(U) Intelligence Community (IC) Commercial Cloud Enterprise (C2E)

(U) Attachment J-1
(U) Cloud Service Provider (CSP) Statement of Work (SOW)

Version 1.1
03 February 2020

21 # Change Log

22

Version	Date	Pages Affected	Comments
1.0	09/23/2019	Initial Draft	Initial version for review and comment by industry.
1.1	02/03/2020	Revised Draft	Updated content and SOO to SOW format for draft RFP review.

23

(U) Contents

1.0 (U) Introduction 1

1.1 (U) Portfolio Vision 2

1.2 (U) Objectives & Values 3

1.3 (U) Contractual Assumptions 3

2.0 (U) Scope 4

3.0 (U) Applicable Documents 6

4.0 (U) Requirements 6

4.1 (U) System Requirements 6

4.1.1 (U) Security First 7
4.1.2 (U) Global Reach 8
4.1.3 (U) Innovation and Technical Parity 8
4.1.4 (U) Operational Excellence 8

4.2 (U) Contract Management 9

4.2.1 (U) Program Management Office (PMO) Support 9
4.2.2 (U) Professional Technical Support Services 10
4.2.3 (U) Personnel Security 10
4.2.4 (U) Physical Security 12
4.2.5 (U) Technical Documentation 13
4.2.6 (U) Supply Chain Risk Management (SCRM) 13
4.2.7 (U) Service Usage, Price Information, and Billing Management 15

4.3 (U) Contract Characteristics 16

4.3.1 (U) Contract Type 16
4.3.2 (U) Period of Performance 16
4.3.3 (U) Place of Performance 16
4.3.4 (U) Contract Security 16
4.3.5 (U) Transition from Existing Cloud-Based Contracts to C2E 16
4.3.6 (U) Contract Lifecycle Transition 16
4.3.7 (U) Government Furnished Property, Facilities, Services, and Information (GFX) 16

5.0 (U) Attachments and Appendices 17

APPENDIX A – (U) FedRAMP Authorized and FedRAMP+ Augmented Clouds 18

APPENDIX B – (U) C2E CSP Definitions 20

APPENDIX C – (U) Acronyms List 28

APPENDIX D – (U) Contract Data Requirements List (CDRL) 30

APPENDIX E – (U) CSP Ascension Strategy & Open Season 31

1.0 (U) Introduction

(U) In 2013, the Central Intelligence Agency (CIA) (hereafter referred to as Executive Agent) awarded the Commercial Cloud Services (C2S) contract to acquire cloud computing services provided by a large-scale commercial vendor to the Intelligence Community (IC), at up to and including the TOP SECRET (TS)/Sensitive Compartmented Information (SCI) security level. C2S and IC-GovCloud provided two options for cloud computing support under the Intelligence Community Information Technology Enterprise (IC ITE) initiative. Since that time, cloud computing has proven to be transformational for IC consumers, increasing the speed at which new applications can be developed to support mission and improving the functionality and security of those applications. In response to mission demand since 2013, the IC's portfolio of commercial cloud services has expanded by adding new services from the commercial domain, increasing compute and storage capacity, and acquiring services from multiple commercial vendors.

(U) In 2018, the IC Chief Information Officer (CIO) confirmed the objective of cloud diversity under Epoch 2 of IC ITE and confirmed the CIA as the Executive Agent to conduct the follow-on procurement for enterprise commercial cloud services on behalf of the IC. Commercial Cloud Enterprise (C2E) is the name of the portfolio of acquisitions that includes the follow-on contract as part of Epoch 2 of IC ITE to evolve and enhance the capabilities delivered by C2S. CIA will also have the responsibility to manage the transition from C2S to C2E to ensure mission operations continue to execute at full capacity during the transition period. All named intelligence elements[1] contained within Executive Order (E.O.) 12333 shall have access to C2E contract vehicles. Additionally, other U.S. Government, contractor, and Federally Funded Research and Development Center (FFRDC) elements may gain access to C2E upon approval from the Executive Agent and/or sponsoring IC agency.

(U) The C2E Portfolio consists of the following acquisitions:

- (U) Cloud Service Provider (CSP) acquisition: A multiple-award Indefinite-Delivery Indefinite-Quantity (IDIQ) contract for professional services and foundational cloud services, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). For this acquisition, "CSP" will be used in lieu of "Contractor."
- (U) Cloud Integrator/Multi-cloud Management (CIMM) acquisition: Cloud integration support and tools for multi-cloud management to support the foundational cloud services acquired in the CSP acquisition.

(U) The C2E Portfolio will build on the foundation established by the Commercial Cloud Services (C2S) Program by:

- (U) Evolving to a multi-cloud ecosystem on the TOP SECRET (TS), SECRET (S), and U networks that provides the advantages offered through cloud technology and expands on the essential characteristics by leveraging heterogeneous cloud architectures. Multi-

[1] (U) E.O. 12333 includes the following intelligence elements: CIA, Office of the Director of National Intelligence (ODNI), Defense Intelligence Agency (DIA), the Office of Intelligence and Analysis of the Department of Homeland Security (DHS), the Office of Intelligence and Counterintelligence of the Department of Energy (DOE), the Bureau of Intelligence and Research of the Department of State, the Office of Intelligence and Analysis of the Department of the Department of the Treasury, the intelligence elements of the Federal Bureau of Investigation (FBI), the Office of National Security Intelligence of the Drug Enforcement Administration (DEA), National Security Agency (NSA), National Reconnaissance Office (NRO), National Geospatial-Intelligence Agency (NGA), the other offices within the Department of Defense (DoD) for the collection of specialized national foreign intelligence through reconnaissance programs, and the Intelligence and Counterintelligence Elements of Army, Coast Guard, Air Force, Navy, and Marine Corps.

cloud architectures allow cloud services to be selected based on development strategy and project objectives. In a multi-cloud ecosystem, the Government will gain advantages from use of each CSP's unique area of investment in technology, cybersecurity strategy, and best practices.

- (U) Diversifying cloud services offerings to promote competition and to capitalize on commercial investment and innovation
- (U) Continuing the focus on security and insider threat best practices and the integration of cybersecurity technology
- (U) Extending the reach of cloud services to disconnected and low-bandwidth environments

(U) This SOW describes the overarching vision for the C2E Portfolio and specifically defines the scope, requirements, and values associated for the CSP acquisition only. The intent is to provide the maximum flexibility for vendors to develop public, private, and community cloud solutions to meet the IC's requirements.

1.1 (U) Portfolio Vision

(U) In accordance with the Intelligence Community's Strategic Plan to Advance Cloud Computing, published on 26 June 2019, the IC requires an integrated, interoperable cloud ecosystem that promotes mission success through reliable, available, dynamic, and innovative information technology (IT) services with secure access to functions, capabilities, and data anywhere, anytime, and under all conditions. Based on the IC strategic plan, the IC will leverage Government and multiple commercial cloud capabilities that are interoperable and support workflows within and across multiple security fabrics. The goal is to maximize rapid re-use of data and sharing of data in mission systems to support these capabilities.

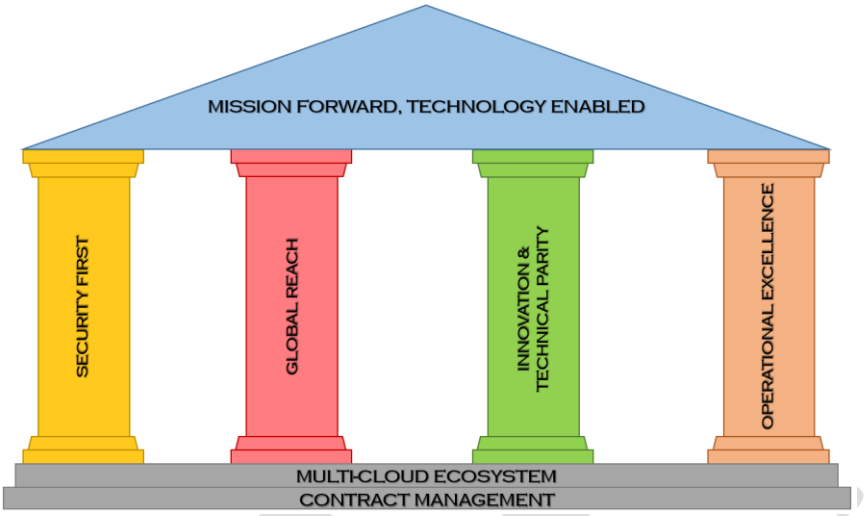
(U) As supported in the Strategic Plan to Advance Cloud Computing, the IC's cloud capabilities will support a diverse set of consumers including disconnected or edge operations. These capabilities will provide innovative and contemporary technologies such as artificial intelligence (AI), machine learning (ML), and high-performance computing to meet current and future needs. These capabilities require unified security processes and acceptance that enable quick adoption and portability of applications, data, and code. The IC will leverage these capabilities in an approach that favors vendor flexibility, simplifies use and adoption of new and cloud-native technologies, and promotes necessary culture changes.

(U) The C2E CSP IDIQ and subsequent task orders will deliver cloud capabilities that achieve an integrated, interoperable, and secure multi-cloud ecosystem that promotes mission success and allows for IC components to execute their mission any time and from anywhere. This vision will be achieved through the full and complete exploitation of secure, reliable, dynamic, and innovative IT cloud service offerings leveraging multi-cloud technology. The CIMM acquisition will provide the implementation support for IC agencies to effectively leverage and optimize the multi-cloud technology; actualizing the vision.

(U) In a multi-cloud ecosystem, the Executive Agent anticipates innovative, cutting edge C2E CSP service offerings to be in high demand by IC mission components; therefore, planning by the Executive Agent and IC elements is underway to establish a security authorization and assessment model that is distributed across IC elements, and based on a set of common standards and policies to ensure consistency in the IC's security implementation of new cloud service offerings. Once this new model is defined and implemented, the Executive Agent will designate the IC Agency that will serve as each CSP's authorizing official during the post-award security assessment phase.

1.2 (U) Objectives & Values

(U) The C2E CSP requirements are organized into four objectives the IC considers as its pillars to overall success as it relates to cloud computing. As shown in Figure 1 below, these objectives include: Security First, Global Reach, Innovation and Technical Parity, and Operational Excellence (refer to the C2E SRD for fabric applicability).



(U) Figure 1 - C2E Objectives

(U) Each objective is accompanied by core values. In the context of this document, a value is a functional area (e.g., Access Control, Global Presence, Integration, Interoperability, Portability, and Continuity of Operations) that is fundamental to meeting IC requirements and technical requirements detailed within Attachment J-2, C2E CSP SRD. The Executive Agent and IC elements particularly value technical requirements associated to cloud maturity and technical agility.

(U) Cloud maturity is defined as the ability to hyperscale, public IaaS with worldwide distribution of IaaS, PaaS, and SaaS offerings, and is supported by technical requirements found throughout the Security First, Global Reach, and Operational Excellence objectives.

(U)Technical agility is defined as the ability to continuously innovate new cloud capabilities based on customer needs and industry trends, and to support the continued adoption of IaaS, PaaS, and SaaS offerings, and is supported by technical requirements found throughout the Security First, Global Reach, and Innovation and Technical Parity objectives.

1.3 (U) Contractual Assumptions

- (U) CSPs will collaborate with the Executive Agent and/or sponsoring IC agency.
- (U//FOUO) CSPs will partner with the Government to mature the security and insider threat processes and capabilities to enable technical parity of new services and the development and maintenance of existing services across all fabrics. Decisions regarding the Assessment and Authorization (A&A) of technology and services shall be prioritized at the discretion of the Executive Agent, or Executive Agent's Designee based on mission need, completeness and quality of documentation, quality of implementation, consumer demand, and the CSPs' available personnel for service evaluation, deployment, and maintenance.

- (U//FOUO) CSPs will develop and carry out a shared insider threat program in partnership with and under the oversight of the Executive Agent, or Executive Agent's Designee with the understanding that some elements of this program may be exclusive to the Executive Agent, and some elements may be exclusive to the CSP. As appropriate based on the fabric, this program will include participation in an information-sharing and incident response consortium to aid the Government in meeting its insider threat monitoring responsibilities for activity on both the user and CSP administrative planes.
- (U) CSPs will provide cleared technical support and development resources who are familiar with the unique security processes and constraints of all IC elements defined in E.O. 12333 (refer to Section 1.0 of the SOW).
- (U//FOUO) CSPs will coordinate with the Executive Agent and IC elements, as needed, on the building of the network and data centers. The Executive Agent may provide Government-owned property (GFP), facilities (GFF), services (GFS), and information (GFI) and will require an Operational Security (OPSEC) plan.
- (U) CSPs will partner and communicate with the Government to share and incorporate best practices and technical strategies, to include but not limited to approaches to security, vulnerability detection, insider threat, data protection, and resource optimization and management.

2.0 (U) Scope

(U) The C2E CSP contract scope includes the following:

- **(U) Service Types and Fabrics:**
  - **(U) Service types:** Provide all types of cloud services (IaaS, PaaS, and SaaS) and associated professional support services for the following fabrics below.
  - **(U) Cloud Solutions across Fabrics:** The CSP shall provide a variety of cloud capabilities to meet information technology needs for Government development, processing, and storage across the fabrics. The C2E CSP IDIQ and associated task orders will acquire clouds on the UNCLASSIFIED (U), SECRET (S), and TOP SECRET (TS) fabrics. Within this document, the C2E environment encompasses clouds on the U, S, and TS fabrics.

    (U) On the U fabric, as the "C2E Commercial Environment," the CSP shall deliver commercial offerings, to be provided in both a COTS cloud offering and a cloud services offering authorized through the Federal Risk and Authorization Management Program (FedRAMP).

    (U) The "C2E Regulated Environment" includes three implementations: a FedRAMP+ Augmented cloud on the U fabric, as well as clouds on the S and TS fabrics. The cloud on the U fabric that is part of the C2E regulated environment will be a more restricted cloud that builds on the FedRAMP authorization with additional controls, and will be known as the FedRAMP+ Augmented Cloud.

    (U) Figure 2 below provides an overview of the C2E Commercial and Regulated Environments, including the corresponding Contract Line Item Number (CLIN) assigned across the C2E Environment. CLIN 0002 will support the C2E Commercial

Environment, which includes the Commercial Cloud and FedRAMP Authorized Cloud on the U fabric. CLIN 0003 will support the FedRAMP+ Augmented Cloud(s) for Controlled Unclassified Information (CUI) within the C2E Regulated Environment. CLINs 0004 and 0005 will support the SECRET Cloud and TOP SECRET/SCI Cloud respectively within the C2E Regulated Environment.

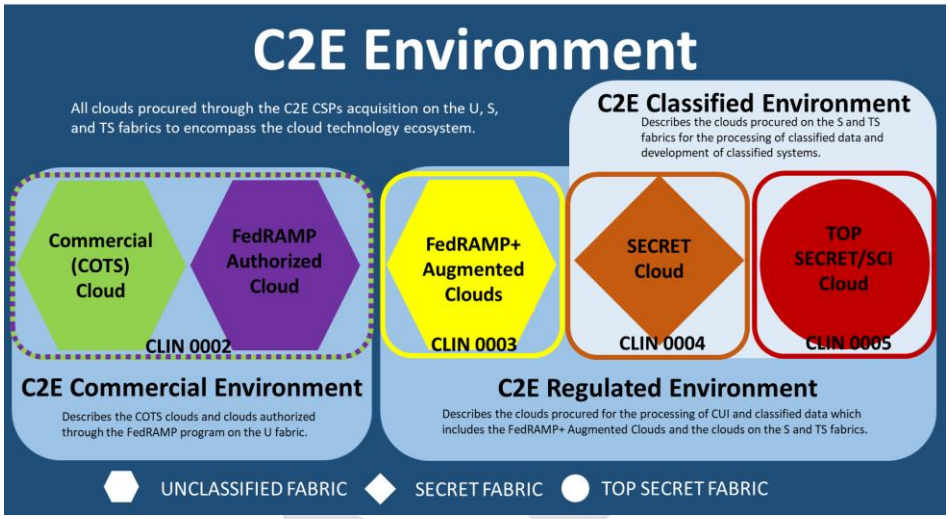


Figure 2 - C2E Environment Overview

- **(U) C2E Commercial Environment**

(U) Unclassified Fabric – Commercial and FedRAMP Authorized Clouds:
(U) The CSP shall provide the full breadth of the CSP's commercially offered cloud services as commercial-off-the-shelf (COTS) technology. When a CSP offers a FedRAMP Authorized cloud, the CSP shall offer FedRAMP Authorized community clouds to support the storage and processing of data within an environment with restricted user access.

- **(U) C2E Regulated Environment (See Appendix E for Ascension Strategy)**

- (U) FedRAMP+ Augmented Clouds for Controlled Unclassified Information (CUI):
(U) The FedRAMP+ Augmented clouds incorporate the FedRAMP Authorized baseline with the addition of a select set of security controls defined by Executive Agent in consultation with the DoD. These are multi-tenant clouds that are restricted to specific IC communities of users. The FedRAMP+ Augmented clouds are designed to support the processing and storage of sensitive workloads, including CUI or non-CUI Non-Critical Mission Information and designated unclassified National Security Systems (NSS), with separately defined controls. While these cloud environments are considered U, they will be physically and logically isolated from the commercial cloud service offerings that support the U fabric, as the security controls describe.

- (U) C2E Classified Environment:

(U) On the classified fabrics, there is an elevated level of security to ensure the protection of Government data and systems interwoven in the design of the infrastructure, development of cloud service offerings, and deployment of systems. To meet these requirements, CSPs shall work with the Executive Agent and IC elements for accreditation utilizing the Risk Management Framework outlined in ICD 503 to meet the security standards, policies, and guidance for deploying cloud services onto the TS/SCI and S fabrics. The distinction between security controls and requirements for implementation between the TS/SCI and S fabrics is described through the documentation in the references section of the requirements.

- **(U) Security levels:** All security levels including UNCLASSIFIED, SECRET, and TS/SCI with intelligence overlays as required.

- **(U) Locations:** Global – to include terrestrial, satellite/space, and subaquatic – with both on- and off-Government premises options as required.

3.0 (U) Applicable Documents

(U) The following documents and corresponding successors shall be incorporated into the contract:

- (U) National Industrial Security Program Operating Manual (NISPOM) and Supplement
- (U) Intelligence Community Directive (ICD) 503 - IC Information Technology Systems Security Risk Management
- (U) ICD 704 - Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
- (U) ICD 705 - Sensitive Compartmented Information Facilities
- (U) ICD 706 – Security Standards for Protecting Domestic IC Facilities
- (U) ICD 710 – Classification and Control Markings System
- (U) ICD 731 – Supply Chain Risk Management

(U) Additional Applicable and/or Reference documents are included in the SRD, which apply to the Technical Requirements as listed in the SRD “Reference” column.

4.0 (U) Requirements

4.1 (U) System Requirements

(U//FOUO) The C2E CSP IDIQ and subsequent task order contracts will acquire cloud computing services directly from large-scale commercial CSPs with established records for innovation (i.e., Technical Agility) and operational excellence in cloud service delivery (i.e., Cloud Maturity). Acquiring services from CSPs, rather than developing those services in-house, has been shown to scale faster to meet IC compute needs and to facilitate the adoption of innovation happening in the commercial marketplace, all while satisfying the rigorous performance and security requirements of the IC, thereby allowing IC consumers to focus on mission delivery.

(U) CSPs shall comply with National Institute of Standards and Technology (NIST) in Special Publication 800-145, which describes cloud computing as:

> *A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

(U) The essential characteristics of cloud shall include service-oriented architectures, on-demand self-service, broad network access, resource pooling, rapid elasticity, resiliency, and metered service usage.

(U) The CSP shall possess a significant market presence in providing public cloud IaaS service offerings. "Significant" is measured and defined as a CSP that has more than three (3) years of market presence, and demonstrates a minimum of $250 million in annual IaaS service revenue over the last 12 months (excluding all managed and professional services) and a minimum of 100,000 virtual machines (VMs) currently in production, operating simultaneously, within its public commercial cloud.[2]

(U//FOUO) Technical requirements describe how the CSP will implement cloud service technology for IaaS, PaaS, and SaaS while adhering to the standards of the guidance documentation identified for each requirement. The technical requirements highlighted in this section, and further detailed within the SOW Attachment J-2 C2E System Requirements Document (SRD), Section 2.0.

4.1.1 (U) Security First

(U//FOUO) The CSP shall comply with these requirements, which are defined as the ability to access, use C2E service offerings worldwide with security as the top priority, and integrated into the development lifecycle. Security First technical requirements that the CSP shall comply with are located within Section 2.1 of Attachment J-2, C2E CSP SRD.

Value	Traceability to SRD Requirements
(U) Security Fundamentals	2.1.1.1 – 2.1.1.6
(U) Access Control	2.1.2.1 – 2.1.2.6
(U) Encryption and Key Management	2.1.3.1 – 2.1.3.12
(U) Data Protection	2.1.4.1 – 2.1.4.2
(U) Proven Logical Separation	2.1.5.1 – 2.1.5.7
(U) Secure Network Protocols	2.1.6.1 – 2.1.6.3
(U) Monitoring, Logging, Auditing	2.1.7.1 – 2.1.7.11
(U) Intrusion Detection	2.1.8.1 – 2.1.8.2

[2] This requirement is a Mandatory Qualification Item. Prior to each Open Season (SOW Appendix E), the Executive Agent has the ability to modify the definition of "significant" to reflect changes in the commercial market.

4.1.2 (U) Global Reach

(U) These requirements are defined as the ability to provide data centers and the full suite of C2E service offerings to IC mission components globally. Global Reach technical requirements that the CSP shall comply with are located within Section 2.2 of Attachment J-2, C2E CSP SRD.

Value	Traceability to SRD Requirements
(U) Global Presence	2.2.1.1 – 2.2.1.6
(U) Global Resource Management	2.2.2.1 – 2.2.2.14

4.1.3 (U) Innovation and Technical Parity

(U) These requirements are defined as the ability to develop a consistent implementation of services and to maintain technical parity of services across all security fabrics, authorized by the Executive Agent and prioritized by the Government, to enable significant advances in support of the intelligence mission. Innovation and Technical Parity technical requirements that the CSP shall comply with are located within Section 2.3 of Attachment J-2, C2E CSP SRD.

Value	Traceability to SRD Requirements
(U) Core Cloud	2.3.1.1 – 2.3.1.11
(U) Foundational Services	2.3.2.1 – 2.3.2.11
(U) Integration, Interoperability, and Portability	2.3.3.1 – 2.3.3.9
(U) Development Resources	2.3.4.1 – 2.3.4.3
(U) Streamlined Deployment	2.3.5.1 – 2.3.5.2

4.1.4 (U) Operational Excellence

(U) These requirements are defined as the ability to deliver operational excellence in cloud computing by such elements as assuring high system availability and data reliability, and providing best-in-class user support. Operational Excellence technical requirements that the CSP shall comply with are located within Section 2.4 of Attachment J-2, C2E CSP SRD.

Value	Traceability to SRD Requirements
(U) Timely Communication and Operational Awareness	2.4.1.1 – 2.4.1.8
(U) Continuity of Operations	2.4.2.1 – 2.4.2.2
(U) Technical Support and Troubleshooting	2.4.3.1

4.2 (U) Contract Management

(U) As background information, contract management is the foundation for the technical requirements detailed within Section 4.1 above. In order to adapt to the speed of mission, the C2E CSP IDIQ and subsequent task orders will streamline IC procurement processes, implement consumption-based funding and acquisition models to keep pace with rapidly changing technologies, leverage cloud flexibility, and ensure delivery of new capabilities at the speed of mission. This section includes the requirements associated with contract management, as well as other contract characteristics essential to the C2E CSP IDIQ.

(U) This section details the Executive Agent's contract management requirements needed to manage services acquired through the C2E CSP task orders. The contract management requirements have been organized into sections:

- Section 4.2.1: Program Management Office (PMO) Support
- Section 4.2.2: Professional Technical Support Services
- Section 4.2.2: Personnel Security
- Section 4.2.3: Physical Security
- Section 4.2.4: Technical Documentation
- Section 4.2.5: Supply Chain Risk Management (SCRM)
- Section 4.2.6: Service Usage, Price Information and Billing Management.

(U) All applicable Contract Data Requirements Lists (CDRLs) deliverables within this section will be executed in accordance with Appendix D.

4.2.1 (U) Program Management Office (PMO) Support

(U) For clouds residing in the C2E Commercial and Regulated Environments:

A. (U) The CSP shall provide overarching program management support to the Executive Agent, including a dedicated Program Manager (PM) and support staff. Program Management Support will involve overseeing all contract activities during the entire period of performance of the IDIQ. Responsibilities would include, but are not limited to program reviews, CSP management team roles and interactions, scheduling, documentation, and account billing as outlined in the Program Management Plan (PMP) (CDRL 001).

B. (U) The CSP shall conduct monthly Program Management Reviews (PMRs) and/or Business Management Reviews (BMRs), and other status reviews with the Executive Agent. The PMR/BMR presentation materials shall be delivered to the Government and include, at a minimum, updates on action items, contract and financial metrics (e.g.: consumption by fabric and IC element, service usage, billing data, actual costs, budget limits, etc.), key schedule updates (including the Integrated Master Schedule (IMS) through initial operating capability (IOC) for the C2E Regulated Environment), capacity ahead of demand and operational metrics, clearance status, security relevant updates, and service offering strategic plans and roadmaps. (CDRL 002)

C. (U) The CSP shall support joint PMRs and/or BMRs with IC elements as directed by the Executive Agent. These reviews shall address the items covered in the monthly

PMRs/BMRs with the Executive Agent, but tailored to the specific IC elements as required along with any requested IC element specific information.

D. (U) The CSP shall host a Contract Initiation Review (CIR) with the Sponsor PM serving as the chairperson. The CIR is a joint Sponsor and CSP decision point for commitment to and implementation of the CSP PMP and other plans identified by the Sponsor PM. (CDRL 002).

E. (U) The CSP shall deliver Monthly Contract Status Reports (MCSR) to include performance metrics on consumption level on all applicable security fabrics and consumption by IC elements and sponsored partners as well. The MCSRs shall also include end-of-month versions of the billing reports that shall be maintained and available for access by the Executive Agent and IC elements for the life of the C2E CSP IDIQ and subsequent task orders. (CDRL 003)

F. (U) The CSP shall provide Service Level Agreements (SLAs) that will address issues, to include but not limited to cloud service availability, scalability, and data reliability. (CDRL 004)

G. (U) The CSP shall work with the CIMM contractor to include, but not limited to, providing consolidated data inputs such as, ordering/spending against each funded task order amount and consumption/usage metrics by service.

H. (U) The CSP shall deliver Transition Plan updates that include all of the steps necessary for a successful transition to the new contract with minimal disruption (refer to SOW 4.3.5) and transition details for the contract lifecycle to address seamless transition between task orders (refer to SOW 4.3.6). (CDRL 006)

4.2.2 (U) Professional Technical Support Services

(U) For clouds residing in the C2E Commercial Environment:

A. (U) The CSP shall offer cloud-adoption accounts for users requiring temporary access to C2E for orientation to services and training.

(U) For clouds residing in the C2E Commercial and Regulated Environments:

A. (U) The CSP shall provide professional and engineering services such as support for planning, design, development, acquisition, provisioning, cost optimization, and implementation of cloud-based systems and applications. Engineering services shall be furnished as needed during any phase of the development lifecycle of system design, development, and operation.

B. (U) The CSP shall provide support services, including but not limited to on-call capability to resolve user technical issues. Based on mission criticality, Tier 4 support services with 24/7/365 operational capability may be required. (CDRL-004)

4.2.3 (U) Personnel Security

(U) For clouds residing in the C2E Regulated Environment:

A. (U//FOUO) The CSP shall provide Industrial Security Approval/SECRET (ISA/S), Industrial Security Approval/TOP SECRET (ISA/TS) and Industrial Security Staff-like Approval/TOP SECRET (ISSA/TS) cleared personnel, or personnel able to be cleared, to support the services offered on the classified fabrics.

B. (U) The CSP shall establish, maintain, and operate an adequately staffed, trained, and cleared C2E Security Program dedicated to directly support an Executive Agent led integrated security team to address all security relevant items in the C2E ecosystem.
C. (U) The CSP shall ensure that all personnel performing work for the CSP contract with access to the Executive Agent's information systems complete all mandatory training requirements.
D. (U//FOUO) The CSP shall provide cleared or able to be cleared maintenance staff including those responsible for the integration and maintenance of IT and mechanical systems. (ICD 704; DoD Cloud Computing SRG v1r3 DISA Risk Management, Cybersecurity Standards 6 March, 2017-Developed by DISA for DoD)
E. (U//FOUO) The CSP shall ensure that personnel maintaining equipment and facilities shall not display any Government or company identification, logos, or advertisements in accordance with the OPSEC plan and security requirements. (ICD 704; DoD Cloud Computing SRG v1r3 DISA Risk Management, Cybersecurity Standards 6 March, 2017-Developed by DISA for DoD)
F. (U//FOUO) The CSP shall identify and assemble security staff with appropriate privileged access to work at the behest of the Government to identify and analyze security incidents. The provider's security professional POC will serve as the Incident Response point of contact to the Executive Agent's or the Executive Agent's Designee Incident Response Team for security incidents. (ICD 702; ICD 704; ICD 705; NIST SP 800-53, revision 4, AC-6, IR-4; CNSSI 1253F Amendment 4, AC-6, IR-4; NISPOM)
G. (U) The CSP shall provide overarching Industrial Security Approval/TOP SECRET (ISA/TS) cleared personnel, including one dedicated Program Management Lead and dedicated support staff, under the Commercial Cloud Enterprise Program Management Office (C2E PMO).
H. (U//FOUO) The CSP shall provide a senior, technical POC with deep technical knowledge in cloud services offerings, cybersecurity, and large scale analytics; appropriate privileged access; appropriate clearance and vetting; and authority on behalf of the CSP to execute the Insider Threat communication and incident response plan and to serve as a representative to jointly build a shared insider threat program and serve on the EA's incident response consortium. (NISPOM (DoD 5220.22-M, Incorporating Change 2, 2016; EO 13587; NITTF 2017 Insider Threat Guide; NITTF Maturity Framework; Presidential Memorandum on National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; ICS 700-02; ICD 503)

(U) For clouds residing in the C2E Classified Environment in the C2E Regulated Environment:

A. (U//FOUO) The CSP shall provide technical network personnel into the Executive Agent's Security Operations Center (SOC).
B. (U//FOUO) The CSP shall integrate provider's key technical network personnel into Government security teams based on the scale of applications residing within the C2E ecosystem.

4.2.4 (U) Physical Security

(U) For clouds residing in the C2E Regulated Environment:

A. (U//FOUO) The CSP shall permit Government auditing and on-the-spot inspections of all administrative actions in the CSP's physical location and facilities. (ICD 705, ICS 705-1, NISPOM)
B. (U//FOUO) The CSP shall permit Government personnel access to data centers in order to evaluate security implementation of Risk Management Frameworks (RMF) as it relates to data center solution implementation. (ICD 705, ICS 705-1, NISPOM)
C. (U//FOUO) The CSP shall allow for Government physical access control and intrusion detection systems to be installed in accordance with the level of protection for commercial facilities in accordance with the Government direction. (ICD 705, ICS 705-1, NISPOM)
D. (U) The CSP shall provide planning, engineering, staffing, and operations and maintenance resources to comply with all physical and technical security directives, policies, and specifications at the request of the Government. (ICD 705, ICS 705-1, NISPOM)
E. (U) The CSP shall notify and alert the Government of any physical intrusion and security breach within the timeframe dictated by the Government. (NIST SP 800-53 version 4, PE-6, IR-6; CNSSI No. 1253, PE-6, IR-6; ICS 705-1 G.2.c.(1); IC CIO Memo 2011-0463; CNSSI 1253F Attachment 4: Intelligence Overlays, PE-6; 32 CFR Parts 2001 and 2004)
F. (U//FOUO) The CSP shall not allow materials to contain or display any Government or company identification, logos, or advertisements in accordance with the OPSEC plan and security requirements.
G. (U) As necessary, the CSP shall provide access to Government personnel and the Government's approved agent(s) to add or remove equipment as necessary and to enable the collocation of more than one CSP within a facility. If more than one CSP is collocated in a facility owned by the Government, proper separation will allow for the protection of the CSPs' IP/PROPIN equipment, designs, processes, and administration. (ICD 906, FAR 45.401, NIST SP 800-53, revision 4 PE-2)
H. (U//FOUO) The Contractor shall implement and maintain physical separation of infrastructure and networks, as required. (CNSSAM Tempest 1-13, Red/Black Installation Guidance; CNSSI No. 7003; NISPOM)

(U) For clouds residing on the TS/SCI and S security fabrics only in the C2E Regulated Environment:

A. (U//FOUO) The CSP shall secure all physical infrastructure, networks, and hardware to achieve and maintain Sensitive Compartmented Information Facility (SCIF) and facility accreditations, and complete all required actions and deliverables in order to achieve and maintain facility SCIF accreditation prior to the contractually agreed upon IOC dates for services. (ICD 705, ICD 706, ICS 705-1, ICS 705-2, NISPOM)

B. (U//FOUO) The CSP shall maintain access control policies and procedures to ensure access to accredited facilities is limited to cleared and approved individuals. (ICD 704, ICD 705, NISPOM)
C. (U//FOUO) The CSP shall submit construction security plans that incorporate the established procedures for the protection of classified material. (NISPOM, ICD 705, ICS 705-1, CDRL 007)
D. (U//FOUO) The CSP shall complete all required actions and deliverables in order to achieve and maintain facility SCIF accreditation prior to the contractually agreed upon IOC dates for services. (ICD 705)
E. (U//FOUO) The CSP shall provide an accredited SCIF to support communication, collaboration, and work for the execution of the C2E program to include connected access to the network and Remote Management Area (RMA). (ICD 705, ICS 705-1, NISPOM)

4.2.5 (U) Technical Documentation

(U) For clouds residing in the C2E Commercial and Regulated Environments:

A. (U) The CSP Shall provide commercially available online user guides, tutorials, and training seminars designed for classroom and self-guided training tailored for different user types (i.e., technical and non-technical users).

(U) For clouds residing in the C2E Regulated Environment:

A. (U) The CSP shall develop, deliver, and maintain all Information Security (INFOSEC), Concepts of Operations (CONOPS), and Operational Security (OPSEC) plans for all cloud environments in the C2E Regulated Environment. (CDRL 007)
B. (U) The CSP shall deliver a data center location proposal within its CONOPS including, but not limited to site surveys, power specifications and access, and utility access. (CDRL 007)
C. (U) The CSP shall provide and maintain an Operations and Maintenance Plan for conducting operations under normal conditions including but not limited to change management, incident response, patch management, routine maintenance, repair, and recapitalization of equipment. (CDRL 009)
D. (U//FOUO) The CSP shall provide a data center architecture and contingency plan that accounts for IC-wide COOP and disaster recovery (DR) requirements, including but not limited to geographic distribution of facilities. (NIST SP 800-53, rev 4 CP-1, CP-2, CP-10; NIST SP 800-34, rev 1; CDRL 010)
E. (U//FOUO) The CSP shall develop a strategic plan in conjunction with the Government to accommodate COOP and DR for failover of cloud service offerings, including but not limited to compute, storage, networks, and processing. (NIST SP 800-53, rev 4 CP-1, CP-2, CP-10; NIST SP 800-34, rev 1; CDRL 010)

4.2.6 (U) Supply Chain Risk Management (SCRM)

(U) For clouds residing in the C2E Commercial and Regulated Environments:

A. (U) The CSP shall adhere to policies and directives and provide notification regarding the acquisition of intellectual property and integration of new code baselines in support of the Government's adherence to references. (ICD 731, Secure Technology Act, FAR part 9.105)
B. (U//FOUO) As a part of the Program Management Plan (PMP) CDRL, the CSP shall provide and maintain an SCRM approach for approval by the Executive Agent or the Executive Agent's Designee. (41 USC 1326, CDRL 001)
C. (U//FOUO) The CSP shall provide completed SCRM questionnaires to support the software supply chain for all third party vendor services, third party vendor companies, and subcontractors (down to the third level of sub-contracts) services and are considered for use in the C2E environment in order to allow the Government to make an informed risk management decision. (ICD 731, Secure Technology, 41 USC 1326)
D. (U//FOUO) The CSP shall provide completed SCRM questionnaires in a timely manner to support the hardware supply chain for all third party vendor services, third party vendor companies, and subcontractors (down to the third level of sub-contracts) used in the hardware infrastructure when hardware infrastructure is considered for use in the C2E environment in order to allow the Government to make an informed risk management decision. (ICD 731, Secure Technology Act, 41 USC 1326)
E. (U) The CSP shall adhere to policies and directives and provide notification regarding the acquisition of hardware and equipment in support of the Government's adherence to references. ICD 731 Secure Technology Act)

(U) For clouds residing in the C2E Regulated Environment:

A. (U//FOUO) The CSP shall develop and maintain an SCRM repository containing SCRM questionnaire results and any further research conducted by the CSP in order to vet companies and their associated software code to support the software supply chain. The CSP shall maintain the availability of the repository to the Government for on-going risk assessment. The CSP shall provide a self-service capability to the Government to ingest data from the repository as requested. (41 USC 1326)
B. (U//FOUO) The CSP shall develop and maintain an SCRM hardware repository containing SCRM questionnaire results and any further research conducted by the CSP in order to vet companies and to support the hardware and physical supply chain. The CSP shall maintain the availability of the repository to the Government for on-going risk assessment. The CSP shall provide a self-service capability to the Government to ingest data from the repository as requested. (ICD 731, Secure Technology Act, 41 USC 1326)
C. (U//FOUO) The CSP shall align with procurement requirements defined by the Government to support global access to C2E offerings. (NIST SP 800-145)
D. (U//FOUO) The CSP shall ensure technical parity with publicly available commercial cloud for generational recapitalization and upgrading of all CSP-furnished hardware, as prioritized by the government in conjunction with the CSP, while complying with all supply chain risk management requirements and policies.

E. (U) The CSP shall repair damage caused by the CSP that impacts the cloud technology in accordance with Government prescribed standards and timelines at no additional cost, such as damage to hardware, facilities, and network.
F. (U) The CSP shall dispose or surrender for destruction any Government-Furnished Property (GFP) or CSP-Acquired Property (CAP) that records, processes, stores and/or transmits Agency classified or sensitive data per the policies of the Executive Agent or the Executive Agent's Designee. (FAR 52.245-1, Internal policies and details will be provided post award)
G. (U//FOUO) The CSP shall provide notification to users and replace equipment that has been identified by the Government as a security concern within the timeframe dictated by the Executive Agent or the Executive Agent's Designee. (Executive Agent policies and details will be provided post-award)

4.2.7 (U) Service Usage, Price Information, and Billing Management

(U) For clouds residing in the C2E Commercial and Regulated Environments:

A. (U) The CSP shall provide the capability of setting billing alerts or notifications based on cloud service usage at both the Agency and individual account level, to include but not limited to real-time cost tracking, thresholds (ceilings) for cost management, and consumption cost for services.
B. (U) The CSP shall provide services in a utility model whereby the IC elements are billed only for services that are consumed during the prior billing period, or in a licensing model as appropriate to the service for the duration of the license.
C. (U) The CSP shall provide a commercial Service Pricing Catalog and a self-service price calculator, whereby the IC elements can efficiently estimate service prices. The self-service price calculator shall for all applicable security fabrics. The self-service price calculator shall include any applicable information for transaction costs and optimizing costs to include but not limited to purchasing economies of scale and volume discount pricing. (CDRL 005)
D. (U) The CSP shall provide a structured pricing model for the C2E Regulated Environment, including but not limited to a description of the most current version of the CSP's commercial Service Pricing Catalog, and any proposed multiplier factor for increase or decrease from those rates, as applicable,
E. (U) The CSP shall provide on-going pricing parity, as adjusted by any multiplier factor proposed by the CSP and agreed upon in the Contract, such that C2E pricing for the C2E Regulated Environment aligns with its commercial pricing methodology that incorporates such factors as economies of scale, volume discounts, etc. to drive cost and cost reductions.
F. (U) The CSP shall permit the use of subscription, on-demand, and software and service license models, including the use of the Government's software and service licenses, known as "bring-your-own-license" (BYOL). When applicable, ensure that service accounting reflects existing licenses so that customers are properly billed.

4.3 (U) Contract Characteristics

4.3.1 (U) Contract Type

- (U) C2E CSP will be multiple-award IDIQ contract, with Firm Fixed Price (FFP) task orders.

4.3.2 (U) Period of Performance

- (U) The C2E CSP IDIQ will have a five-year base ordering period with two, five-year optional ordering periods.

4.3.3 (U) Place of Performance

- (U) The C2E CSP IDIQ shall be performed at CSP and Government locations throughout the world.

4.3.4 (U) Contract Security

- (U) All security fabrics:
  - (U//FOUO) The association between the Executive Agent and the CSP will be classified UNCLASSIFIED//For Official Use Only (U//FOUO). Other classification standards are contained in the Contract Data Classification Guide (CDCG).
  - (U) The CSP shall be Foreign Ownership Control or Interest (FOCI) eligible to perform the work under the contract.
  - (U) The CSP shall ensure that all systems have documented security approvals from the ordering Agency before resources are provisioned for customer use under a Task Order.

4.3.5 (U) Transition from Existing Cloud-Based Contracts to C2E

- (U) All security fabrics:
  - (U) The CSP shall provide a plan for a logical IC element to transition of workloads from existing or predecessor cloud-based contracts, such as the C2S contract, to the C2E multiple-award IDIQ contract (to include IaaS, SaaS, and PaaS offerings) to minimize, to the maximum extent practicable, any adverse effect created by the transition process. (CDRL 006)

4.3.6 (U) Contract Lifecycle Transition

- (U) All security fabrics:
  - (U) As required under Appendix D, the CSP shall provide the capability to transition off a CSP's cloud infrastructure as required by mission needs and when the contract or task order ends (CDRL 006). The Executive Agent may "on-ramp" or "off-ramp" CSPs to/from the C2E contract, as defined in SOW, Appendix E.

4.3.7 (U) Government Furnished Property, Facilities, Services, and Information (GFX)

- (U) For the C2E Commercial Environment:
  - (U) The Executive Agent will not provide any Government-furnished property (GFP), facilities (GFF), services (GFS), and information (GFI).
- (U) For the C2E Regulated Environment:

- (U) The objective is to provide minimal or no GFX. If GFX is necessary, the Executive Agent shall retain title to any property provided. The CSP shall use, transfer, account for, and manage GFX used on this contract in accordance with the applicable contract clauses and the Government Furnished Property List attached in Section J, Attachment TBD of the contract.

5.0 (U) Attachments and Appendices

- (U) Attachment J-2, C2E CSP System Requirements Document (SRD), date 03 February 2020.
- (U) Attachment J-3, Contract Data Classification Guide (CDCG), date 15 January 2020.
- (U) Attachment J-4, C2E CSP Contract Data Requirements List (CDRL), dated 03 February 2020
- (U) Appendix A, FedRAMP+ Background
- (U) Appendix B, C2E CSP Definitions
- (U) Appendix C, C2E CSP Acronyms List
- (U) Appendix D, C2E CSP CDRL Table
- (U) Appendix E, C2E CSP Ascension Strategy
- (U) Policy References, Bidder's Library, TBD.

APPENDIX A – (U) FedRAMP Authorized and FedRAMP+ Augmented Clouds

(U) The Government requires community cloud environments on the UNCLASSIFIED fabric with restricted access that are separate from CSP commercial cloud environments. These separate cloud environments, consisting of FedRAMP Authorized and FedRAMP+ Augmented Clouds, will further facilitate cloud adoption across the IC, offer a secure environment that allows for the development of new mission capabilities for future use on the classified fabric(s), and accelerate innovation in order to keep pace with IC mission component needs.

(U) C2E Commercial Environment: FedRAMP Authorized Clouds:
(U) When a CSP offers a FedRAMP Authorized cloud, the Government will be able to procure FedRAMP Authorized cloud services to support the storage and processing of UNCLASSIFIED data within an environment held to a high level of scrutiny and validation for cybersecurity and other mandatory requirements.

(U) C2E Regulated Environment: FedRAMP+ Augmented Clouds for Controlled Unclassified Information (CUI):
(U) The FedRAMP+ Augmented clouds incorporate the FedRAMP Authorized baseline with the addition of a select set of security controls defined by Executive Agent and the DoD. These are multi-tenant clouds that are restricted to specific IC communities of users. The FedRAMP+ Augmented clouds are designed to support the processing and storage of sensitive workloads, including CUI or non-CUI Non-Critical Mission Information and designated unclassified National Security Systems (NSS), with separately defined controls as shown in Figure 3. While these cloud environments are considered U, they will be physically and logically isolated from the commercial cloud service offerings that support the U fabric, as the security controls describe.

(U) The below diagram provides a summary description of FedRAMP+ Augmented requirements, further defined within the C2E CSP Systems Requirements Document (SRD).

757 **(U) Figure 3[3] – Summary of FedRAMP+ Augmented Clouds for CUI Requirements**

758

DoD IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set (Approved by Executive Agent/ DoD, per ICD 503)	US / US outlying areas or On-Government premises	Direct connect to one or more tenant IC agency/ DoD networks	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set (Approved by Executive Agent/ DoD, per ICD 503)	US / US outlying areas or On-Government premises	Direct connect to one or more tenant IC agency/ DoD networks	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	

759

[3] Defense Information Systems Agency (DISA) for the Department of Defense (DoD), *Department of Defense Cloud Computing Security Requirements Guide*, Version 1, Release 3 (6 March 2017).

APPENDIX B – (U) C2E CSP Definitions

Term	Definition
(U) Access Delegation	Authorization for an action on behalf of a user or application through a permission model
(U) Air-Gapped Network	A network, including devices or computers, this is not connected to the Internet.
(U) Alert	Notification that a specific attack has been directed at an organization's information systems.
(U) Application Programming Interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.
(U) Attribute Based Access Control (ABAC)	An access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, environment attribute etc.
(U) Audit Context	Lists, records, databases, etc. needed to attribute, interpret, and disposition other forms of audit data.
(U) Automation/automated	Digital enablement of processes and functions beyond conventional data manipulation and record keeping activities, usually through the use of advanced technologies.
(U) Bring Your Own License (BYOL)	The ability of a Cloud consumer to deploy software or platform offerings into the Cloud without additional licensing cost for that software or platform offering because the Cloud consumer already possesses a valid license from a separate contracting action.
(U) C2E Classified Environment	Describes the clouds procured on the S and TS fabrics for the processing of classified data and development of classified systems.
(U) C2E Commercial Environment	Describes the COTS clouds and clouds authorized through the FedRAMP program on the U fabric.
(U) C2E Environment	All clouds procured through the C2E CSP IDIQ on the U, S, and TS fabrics to encompass the cloud technology ecosystem.
(U) C2E Regulated Environment	Describes the clouds procured for the processing of CUI and classified data which includes the FedRAMP+ Augmented Clouds and the clouds on the S and TS fabrics.
(U) Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
(U) Cloud Consumer	A person or organization that is a customer of a cloud; note that a cloud consumer may itself be a cloud and that clouds may offer services to one another.

Term	Definition
(U) Cloud infrastructure	The collection of hardware and software that enables the five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.
(U) Cloud Service Provider (CSP)	An organization that provides cloud services.
(U) Cloud-Native Audit	User attributable audit records of activity using cloud services, including information on administration and configuration of cloud user accounts.
(U) Community Cloud	Multitenant cloud but limited to a particular customer community
(U) Consumer Plane	Administration, configuration, and direct use of cloud accounts, resources, and services, including IaaS, PaaS, SaaS, etc. This does not include indirect use of cloud services, such as visiting a website or use of an application hosted in the cloud by another cloud user.
(U) Cryptographic Certainty	Formal certification of Type 1 Hypervisors certified against FIPS 140-2 to confirm the cryptographic algorithm used has been reviewed for conformance to module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. FIPS 140-2 certification ensures a high degree of confidence that the Type 1 Hypervisor provides logical isolation of the image within a cloud environment with cryptographic certainty.
(U) CSP Air-Gapped Administrative Plane	Systems and/or networks used for administration of air-gapped cloud fabrics by privileged users.
(U) CSP Cloud-Support Audit	User attributable audit records of user activity on the CSP administrative plane. This may include, but is not limited to user activity monitoring (UAM) data, other user activity logs generated by an operating system, and audit logs from non-cloud-native tools used to administer the cloud.

Term	Definition
(U) CSP Commercial Air-Gapped Administrative Plane	Systems and/or networks that are used for direct administration of commercially available cloud fabrics by privileged users. For CSPs providing air-gapped cloud fabrics, this plane also provides indirect support of those air-gapped fabrics.
(U) Data Erasure	Process intended to render magnetically stored information irretrievable by normal means.
(U) Data Localization	Requirement that data created or collected within the borders of a country must be processed and stored within the boundaries of the same country.
(U) Data Purge	Application of physical or logical techniques that render Target Data recovery infeasible.
(U) Data Residency	The geographic location where data is stored.
(U) Data Sovereignty	The laws, rights, and regulations that govern data due to the geographic location of the data storage.
(U) Data-at-Rest	Data in persistent storage.
(U) Data-in-Transit	Data actively moving from one location to another.
(U) Edge Computing	A distributed computing paradigm in which computation is largely or completely performed on distributed edge nodes.
(U) Elasticity	For a CSP, the ability to increase or decrease the amount of system capacity (for example, CPU, storage, memory and input/output bandwidth) that is available for a given cloud service on demand, in an automated fashion. From the consumer and Real Time Infrastructure (RTI) perspectives, cloud service elasticity is an automated means to increase or decrease a specific service capacity in response to increasing or scheduled demand changes.
(U) Encrypt	Cryptographically transform data to produce cipher text.
(U) Encryption	Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.
(U) Everything-as-a-Service (XaaS)	The capability provided to the consumer to deploy any and every consumer-created or acquired service on a cloud infrastructure.

Term	Definition
(U) Fabric	A term used generally to describe an information environment that supports data at a particular classification level; a fabric is comprised of multiple agencies supporting a variety of authorities with multiple operational capabilities that can include infrastructure and systems. A fabric is a logical collection of physical and virtual networks, systems and applications that are accredited to protect information up to a specific classification level.
(U) Federated Identity Management	A process that allows for the conveyance of identity and authentication information across a set of networked systems.
(U) FedRAMP+ Augmented Clouds	These clouds are developed from the FedRAMP program's Moderate and High baselines with additional controls designated by the Government for the processing and storage of CUI data and NSS.
(U) Fog Computing	A layered model for enabling ubiquitous access to a shared continuum of computing resources.
(U) Graphical User Interface (GUI)	A form of user interface that allows users to interact with functionality through graphical icons.
(U) Hyperscale	Computing architecture that expands and contracts based on demand.
(U) Hypervisor	The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware and provides isolation for various execution stacks represented by Virtual Machines.
(U) Identification and Authentication	The process of establishing the identity of an entity interacting with a system.
(U) Identity Management System (IDMS)	A system comprised of one or more systems or applications that manages the identity verification, validation and issuance process.
(U) Identity Verification	The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.
(U) Identity-based Authentication	A process that provides assurance of an entity's identity by means of an authentication mechanism.
(U) Infrastructure-as-a-Service (IaaS)	The capability provided to the consumer to provision 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 consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Term	Definition
(U) Insider	Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems.
(U) Insider Threat	The threat than an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through loss or degradation of departmental resources or capabilities.
(U) Insider Threat Alerts	Events, triggers, or near-real time alerts derived from one or more of the other audit types (cloud-native audit, CSP cloud-support audit, cloud audit context as applicable) related to potential insider threat activity. These may be generated by rules, algorithms, machine learning, etc.
(U) Interoperability	Ability to process data using different services on different cloud systems through common specifications.
(U) Intrusion detection	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.
(U) Intrusion detection system (IDS)	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
(U) Isolation	The ability to keep multiple instances of software separated so that each instance only sees and can affect itself.
(U) Logical Isolation	Logical partitioning may divide resources on a single host or across multiple hosts as in a pool of resources with the same security impact level categorization, allowing multiple guest OSs to share the same physical resources, such as processors and RAM, with the hypervisor mediating access to the resources. Isolation involves limiting guest OS communications and the access that each guest OS has to the other guest OSs, to the hypervisor, and to the host OS (if present).

Term	Definition
(U) Migration	Moving data, applications, and even infrastructure from on-premises computers or infrastructure to a virtual pool of on-demand, shared resources that offer compute, storage, and network services at scale.
(U) Mist Computing	Mist computing is a lightweight and rudimentary form of fog computing that resides directly within the network fabric at the edge of the network fabric.
(U) Multi-cloud	The deliberate use of cloud services from multiple cloud providers.
(U) Multitenancy	The mode of operation where multiple independent instances (tenants) of one or multiple applications operate in a shared environment. The instances are logically isolated, but physically integrated.
(U) Network Domain	Includes Wide Area Networks (WANs), Local Area Networks (LANs), Campus Area Networks (CANs), and Metropolitan Area Networks (MANs). Logically combines both classification and dissemination domains.
(U) Notification	A report to inform users.
(U) Off-Government Premises	Away from or outside of a building or the area of land that it is on-Government Premises.
(U) On-Demand	Resources that are provisioned as needed such as computing capabilities.
(U) On-Government Premises	The physical infrastructure providing cloud services is located on property that is owned or controlled by the U.S. Government.
(U) Physical Isolation	Condition of a network that is not connected physically to entities or systems.
(U) Platform-as-a-Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
(U) Portability	Ability to move data from one cloud system to another and have the ability to run on different cloud systems.
(U) Pricing Parity	The application of the commercial pricing methodology that incorporates economies of scale, volume discounts, etc. to drive cost and cost reductions in the non-commercial cloud environments (i.e. FedRAMP and the C2E Regulated Environment).

Term	Definition
(U) Private Cloud	Single-tenant cloud computing in which the tenant is only one organization or the tenants are completely isolated from one another. CSP delivers cloud based compute resources though a dedicated infrastructure with restricted access to the client organization.
(U) Public Cloud	Multitenant or mixed tenancy cloud
(U) Rapid elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
(U) Risk Management Framework (RMF)	The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.
(U) Role Based Access Control (RBAC)	An access control paradigm based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
(U) Scalability	The ability to increase capacity to meet demand.
(U) Scale	The act of increasing capacity to meet demand.
(U) Security Assessment (Assessment for A&A)	A security assessment is the required comprehensive assessment of the management, operational, and technical security controls in an information system, or for a particular item of information technology, made in support of authorization decisions.
(U) Security Authorization (Authorization for A&A)	Authorization decisions are official management decisions that explicitly accept a defined level of risk associated with the operation of an information technology system at a particular level of security in a specific environment on half of an IC element. By authorizing an information system, an IC element approves it for operation at a particular level of security in a particular environment, and thus establishes the level of risk associated with the operating the system and the associated implications for operations, assets, or individuals.
(U) Self-Service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, without requiring human interaction with each service provider.

Term	Definition
(U) Software-as-a-Service (SaaS)	The capability provided to the consumer is 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 email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
(U) Technical Parity	Providing equivalent functionality to commercial cloud services and capabilities for cloud services in the C2E Regulated Environment through the introduction of new services that are prioritized by the Government as having mission impact and by maintaining consistency in version, patching, and O&M for existing services.
(U) Tier 4 Support	Reach back for development and engineering support to resolve complex issues.
(U) Transport Layer Security (TLS)	A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.
(U) Virtual Machine (VM)	A software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.
(U) Virtualization	The use of an abstraction layer to simulate computing hardware so that multiple operating systems can run on a single computer. A methodology for emulation or abstraction of hardware resources that enables complete execution stacks including software applications to run on it.

761

762 # APPENDIX C – (U) Acronyms List

A&A	Assessment and Authorization
AI	Artificial Intelligence
APT	Advanced Persistent Threat
BYOL	Bring-Your-Own-License
C2E	Commercial Cloud Enterprise
C2S	Commercial Cloud Services
CIA	Central Intelligence Agency
CDCG	Contract Data Classification Guide
CDRL	Contract Data Requirements List
CIO	Chief Information Officer
COOP	Continuity of Operations
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DevSecOps	Development Security Operations
DOD	Department of Defense
DOE	Department of Energy
DIA	Defense Intelligence Agency
DHS	Department of Homeland Security
EO	Executive Order
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FFP	Firm Fixed Price
FFRDC	Federally Funded Research and Development Center
FOCI	Foreign Ownership Control or Interest
GFF	Government Furnished Facilities
GFI	Government Furnished Information
GFP	Government Furnished Property
GFS	Government Furnished Services
GFX	Government Furnished Property, Facilities, Services, and Information
IaaS	Infrastructure-as-a-Service
IC	Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICN	Intelligence Community Network
IDIQ	Indefinite-Delivery Indefinite-Quantity
ISA	Industrial Security Approval
ISP	Internet Service Provider
ISSA	Industrial Security Staff-like Approval
ITAR	International Traffic and Arms Regulations
IXP	ICN eXchange Point

ML	Machine Learning
NISPOM	National Industrial Security Program Operating Manual
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
NSS	National Security Systems
O&M	Operations and Maintenance
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSEC	Operational Security
PaaS	Platform-as-a-Service
PMO	Program Management Office
RFI	Request for Information
SaaS	Software-as-a-Service
SCI	Sensitive Compartmented Information
CIMM	Cloud Integrator/Multi-Cloud Management (CIMM)
SOW	Statement of Work
SRD	System Requirements Document
TEM	Technical Exchange Meeting
TS	Top Secret
VPN	Virtual Private Network
XaaS	Everything-as-a-Service

763
764

APPENDIX D – (U) Contract Data Requirements List (CDRL)

(U) Awardees will be required to provide initial versions of CDRL items 001 through 006 as part of Task Order (TO) 001, for the Unclassified CSP Program Management Office (PMO). All IDIQ awardees will also be awarded TO 001. Those awardees that receive unexercised options under the C2E Regulated Environment (as explained in Appendix E), and that are awarded the Classified CSP PMO task order, will provide initial versions of CDRL items 007 through 010 as part of the Classified CSP PMO task order. After the periods of performance of Unclassified and/or Classified CSP PMO task order end, awardees will be required to provide updated versions of the CDRL items and other administrative documents as required (A/R), as part of overall contract administration. Any costs associated with such revisions or updates to documents will be built into the awardee's service prices.

CDRL #	Title	Fabric	CLINs	Delivery
001	Program Management Plan (PMP)	All	All	• Initial w/Proposal • Updates via TO 001, Classified PMO TO and A/R
002	Presentation Materials	All	All	• Initial w/TO 001 • Updates via Classified PMO TO and A/R
003	Monthly Contract Status Report (MCSR)	All	All	• Initial w/TO 001 • Updates via Classified PMO TO and A/R
004	Service Level Agreements (SLAs)	All	All	• Initial w/Proposal • Updates via TO 001, Classified PMO TO and A/R
005	Service Pricing Catalog	All	All	• Initial w/Proposal • Updates via TO 001 and A/R
006	Transition Plan Updates	All	All	• Initial w/TO 001 • Updates via Classified PMO TO and A/R
007	Assessment & Authorization (A&A) Process Documentation	FR+ Augmented and Classified	0003, 0004, 0005 and applicable Option period CLINs	• Initial w/ Classified PMO TO • Updates A/R
008	Technical Documentation	FR+ Augmented and Classified	0003, 0004, 0005 and applicable Option period CLINs	• Initial w/ Classified PMO TO • Updates A/R
009	Operations and Maintenance (O&M) Plan	FR+ Augmented and Classified	0003, 0004, 0005 and applicable Option period CLINs	• Initial w/ Classified PMO TO • Updates A/R
010	COOP/DR Documentation	FR+ Augmented and Classified	0003, 0004, 0005 and applicable Option period CLINs	• Initial w/ Classified PMO TO • Updates A/R

APPENDIX E – (U) CSP Ascension Strategy & Open Season

(U) Contract Life Cycle: Award and Ascension Strategy

(U) The purpose of this Appendix is to provide context of how the evaluation process and unexercised, priced C2E Regulated Environment option CLINs are executed, as well as the relationship to IDIQ contract life cycle with the use of Open Season as described below.

(U) The C2E IDIQ award strategy includes the following:

- Mandatory Qualification Items (Pass/Fail) (REQUIRED)
- C2E Commercial Environment (Tradeoff) (Part 1 – REQUIRED)
- C2E Regulated Environment (Confidence Assessment) (Part 2 – OPTIONAL)

(U//FOUO) CSP(s) must pass the Mandatory Qualification Items prior to being evaluated in the best value tradeoff process under Part 1. Part 1 evaluates the extent to which a proposal demonstrates an effective technical and management approach to meet C2E Commercial Environment requirements of the Statement of Work (SOW) and System Requirements Document (SRD). The Government expects to award IDIQ contracts to multiple CSPs to provide cloud services under the C2E Commercial Environment. CSP(s) must submit proposals for both the Mandatory Qualification Items and Part 1 in order to be considered for award of the base C2E CSP IDIQ contract.

(U//FOUO) Part 2 is optional and allows CSP(s) who are interested to compete for unexercised, priced option CLINs for moving up, or "ascending," to the C2E Regulated Environment (FedRAMP+ Augmented Clouds, Secret, and Top Secret/SCI). Only CSP(s) who are selected for award of the required CLINs on the basis of the Mandatory Qualification Items and Part 1 will be eligible for award of the optional CLINs under Part 2. The Part 2 evaluates the extent to which a proposal demonstrates an effective technical and management approach to meet C2E Regulated Environment requirements. CSP(s) proposing for this optional piece will be evaluated and assigned a confidence rating during the evaluation process. CSP(s) that are awarded Part 2 will receive the unexercised, priced option CLINs as part of their IDIQ contract. CSP(s) who do not propose to Part 2, or are not selected for award under Part 2, will not receive the unexercised, priced option CLINs and therefore will not be eligible to compete for task orders under the C2E Regulated Environment. The Open Season section addresses the next opportunity for those CSP(s) (among others) to compete for the C2E Regulated Environment scope of work. Post-award, CSPs with unexercised, priced option CLINs will have the opportunity to "ascend" the various security fabrics.

(U//FOUO) In order to ascend to FedRAMP+ for CUI, CSP(s) may submit the required documentation any time starting 30-days after award of the base IDIQ contract. The anticipated Initial Operating Capability (IOC) would be 45-days post receipt of the documentation. The FedRAMP+ for CUI optional CLIN will be exercised upon achieving IOC.

(U//FOUO) In order to ascend to the C2E Classified Environment (Secret and/or Top Secret/SCI), CSP(s) must compete for and receive award of a task order to obtain the services of a Classified CSP PMO to fulfill security-unique requirements associated with achieving IOC in the C2E Classified Environment. Proposals for Classified CSP PMOs will be requested after award of the base IDIQ contract. The Government anticipates soliciting additional Classified CSP PMO task orders yearly or at the Executive Agent's discretion. Only CSP(s) with unexercised, priced option CLINs (S and TS/SCI) may compete for the Classified CSP PMO task order(s). Such task orders may be awarded to one or multiple CSP(s), as will be further explained in the Task Order Proposal Requests, based on the quality of proposals and internal Government resource or mission constraints. A CSP must receive a Classified CSP PMO task order award prior to beginning the ICD 503 process to achieve IOC on the applicable classified fabric(s). CSP(s) with unexercised, priced option CLINs (S and TS/SCI) who elect not to compete for the first Classified CSP PMO order or who are not awarded an order may compete on future Classified CSP PMO orders. The Secret and Top Secret/SCI option CLINs will be exercised upon achieving IOC.

(U) <u>Open Season – On/Off Ramping</u>

- **(U) On-Ramping (Qualifying new CSP(s) to the Base IDIQ Pool):**
  (U//FOUO) It is in the Government's best interest to maintain a competitive environment and to ensure that the CSP pool remains dynamic and can respond to emerging requirements and advances in technology. As such, if the C2E Contracting Officer determines that it is in the best interest of the Government to open the C2E CSP base IDIQ pool to new contractors, the Government reserves the right to announce and implement an "Open Season." The Government anticipates that it will do so prior to exercising the two option periods (at the beginning of the 5th contract year of the base ordering period and at the beginning of the 10th contract year of the first ordering option period). The selection/inclusion of new CSP(s) into the IDIQ pool would be effective at the start of each option period. Alternatively, at the discretion of the Executive Agent, an Open Season may also be announced and implemented at other times during the period of performance. During Open Seasons, new CSP(s) can compete and receive IDIQ awards for the C2E Commercial Environment (Mandatory Qualification Items and Part 1) and unexercised, priced option CLINs for the C2E Regulated Environment (Part 2) using the same criteria (or equivalent criteria based on market maturity) as in C2E CSP IDIQ Section M, Evaluation Factors for Award. Any CSP receiving an IDIQ contract during open season would be eligible to compete on task orders solicited after the date of its IDIQ award to the same degree as other C2E CSP(s).

- **(U) On-Ramping (Qualifying existing CSP(s) for an unexercised option CLIN for C2E Regulated Environment):**
  (U//FOUO) For CSP(s) that are awarded a base IDIQ pool and currently on the C2E Commercial Environment, but either did not propose for the unexercised, priced options, or were not awarded these options, Open Season provides the opportunity to compete for the unexercised, priced option CLINs for the C2E Regulated Environment. If they receive awards of these CLINs, existing CSP(s) can then ascend the C2E Regulated Environment, as described above.

(U//FOUO) In both instances, existing and new CSP(s) that receive award of an optional CLIN for the C2E Regulated Environment during Open Season can ascend the C2E Regulated Environment per the Ascension Strategy outlined above. The Ascension Strategy applies to all CSPs, regardless of when the CSP joins the base IDIQ pool.

- **(U) Off-Ramping (Removing existing CSP(s) from the Base IDIQ Pool):**
(U//FOUO) During contract performance, the Government will also review its existing CSP pool to determine whether it is appropriate to off-ramp awardees from the IDIQ pool. CSP(s) may be off-ramped from the base IDIQ pool based on the following considerations:

    - Active participation in task orders competitions
    - Corporate commitment to supporting the C2E program
    - Competitive pricing and technical innovation
    - Sound security practices, as applicable
    - Continued market presence as a commercial CSPs

(U//FOUO) The C2E Contracting Officer will notify any CSP(s) being off-ramped, and option period CLINs will not be exercised upon notification.