**IC C2E MARKET SURVEY**

|  |
| --- |
| Acquisition Background, Objectives and Overview |
| **Background**  In 2013, the CIA awarded the Commercial Cloud Services (C2S) contract to provide cloud computing services acquired from a large-scale commercial vendor, at up to and including the TOP SECRET (TS)/Sensitive Compartmented Information (SCI) security level, to the Intelligence Community (IC). 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 transformational for the IC – 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.  In 2018, the IC Chief Information Officer confirmed the objective of cloud diversity under Epoch 2 of IC ITE and confirmed CIA as the Executive Agent to acquire enterprise commercial cloud services on behalf of the IC. Commercial Cloud Enterprise (C2E) is the name of the program to expand and enhance the capabilities delivered under C2S. C2E will proceed in two phases. The first phase – the subject of this Market Survey – will acquire foundational cloud services, as defined in the scope section below, from multiple vendors. The second phase will acquire through multiple vehicles specialized Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and multiple cloud management capabilities to augment those acquired in Phase 1. |
| **Phase 1 Scope**  The anticipated scope of the Phase 1 contracts includes the following:   * *Service types:* All types of cloud services (including Infrastructure-as-a-Service (IaaS), PaaS, and SaaS) and associated professional support services * *Security levels:* All security levels including UNCLASSIFIED, SECRET, and TS/SCI with intelligence overlays * *Location:* Worldwide – both terrestrial and satellite/space – with both on- and off-government premises options * *Users:* Supporting all components of the IC and other partners that the components sponsor for use * *Estimated Value:* Tens of billions |
| **Acquisition / Contract Objectives**  The principal C2E Program objective is to acquire cloud computing services directly from commercial cloud service providers with established records for innovation and operational excellence in cloud service delivery for a large customer base.    In support of this program objective, the IC’s objectives for the Phase 1 contracts are as follows:   * *Cloud Service Innovation*. The Provider has documented past performance of implementing new cloud services in its commercial offering that will permit significant advances in support of the intelligence mission when implemented in C2E. * *Technical Parity*. When new cloud services are introduced in the Provider’s commercial environment, the same services become rapidly available in the C2E environment at all security levels as prioritized by the Government. * *Interoperability / Portability*. The Provider has the technical capabilities and management processes to effectively and efficiently facilitate application and data interoperability and portability, as prioritized, between IC cloud environments, including between cloud offerings from different providers. * *Operational Excellence*. The Provider will deliver operational excellence in cloud computing by such elements as scaling quickly to satisfy user computing demands, proactively exceeding IC security requirements, assuring high system availability and data reliability, and providing best-in-class user support. * *Service Pricing Parity*. The Provider provides a range of service pricing structures to cost-effectively support different use cases and revises C2E pricing regularly to maintain parity with the Provider’s commercial environment pricing. * *Superior Contract Management*. The Provider demonstrates the expertise and commitment required to manage a complex effort at the speed of mission that is critically important to the IC and national security. |
| **Type of Procurement**  *Contract Type:* The Government anticipates awarding one or more IDIQ contracts with Firm Fixed Price task orders in Phase 1.  *Period of Performance:*  The Government anticipates a five-year base ordering period with two, five-year optional ordering periods.  *Procurement Schedule*: The Government has set the following draft acquisition milestones for Phase 1:   * Market Survey Responses Due April 8, 2019 * One-on-One Exchanges with Vendors May – June, 2019 * Draft RFP Release January, 2020 * Final RFP Release May, 2020 * Contract Awards CY 2021 |
| **Instructions for Responding to the Survey**  Please respond to the survey questions below in no more than 10 pages. Responses must be posted to the Acquisition Resource Center (ARC) by close of business on April 8.  The Government will review all responses and may invite vendors back for a one-on-one exchange meeting. Please ensure that your market survey response includes contact information to facilitate any feedback.  In addition to responding to the questions, the government will accept white papers providing a more in-depth treatment of issues you deem to be important for this effort. The white papers do not count against the 10 page survey questions response limit, however white papers should not exceed 10 pages.  Responses to the Sponsor’s Market Survey *shall not* contain any propriety information. If a White Paper is submitted, please ensure any proprietary information is *portion marked* appropriately. Please note that any information in white papers marked ‘proprietary’ will be considered by the Sponsor for informational purposes only, and will not be incorporated in the development of the Sponsor’s requirements or acquisition approach unless this information is available to the Sponsor from an unrestricted source.  Please contact Melissa C. at 571-280-4630 or melislm2@ucia.gov with any questions about this market survey. Thanks in advance for your participation in the C2E Market Survey. |

|  |
| --- |
| High-Level Phase 1 Requirements |
| 1. Be a commercial cloud service provider with an established record for innovation and operational excellence in cloud service delivery for a large customer base by industry standards. |
| 1. Have the capability to provide commercial cloud service offerings (IaaS, PaaS, SaaS, etc.) from worldwide locations with off- and on-government premises service delivery options. |
| 1. Provide an extension of enterprise cloud services at tactical edge locations that offers a comprehensive range of services that minimize the loss of cloud capability support for tactical edge missions if network communications is lost. Tactical capabilities shall enable to the maximum extent possible the broad range of cloud services that include IaaS, PaaS and support edge AI/ML use cases. |
| 1. Provide cloud service offerings that can be configured to process data at all security levels including UNCLASSIFIED, SECRET, and TS/SCI with intelligence overlays. |
| 1. Deliver initial operating capability (IOC) cloud service offerings that meet security requirements in all C2E security fabrics within the following timeframes upon conclusion of the contract initiation review:    * UNCLASSIFIED fabric: 30 days    * SECRET fabric: 180 days    * TS/SCI with overlays fabric: 270 days |
| 1. Provide continuous cloud service innovation with a wide variety of offerings in advanced cloud technologies including, but not limited to, artificial intelligence, machine learning, distributed computing (edge, fog, mist), mobile device platform support, high-performance compute, and cloud service automation. |
| 1. Maintain technical parity by instantiating new services - identified by the Government as having IC Mission Priority - within 90 days of commercial availability. New services will be available across all C2E security fabrics. |
| 1. Provide architectural options to ensure continuity of operations across all security fabrics in the event of a disaster disabling a portion of the infrastructure. |
| 1. Deliver cloud service capabilities that effectively and efficiently provide application and data interoperability between IC cloud environments. |
| 1. Provide a marketplace capability to facilitate the use and billing of Bring-Your-Own-License (BYOL) PaaS and SaaS offerings, including those that may be acquired in Phase 2 of C2E. |
| 1. Provide cloud security offerings that proactively ensure protection of the physical infrastructure and information security, and limit and/or mitigate against threats, internally and externally, to the C2E environment. |
| 1. Provide industry-leading Service Level Agreements (SLAs) for cloud service availability, scalability and data reliability that includes significant penalties for failure to meet the established thresholds. |
| 1. Provide C2E service pricing options comparable to the provider’s commercial offering and adjust C2E prices accordingly within one month of changes in the prices of commercial offerings. |
| 1. Provide industry-leading user/management support, including features such as robust documentation, multimode training, cost management tools, flexible/timely utilization/cost reporting, and help desk assistance. |
| 1. Provide professional services to support the use of C2E including, but not limited to, cloud migration projects and expert consulting on cloud architecture, infrastructure, development, integration, and security topics. |
| 1. Provide skilled and experienced personnel with the ability to obtain clearances with clearances appropriate for the security fabric being supported as directed by the government. |
| 1. Provide the capability to transition off of the provider’s cloud infrastructure as required by mission needs and when the contract expires. |

|  |
| --- |
| Survey Questions |

|  |
| --- |
| 1. Does your company plan to propose to perform against Phase I? |
| 1. How large is your commercial cloud business annual revenue (excluding professional services)? and 2) number of customers with at least 100 virtual machines (VMs) in operation at any one time? |
| 1. Which of the requirements may be most difficult/costly for your company to satisfy? What additional information would improve your understanding of these challenging requirements? |
| 1. Describe the capabilities and limitations of your distributed cloud capabilities to edge nodes, some of which are disadvantaged with limited network communications, and intermittent network interruptions? What degree of remote management for edge cloud capabilities exists and what is the degree of parity between the edge node offerings and your enterprise scale services? |
| 1. The Government is pursuing a multiple cloud strategy to increase access to cloud innovation and reduce the disadvantages associated with using a single cloud service provider.   What features of your offering and business approach support application and data interoperability between different Provider’s clouds and portability to facilitate the use of multiple clouds (to include private clouds on USG premises)?  Please provide specific examples of where these features have been applied. |
| 1. What approach do you use for identifying and instantiating innovative new services in your cloud environment? |
| 1. Recognizing that information security is an absolute prerequisite for IC systems, what recommendations do you have to implement the objective of technical parity, as defined above? |
| 1. What resources would you require to supply your cloud computing services from on-government-premises locations? |
| 1. Given your understanding of the intelligence mission, what new features planned near-term and long-term in your technical roadmap for cloud services will be of most value in supporting that mission? |
| 1. The Government is open to teaming arrangements that would support the acquisition objectives. What teaming approaches have you used or are willing to use to support requirements such as those specified for C2E? |
| 1. The Government is interested in your view of the acquisition approach.   What contract type(s) do you believe would be most effective for obtaining the IC’s requirements, as described above, and why?   Based on your commercial experience, how do you recommend customers allocate their requirements between multiple cloud providers?   What ordering process would you recommend the IC consider for task orders in a multiple provider scenario?   What requirements or features of cloud computing services have you found most useful to ensure that data can be moved between different storage providers? And, to ensure that a large set of data can be stored by multiple providers, and accessed seamlessly?   What pricing method would you recommend to facilitate parity between companies’ commercial offerings and the C2E offering?   What steps (contract requirements, procurement process, etc.) do you think would most help the IC to obtain a robust competition for these requirements? |
| 1. Please provide additional comments concerning any aspect of this market survey, including both the requirements and procurement approach. |

|  |
| --- |
| Definitions |

|  |
| --- |
| **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. (NIST) |
| **Bring Your Own License (BYOL).** The ability of a Cloud user to deploy software or platform offerings from the online marketplace into Cloud without additional licensing cost for that software or platform offering because the Cloud user already possesses a valid license from a separate contracting action. (JEDI cloud contract) |
| **Edge Computing.** A distributed computing paradigm in which computation is largely or completely performed on distributed edge nodes. (European Telecommunications Standards Institute (ETSI)) |
| **Fog Computing.** A layered model for enabling ubiquitous access to a shared continuum of computing resources. (NIST) |
| **Infrastructure as a Service (IaaS).** The capability provided to the consumer is 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. (NIST) |
| **Interoperability.** Ability to process data using different services on different cloud systems through common specifications. (NIST) |
| **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. (NIST) |
| **On-Government Premises.** The physical infrastructure providing cloud services is located on government property. (C2E PMO) |
| **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 and tools supported by the provider. (NIST) |
| **Portability.** Ability to move data from one cloud system to another and have the ability to port and run on different cloud systems at an acceptable cost. (NIST) |
| **Software as a Service (SaaS).** The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. (NIST) |