud infrastructure. The Contractor shall deliver PaaS services as specified in the task order.

2.3 Software as a Service (SaaS) - Reference SIN 132-40 (CLIN 0003, Optional CLINs 1003, 2003, 3003, 4003)

SaaS is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a

thin client interface, such as a web browser (e.g., web-based e-mail) or a program interface. The Contractor shall deliver SaaS services as specified in the task order level.

2.4 Other Commercially Available Cloud Service Offerings

As additional cloud service offerings receive DoD PAs, the Contractor shall notify the Contracting Officer for inclusion into the contract by contract modification. This requires that services are available for order on the underlying GSA Schedule 70 SINS and added to the BPA prior to services being available for ordering.

2.5 The Contract shall deliver Commercial Cloud Services that include the following:

(a) Capability for consumers to provision on-demand self-service computing capabilities, such as server time and network storage, as needed, without requiring human interaction with each service provider.
(b) Capabilities available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
(c) Resource pooling of computing resources to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
(d) Rapid elasticity, to automatically scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.
(e) Measured service that leverage a metering capability to automatically control and optimize resource use. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

An exception to the above requirements is permitted for unique instances supporting DoD cloud service delivery that have been granted DoD PATO Information IL5.

2.6 Professional Services (FFP CLIN 0004, Optional CLINs 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINs 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINs 1006, 2006, 3006, 4006)

The Contractor shall deliver professional services such as development and testing, risk and vulnerability assessment (SIN 132-45D), operating system security assessment, penetration testing (SIN 132-45A), incident response (SIN 132-45B), cyber hunt services (SIN 132-45C) and customer assistance in identifying services necessary for migrating applications to the cloud environment, managed services, other professional services (SIN 132-51). Such services will be specified at the task order level.

Managed services entail the implementation of best practices and tools to reduce operational risk. Common activities include, but are not limited to change management, monitoring through the use of HBSS, ACASS, AD and other tools and procedures, patching, updating, and security and backup and automating routine processes. Managed services shall comply with the DoD Cloud Computing SRG and DoD RMF security requirements.

2.7 Technical Areas (FFP CLIN 0004, Optional CLINs 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINs 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINs 1006, 2006, 3006, 4006)

Cloud-based services that are to be delivered include, but are not limited to the following technical areas:

2.7.1 Network Normalization

The Contractor shall provide Network Normalization. DON's current system of disparate network, processing, and storage infrastructures impedes internal and external collaboration for the warfighter and mission partners. As such, a foundational aspect of achieving the Joint Information Environment (JIE) is to provide a single, protected information environment that securely, reliably, and seamlessly interconnects users.

2.7.2 Identity and Access Management

The Contractor shall provide Identity and Access Management. Optimized Global Identification, Authentication, Access Control, and Directory Services are central to satisfying the need for a portable identity and the ability to share contact information between organizations.

2.7.3 Enterprise Services

The Contractor shall provide Enterprise Services. An enterprise service is a service that is federated and is provided by a single organization acting as the enterprise-service provider. DON is emphasizing development and deployment of enterprise services as part of JIE that are designed to operate in deployed, disconnected, or low-bandwidth information environments.

2.7.4 Storage Services

The Contractor shall provide short and long-term Cloud Based Storage Services in support of DON applications, Continuity of Operations, Disaster Recovery, and customer data storage.

2.7.5 Secure File Transfer Services

The Contractor shall provide an enterprise-wide capability to securely transfer files of any size and type to either internal or external Government and Contractor DON network users.

2.7.6 Virtual Machine Services

The Contractor shall provide Cloud Based Virtual Machine Services in support of application Transition Support and New Application Implementation Requirements to include Virtual Machine Migration and Consolidation.

2.7.7 Database Hosting Services

The Contractor shall provide Cloud-based Database Hosting Services, which includes stand-alone databases, shared data sources, or tiered database solutions including components of detailed technical areas.

2.7.8 Web Hosting Services

The Contractor shall provide Cloud Based Web Hosting Services in public, private, community, and hybrid cloud environments. This includes any combination of other Technical Areas

necessary to deliver static and/or dynamic information to the DON stakeholders and hosting for an enterprise-wide content management system.

2.7.9 Development and Test Environment Hosting Services

The Contractor shall provide a flexible, scalable, on-demand environment to support development, testing, staging, and/or quality assurance before releasing new applications and changes into the Navy production environment.

2.7.10 Training (SIN 132-50) (FFP CLIN 0004, Optional CLINs 1004, 2004, 3004, 4004; T&M CLIN 0005, Optional CLINs 1005, 2005, 3005, 4005; and LH CLIN 0006, Optional CLINs 1006, 2006, 3006, 4006)

Training will be defined at the task order level and may include use of Contractor web-based consoles and portals, provisioning, usage, billing, reporting, alerts, tagging, and other commercial training offerings related to commercial cloud services provided under the Agreement.

3. Agreement Data Deliverable (Task Order Level CLIN 0011, Optional CLINs 1011, 2011, 3011, 4011; Agreement Level CLIN 0012, Optional CLINs 1012, 2012, 3012, 4012)

CDRL requirement has been identified for the Agreement, and additional CDRLs will also be included in individual task orders, as required.

CDRL #	Deliverable	Frequency
A001	Monthly Agreement Status Report (MASR)—Summary of significant activities, problems, developments and progress	Due 45 days after Agreement award for initial report. Subsequent ones are due on the 15th of each month after the end of the prior month.
A0002	Order Summarization – Services Delivered and Orders Received	Due 45 days after Agreement award for initial report. Subsequent ones are due on the 15th of each month after the end of the prior month.

4. Meetings

Required meeting conduct, coordination, and attendance will be required in support of the Agreement as detailed in paragraphs 1.13 above and 6.1 below. Additionally, meeting requirements will be as detailed in the individual task orders.

5. Non-Personal Services

The DON will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the Contractor

believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the Ordering Contracting Officer immediately.

6. Special Instructions

6.1 Agreement Management

The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. All Navy cloud services must be brokered through a Managed Service Organization (MSO), also referred to as the "Cloud Broker." Program Executive Office for Enterprise Information Systems (PEO EIS) is the Navy Enterprise Cloud Broker (NECB) Executive Agent. The Contractor shall provide expertise to accomplish program planning and control of activities required to meet the requirements of the contract. During the life of the Agreement, periodic meetings will be held at both Contractor and Government sites. Participation in periodic meetings and conferences shall be at no additional cost to the Government.

6.2 Contractor Personnel, Disciplines, and Specialties

The Contractor shall employ, for the purpose of performing that portion of the work in the State of Hawaii, individuals who are residents thereof, and who, in the case of any craft or trade, possess or would be able to acquire promptly the necessary skills to perform the Agreement. The Contractor shall insert the substance of this clause, including this paragraph (6.3), in each subcontract or teaming partner arrangement supporting performance of the Agreement and any awarded task orders.

6.2.1 Conduct of Contractor Personnel

If the PCO or OCO finds it to be in the best interest of the DON, the PCO or OCO may at any time during the performance of this Agreement or task order request the Contractor to consider Government performance, safety, health or other concerns with contracted service delivery and to take necessary corrective action. In the event that it becomes necessary to replace any Contractor personnel for any of the above reasons, the Contractor shall bear all costs associated with such removal, including the costs for the replacement of any personnel so removed. The Contractor or Contractor personnel shall be responsible for the return of all logistical support items (i.e., ID cards, ration cards, POV tags and registration, POV and GOV operator's licenses, etc.) prior to departure from area of operation.

6.2.2 Notice of Internet Posting of Awards

It is the DON's intent that the Agreement holder will electronically post the Commercial Cloud Service Agreement and any modifications to the Agreement, as well as the Agreement Ordering Guide to their website to facilitate requirement planning and order placement. This does not include Agreement holder proposals or any other proprietary information provided by Agreement holder relevant to performance of this Agreement. Accordingly, the Agreement holder shall provide any necessary redaction of award documents within 5 working days following execution to permit posting of applicable information to their website.

7. DON Enterprise Control Standards (ECS) and Support Controls

Only the standards applicable to the hosted systems apply (applicability will be determined by the Government system owner). At the time that a financially relevant system is authorized under the Agreement or task order, the Contractor shall provide services that comply with the below requirements:

(a) The Contractor shall comply with DON ECS. Copies of the DON ECS can be found at:
(b) https://portal.secnav.navy.mil/orgs/FMC/FMP/FMP-1/FMP-10/SitePages/Home.aspx (access to this site is CAC controlled and requires registration).
(c) The Contractor shall comply with Support Controls described in the Government Accountability Office (GAO) Federal Information System Control Audit Manual (FISCAM); a copy of the FISCAM manual can be found at: http://www.gao.gov/fiscam/overview.

8. System Compliance with DoDI Risk Management Framework (RMF)

At the time that a financially relevant system is authorized under the Agreement or task order, the Contractor shall provide services that comply with the below requirements:

(a) System Compliance with DoDI Risk Management Framework (RMF) for DoD IT Applicable to systems deemed financially relevant by the DON. The Contractor shall ensure systems are in compliance with DoDI 8510.01, Department of Defense Instruction Risk Management Framework (RMF) for DoD Information Technology (IT).
(b) Security Requirements for Federal Information Technology Resources Applicable to systems deemed financially relevant by the Navy. Any equitable adjustment for Contractor compliance with tasks under this paragraph will be accomplished at the task order level for the particular financially relevant tasking being audited.
(c) Financial Statement Audit (FSA) support by the Contractor for audit of systems deemed financially relevant by the Navy. The Contractor shall support needed interaction with DON Financial Statement (FS) auditors, respond to queries, and implement requested corrective action(s). Audits are conducted annually and necessitate timely, complete response, temporary provision of on-site work space for audit personnel, and provision of personnel resources similar to the commitment required for other commercial audits experienced by the Contractor. Contractor support includes but is not limited to:
    1. Identify the Contractor's point of contact authorized to speak for the company and facilitate Navy performance of a financial system audit.
    2. Participate in interviews with the FS auditor.
    3. Participate in interviews with the DON FSA FMP support team.
    4. Conduct IT control walkthroughs of relevant business operations and process, and respond to auditor observations.
    5. Respond to auditor documentation requests (e.g., Provided by Client) lists, to include key supporting documents and other information as required by reporting entities' auditors. Any document prepared by the Contractor in response to an auditor's request shall be marked as draft and be submitted to the COR for their finalization and their response to the auditor.

6. Engage in reporting entity updates and communications with Independent Public Accounting firms.
7. Establish communication protocols and processes for receiving, tracking, and responding to auditor requests with the audit team.
8. Define escalation procedures with the audit team for instances when responses to auditor requests have not been provided or are delayed.
9. Respond to auditor's IT Notice of Finding and Recommendation (NFR). Any document prepared by the Contractor in response to an auditor's request shall be marked as draft and be submitted to the COR for their finalization and their response to the auditor.
10. Provide an IT Corrective Action Plan (CAP) to remediate findings and implement recommendations.

(d) FM Overlay Implementation. The Contractor shall support DON's FM overlay process as an enhancement to their Risk Management transition and Assessment and Authorization (A&A) efforts. The FM overlay controls are IT controls that are FSA centric and are required in addition to the controls that are base lined in RMF A&A efforts. Required security and management controls for the financially relevant system will be identified and funded to enable Contractor implementation at the time the system is contracted on individual task order.

(e) Third Party Assurance. The Contractor shall provide the DON assurances that cloud service provider relationships are being monitored and documented. A combination of attestation products may be provided to satisfy third party relationships between the DON and their Contractor's cloud service provider; attestation products include SSAE-18 SOC1 report.

(f) Contractor Hosting Center and DON IT Control Responsibilities. The Navy customer will identify the IT controls applicable to the financially relevant system to be implemented by the Contractor as part of the OCO's authorization to commence system hosting services. Specific Navy and Contractor responsibilities pertaining to the financially relevant system will be documented and agreed upon as part of OCO authorization for hosting. Additionally, the Contractor shall implement the IT controls for the contracted hosting center and the DON users (end user, administrators) as detailed in the PWS and task order pertaining to access controls, segregation of duties, configuration management, contingency planning, security management, audit logging, incident response, identification and authentication, business process controls and interface controls.

(g) Upon DON notification that a Navy Financial System Audit is to be performed, and the Contractor perceives that delivery of audit support creates entitlement to a price, schedule or technical revision, the Contractor shall notify the Ordering Contracting Officer of the impacts of the change in accordance with the Changes clause of the contract. Contractor implementation of the Changes shall follow OCO instruction and issuance of a task order modification, as necessary.

(h) Compliance with Section 508 of the Rehabilitation Act of 1973; Clinger-Cohen Act of 1996, also known as the "Information Technology Management Reform Act of 1996," is required as detailed in individual orders issued. Information about Section 508 is available at http://www.section508.gov/.

(i) The Contractor shall submit a close out plan, if required by the individual task order, for the movement of accounts out of the Hosting Environment, return of backups to the Customer, transfer of accounts, and disposal of electronic data, at the end of the task order.

9. Close Out (CLIN 0013, Optional CLINs 1013, 2013, 3013, 4013)

The Contractor shall support the smooth migration of applications out of the Hosting Environment, return of backups to the Customer, transfer of accounts, and ensure proper disposal of electronic data. Once an application(s) has been migrated out of the Hosting Environment, the Contractor shall ensure all Government Electronic Data is properly destroyed and not released.

Close out may be directed upon identification of any of the following noted circumstances:
(a) Contract Close Out
(b) Account Close Out

At any time during the period of performance or in the final year of the task order, the Contractor shall:
(a) Follow the Account Close Out guidance for all accounts;
(b) Return all requested data and backups to the customer; and allow full access to accounts hosting environment while systems are being migrated out;
(c) Return all Common Access Cards (CAC) to the COR, and uninstall Government Furnished Software, and return any license key, media and documentation to the COR or their delegate, and notify COR when accomplished;
(d) Ensure all electronic Data is destroyed and not released; and
(e) Residual data and account information must be deleted in accordance with NIST-800-88, Rev 1 requirements.

The Contractor shall work with the Navy to ensure all programmatic support and service management services are transitioned to the Navy or its identified agent. This is essential for a seamless and successful transition, in order for the Navy to preserve full functionality and minimize downtime during the transition.

Account Close Out is defined as the Transition/Transfer of a CSP account to another Reseller/CSP or Termination of the CSP services and account as follows:
(a) Transition/Transfer of the CSP account - The Contractor shall ensure a seamless, disruption-free close out of CSP Accounts, when directed by OCO. The Contractor shall implement the Contractor defined process which has been previously approved for account transition, as applicable to the task order.
(b) Termination of the CSP account - Should the decision be made by the customer to terminate the CSP account vice transferring the account to another CSP, the requiring activity will ensure all services are properly terminated and all data is wiped in accordance with current NISPOM guidance.

Account Close out will be directed by the OCO on a per account basis upon identification of any of the following noted circumstances:
(a) Customer account transfer or termination of Cloud Service provider(s).
(b) Customer account transfer, modification, or termination of Cloud Service agreements and/or workloads in part or in whole.
(c) Customer requested termination of Cloud Service.
(d) Termination of relationship with current contract partners/sub-Contractor agreements/workloads.
(e) Termination of relationship with current contract partners/sub-Contractor agreements/workloads as a result of the dissolution of the business / end of business operations.

In the event of Account Close Out, the Contractor shall:
(a) Follow the Account Close Out guidance for accounts applicable to the task order,
(b) Return all requested data and backups to the customer;
(c) Allow full access to accounts hosting environment while systems are being migrated out;
(d) Ensure all electronic Data is destroyed and not released;
(e) Residual data and account information must be deleted in conjunction with NIST-800-88, Rev 1 requirements; and

10. Safety Issues

10.1 Occupational Safety and Health Requirements

The Contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The Contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the respective task orders under this Agreement. Without Government assistance, the Contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system.

10.1.1 Performance at Government Facilities

The Contractor shall immediately report any accidents involving Government or Contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the Contractor is responsible for securing the scene and impounding evidence/wreckage until released by the Contracting Officer.

11. Letter of Authorization

Some travel will require a Letter of Authorization (LOA). A LOA is necessary to enable a Contractor employee to process through a deployment processing center; to travel to, from, and within a theater of operations; and to identify any additional authorizations and privileges. Applicable to the task order, the Contractor shall initiate a LOA for each prospective traveler.

The Contractor shall use the Synchronized Pre-deployment & Operational Tracker (SPOT) web-based system, at https://spot.dmdc.mil/ to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary, and if in the Government's interest, the Contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed/approved by the SPOT registered Contracting/Ordering Officer for the applicable Agreement/task order.

Logistics Support Privileges to be provided by the Government shall be as established in individual task orders

12. COR Designation

The Contracting Officer Representative (COR) for this Agreement is Steven E. Foster who can be reached at phone (858) 537-0491; e-mail: steven.foster@navy.mil.

13. Acceptance Plan

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables under the basic Agreement. Similarly, inspection and acceptance on task orders is performed by the COR assigned to the individual task order. Modification of Agreement requirements through the CDRL submittal and approval process is not permitted.

14. Non-Disclosure Agreement (NDA) Requirements

The Contractor shall provide corporate NDA prior to award, and employee NDAs upon award and over the Agreement life as workforce changes occur. NDA templates are attached. Similarly, corporate and employee NDA submissions will also be requested by the OCOs at the individual task order level for task order specific support.

15. Funding Allocation (required if utilizing Multiple Funding CLINs, at the task order level)

Task orders issued under this Agreement may be funded with multiple appropriations with various Accounting Classification Reference Numbers (ACRNs) which may or may not cross multiple Agreement performance years. Depending on the services performed and the applicable timeframe, the Contractor shall invoice cost in accordance with Section B, Section C, and Section G of the task order award. The ability of the Contractor to perform adequate billing and accounting will be reflected in the Contractor's annual Government Contractor Performance Assessment Report (CPAR) rating.

Appendix A. Acronyms

Acronym	Definition
ACO	Administrative Contracting Officer
BPA	Blanket Purchase Agreement
CAC	Common Access Card
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COMSEC	Communications Security
CM	Configuration Management
CND	Computer Network Defense
CNSS	Committee on National Security Systems
COR	Contracting Officer Representative
CSIRT	Computer Security Incident Response Team
DBMS	Database Management System
DD254	Department of Defense Form 254 (DoD Contract Security Classification Specification)
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoD ESI	Department of Defense Enterprise Software Initiative
DoDIIS	Department of Defense Intelligence Information Systems
DON	Department of Navy
DT&E	Development, Test, & Evaluation
FAR	Federal Acquisition Regulation
FTR	Federal Travel Regulation
FFP	Firm-Fixed-Price
FTP	File Transfer Protocol
GAO	Government Accountability Office

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Acronym	Definition
GSA PCO	General Services Administration Procuring Officer
HIPAA	Health Insurance Portability and Accountability Act 1996
IA	Information Assurance
INFOSEC	Information Security
IT	Information Technology
IV&V	Independent Verification and Validation
JIE	Joint Information Environment
LAN	Local Area Network
MSO	Managed Service Organization
NAC	National Agency Check
NACLC	National Agency Check with Local Agency Checks and Credit Check
NCB	Navy Cloud Broker
NEDC	Navy Enterprise Cloud Broker
NMCARS	Navy Marine Corps Acquisition Regulation Supplement
OCI	Organizational Conflict of Interest
OCO	Ordering Contract Officer
OCOR	Order Contracting Officer's Representative
ODCs	Other Direct Costs
OMB	Office of Management and Budget
PCO	Procuring Contracting Officer
POC	Point of Contact
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF NAVY (DON) COMMERCIAL CLOUD SERVICES

Acronym	Definition
QCP	Quality Control Program
SA	System Architect
SCI	Sensitive Compartmented Information
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TDY	Temporary Duty
T&M	Time and Materials
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network