# **REQUEST FOR INFORMATION**

**IMMIGRATION CUSTOMS ENFORCEMENT**

Description

United States Immigration and Customs Enforcement’s (ICE) mission is to bring a unified and coordinated focus to the enforcement of federal immigration and customs laws. ICE resources are used to combat terrorism, protect our Nation’s borders, deter illegal immigration, protect intellectual property rights, and combat human trafficking and smuggling. ICE accomplishes these missions by investigating, detaining, and prosecuting criminals and aliens who pose a risk to national security and public safety. To support the agency mission, the ICE Office of the Chief Information Officer (OCIO) is dedicated to delivering innovative information technology (IT) and business solutions that enable ICE to support its mission. OCIO works to ensure that the IT enterprise architecture is in place to provide ICE with full IT capabilities including disaster recovery, cyber security, IT operations, IT systems development, and engineering.

Background

ICE in support of the OCIO has an important role in providing a service to governance the migration of all data and capabilities of current and future services that support mission infrastructure from DHS owed data centers to cloud computing services based on government preference. This service will be available within the government cloud provided by private sector in support of a capability at a lower cost with the same or comparable security.

ICE is seeking industry feedback on available cloud-based capabilities, services and solutions to achieve Information Technology (IT) efficiencies, reliability, interoperability, and improvement in secure end-to-end performance through acquisition of commercially available cloud service providers. This Request for Information (RFI) invites industry to submit information, comments, capabilities, and recommendations for potential development and implementation of near-term acquisition vehicles and corresponding business models to facilitate ICE Enterprise Cloud Service functions as well as maintain partnerships as resellers.

ICE envisions using cloud computing services and finding a provider of cloud services that offers partnerships in reselling services that present an array of options, such as Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) offerings within a FedRAMP certified datacenter that already has capabilities of approved network connections into DHS OneNet. The provider must be able to support ICE defined requirements for business relationships, supporting interfaces, providing capacity, networking and connectivity, security, information assurance and authentication and authorization.

Requested Information

     ICE wishes to obtain feedback from potential providers about (a) their ability to meet these conformance requirements, (b) their interest in acting as providers and (c) any requirement deemed by the provider to be sufficiently difficult that it would prevent the potential provider from participating.

Please answer the following Questions:

1. Please provide following: name and address of firm, size of business; average annual revenue for past 3 years and number of employees; ownership; whether they are large, small, small disadvantaged, 8(a), Woman-owned, Veteran Owned, Service Disabled Veteran Owned, Historically Underutilized Business Zone and Historically Black Colleges and Universities)/Minority Institutions; number of years in business; affiliate information: parent company, joint venture partners, potential teaming partners, prime contractor (if potential sub) or subcontractors (if potential prime); list of customers covering the past five years (highlight relevant work performed, contract numbers, contract type, dollar value of each procurement; and point of contact - address and phone number).
2. Please state if the company is a current holder of any GWACs or MAS (GSA, NASA, etc).

1. Please provide a copy of your standard Cloud Brokerage Agreement or certification for the following:

* Microsoft Reseller as a Direct CSP Partner
* Microsoft Reseller as an Indirect CSP Partner
* Microsoft Azure Silver Cloud Platform (or Higher)
* Microsoft Partner Network (MPN) Organization Partner ID
* Amazon AWS Channel Reseller
* Amazon AWS GovCloud Reseller
* Amazon AWS Public Sector Partner Program
* Advanced Amazon Partner Network (APN) Partner ID

1. Using the NIST cloud definition, describe the cloud management services offered by your company and the corresponding cloud service delivery models.
2. What are the financial, legal, and operational advantages and disadvantages of CSP as a reseller of cloud services and cloud service delivery models? Are there unique issues about each which we should be aware of as a customer?
3. Please summarize your past performance offerings with SaaS, PaaS and IaaS and what cloud services were they with?
4. Describe how your company supports these essential cloud characteristics, as defined by NIST: On Demand Self-Service, Broad Network Access, Rapid Elasticity, Resource Pooling, and Measured Service.
5. Describe your relationship, if any, with the ICE and the licensing implications for the Department of Homeland Security. What issues, if any, would limit ICE’s ability make use of your CSP offerings or delivery models?
6. Please provide a copy of your standard Service Level Agreement (SLA), or equivalent.
7. Please highlight any unique strategies or capabilities that you would provide to make our initiative successful.
8. How does your company address information assurance for data and privacy concerns of individuals; identify and address potential privacy risks, and responsibilities that result from data placed in the cloud environment? Specifically, address the following:

* Compliance with the Privacy Act of 1974
* Personally Identifiable Information (PII)
* Controlled Unclassified Information (CUI)
* Protected Health Information (PHI)
* International Traffic in Arms Regulation (ITAR)
* Certification of the following security enclaves under your control:
  + Commercial Unclassified
  + Commercial Private Unclassified

1. Describe the Cloud Service Provider’s (CSP) ability to encrypt data and software at rest and in transit from current location to the appropriate cloud provider. Describe your ability and processes to participate in data recovery and if working with the government in providing forensics, how would you perform this?

1. Describe suggestions and recommendations you can provide to development teams implementing (“on boarding”) solutions in the cloud, including consulting, engineering, design, testing, acceptance and cutover. What guidelines can you provide to assist the customer in project planning (level of effort, timeline, decommissioning legacy services, etc.)?

1. Describe recommendations for protecting and transitioning a customer's data in case of contract termination (“off boarding”) or contract renewal with another vendor.
2. Please explain any application and data portability considerations (i.e., exit strategy for applications running the cloud).
3. Describe the process you would utilize to convert a customer from an existing account with another reseller over to your account. Also, provide the same process for moving a Microsoft enrollment from another reseller to your company. Be sure to describe the time to transfer, the steps and activities required to perform the transfer and how you will ensure no impact to existing ICE resources will occur.
4. Describe your Customer Relationship Management (CRM) process as a CSP reseller in a brokered service environment.
5. Please discuss your model for providing customer support, including charges for support contacts.
6. Describe your incident/problem reporting and tracking systems that reflects between you and the CSP and the ability for authorized ICE government staff to access those systems directly.
7. What types of access does your customer support have between you and the CSP?
8. What level of automatic alerting can you provide to ICE staff in the event of failure, degraded service, or exceeding planned utilization?
9. Describe your mitigation strategies for potential availability and performance issues such as network outages, bandwidth shortages, or spikes in service demand.
10. Describe the redundancy features of cloud services that ensure availability and performance.
11. Discuss your roles and responsibilities for system maintenance as the service provider and the maintenance roles and responsibilities that the user is expected to assume. Please include information about your procedures for operating system and other core software upgrades, patches, and service pack application. Please provide the past quarter’s availability statistics for cloud services that you feel may be appropriate for this initiative.
12. Discuss how you provide cloud services for scalability of customer applications and data hosted in cloud environment.
13. The level of security the Agency determines a CSP must meet will vary. Using NIST Special Publication 800-53 (as revised) and NIST Publication 800-137 as a framework, discuss your company’s and your CSP’s compliance with NIST for service offerings or allow for ICE to perform the following with respect to:

* Monitoring
* Incident Response
* Key Escrow
* Forensics
* Two-Factor Authentication (Integration with ICE Identity and Access
* Management (IdAM) Services
* Audit
* Failover
* Configuration Management
* Change Control
* Information Sharing

1. Describe your approach to addressing IT security challenges in cloud computing, in particular, dealing with hacker attacks, the potential for unauthorized access, and inappropriate use of proprietary data and IT applications.
2. What are your processes and solutions for preventing these challenges from occurring?
3. What controls are in place for administrative access, both internal to your company and for administrative access from government clients? Please include discussion of administrator controls over provisioning.
4. Operations Management, describe how you will integrate with ICE as the CSP Broker to deliver:
   1. Service Level Management- Provide a framework by which services are defined, service levels required to support business processes are agreed upon, SLAs and Operational Level Agreements (OLAs) are developed to satisfy the agreements and costs of services.
   2. Incident Management- Interact with ICE incident management process as well as restore on IT service to normal state operations as quickly as possible.
   3. Problem Management- Prevent incidents from happening or minimize their impacts by identifying their root causes.
   4. Event Management- Manage operational events and communicate them to appropriate parties for further action.
   5. Access Management- Ensure only authorized users are allowed access to services.
   6. Request Fulfillment- Manage the lifecycle of all service requests.
   7. Service Desk- as the Single Point of Contact as the CSP and the government. A typical Service Desk manages Incidents and Service Requests with government process, and also handles communication with the users. How will you integrate your service desk with the ICE or CSP service desk(s)?
   8. Information Security Management- Ensure organizational information is evaluated, risks assessed, and appropriate policies to control access and dissemination are put in place that meet regulatory agency requirements, such as Health Insurance Portability and Accountability Act (HIPAA).
   9. IT Service Continuity Management- Ensure plans and alternative service options are in place to meet business continuity management needs in the event of a significant business outage or disruption per government standards.
5. As anomalies in operational infrastructure occur, how do you propose to support relationships with ICE and CSP?
6. ICE requires the ability to monitor information systems for availability. Describe how you will integrate your availability monitoring systems as the CSP.
7. ICE relies on information systems to execute missions. Systems regularly must be updated or taken offline for maintenance.
8. Describe how you will interact with the ICE as the CSP when such maintenance or authorized service interruptions must occur.
9. Do you have dashboards, scorecards, or portals that ICE government staff can access? Please describe them and any costs associated with them. If so, what type of information does this provide?

Pricing

1. Describe your pricing models and other relevant pricing factors such as consulting, engineering, hardware, VM, CPU, memory, storage, bandwidth, Continuity of Operations (COOP), Disaster Recovery (DR), and data transfers. Include break points for price changes and prices for transition services. Please be certain bandwidth charges for uploading and downloading data are clearly described.
2. Describe your pricing model for loading data on a recurring basis and for transaction processing.
3. Describe your pricing model for on-demand extraction of data by third parties and any approaches that would control cost for the consumer.
4. Describe the pricing differences for non-volatile data that requires only restore rather than recovery capability.
5. Please add any additional financial information that would be useful in evaluating the suitability of your cloud services.

­­

Definitions

The National Institute of Standards and Technology (NIST) define 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.”*[[1]](#footnote-1)

While the Agency has acknowledged and adopted the NIST definition above, in implementation cloud computing for the ICE is complex and multifaceted and includes the use of private and public clouds, technologies that enable data center consolidation, automated cloud service provisioning, and the enterprise offering of cloud services, such as infrastructure, platform, and software services, to a worldwide community of ICE consumers.

The following terms are working definitions for concepts referenced in this RFI:

**NIST Cloud Computing Standards** – The National Institute of Standards and Technology (NIST) publishes guidance and standards for agencies to follow when procuring cloud and other technologies. These publications address, for example, security, interoperability, and portability. NIST Special Publication 500-291, NIST Cloud Computing Roadmap, presents these standards in the context of the NIST Cloud Computing Reference Architecture using the NIST taxonomy in NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture.

**Committee on National Security Systems (CNSSI) Instructions** – These instructions include technical or implementation guidelines, restrictions, doctrines, and procedures applicable to information assurance. All instructions are binding upon all U.S. Government departments and agencies. ICE CNSSI -1253, Security Categorization and Control Selection for National Security Systems (current version), presents the standards by which NIST 800-53 security controls will be implemented for National Security Systems.

**Federal Information Security and Management Act (FISMA)** – The **Federal Information Security Management Act of 2002** ("**FISMA**", [44 U.S.C.](http://encyclopedia.thefreedictionary.com/Title+44+of+the+United+States+Code) [§ 3541](http://www.law.cornell.edu/uscode/44/3541.html), *et seq.*) is a United States federal law enacted in 2002 as Title III of the [E-Government Act of 2002](http://encyclopedia.thefreedictionary.com/E-Government+Act+of+2002) ([Pub.L. 107-347](http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html), 116 [Stat.](http://encyclopedia.thefreedictionary.com/United+States+Statutes+at+Large) 2899). The act recognized the importance of [information security](http://encyclopedia.thefreedictionary.com/Information+security) to the economic and national security interests of the United States.[[1]](http://encyclopedia.thefreedictionary.com/Federal+Information+Security+Management+Act+of+2002#cite_note-nist_overview-0) The act requires each [federal agency](http://encyclopedia.thefreedictionary.com/Government+agency#Government_agencies_in_the_United_States) to develop, document, and implement an agency-wide program to provide [information security](http://encyclopedia.thefreedictionary.com/Information+security) for the information and [information systems](http://encyclopedia.thefreedictionary.com/Information+systems) that support the operations and assets of the agency, including those provided or managed by another agency, [contractor](http://encyclopedia.thefreedictionary.com/Government+contractor), or other source.[[](http://encyclopedia.thefreedictionary.com/Federal+Information+Security+Management+Act+of+2002#cite_note-nist_overview-0)

**Federal Risk and Authorization Management Program (FedRAMP) –** The FedRAMP assessment process is initiated by agencies or cloud service providers (CSPs) beginning a security authorization using the FedRAMP requirements which are FISMA compliant and based on the NIST 800-53 rev4 and initiating work with the FedRAMP PMO.

**Personally Identifiable Information (PII)** – Information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is lined or linkable to a special individual. <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>

**Controlled Unclassified Information (CUI)** –Information in categories such as For Official Use Only (FOUO), Sensitive But Unclassified (SBU) and Law Enforcement Sensitive (LES) categories.

**Protected Health Information (PHI)** – Information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

**International Traffic in Arms Regulation (ITAR)** – A set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML).

**Privacy Act of 1974** – The Privacy Act establishes a wide range of privacy protection for covered Federal records in which information about an individual is retrieved by name or other personal identifier. See FAR Subpart 24-1, Protection of Individual Privacy; FAR 52.224-1 – 52-224-2 (2010).

**Service Models** – The NIST has defined three cloud computing services models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). See NIST Special Publication 800-145. These service models are summarized as follows:

**Infrastructure:** the provision of processing, storage, networking and other fundamental computing resources;

**Platform:** the deployment of applications created using programming languages, libraries, services, and tools supported by a cloud provider; and

**Software:** the use of applications running on a cloud infrastructure environment.

**Service Level Agreement (SLA)** – Agreements which are under the umbrella of the overall cloud computing contract between a CSP and a Federal agency. SLAs define acceptable service levels to be provided by the CSP to its customers in measurable terms.

Industry Discussions

ICE representatives may or may not choose to meet with potential offerors. Such discussions would only be intended to get further clarification of potential capability to meet the requirements, especially any development and certification risks. Any meetings with potential offerors during the market research process do not commit the Government in any way and are only for the purpose information gathering.

1. [↑](#footnote-ref-1)