SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: On Individual Orders

PAGE 1 OF 2

2. CONTRACT NO. 70SBUR19A00000012

3. AWARD/ EFFECTIVE DATE

4. ORDER NUMBER

5. SOLICITATION NUMBER 70SBUR19Q00000040

6. SOLICITATION ISSUE DATE 03/20/2019

7. FOR SOLICITATION INFORMATION CALL: a. NAME EMILIO CIBULA b. TELEPHONE NUMBER *(No collect calls)* 802-872-4640

8. OFFER DUE DATE/LOCAL TIME ET

9. ISSUED BY CODE CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR □ SET ASIDE: % FOR:
□ SMALL BUSINESS
□ HUBZONE SMALL BUSINESS
□ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
□ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
□ EDWOSB
□ 8(A)
NAICS:
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED □ SEE SCHEDULE

12. DISCOUNT TERMS As Indicated On Each Call

13a. □ THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION ☒ RFQ □ IFB □ RFP

15. DELIVER TO CODE

As Indicated On Each Call

16. ADMINISTERED BY CODE CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

17a. CONTRACTOR/ OFFEROR CODE 9570508830000 FACILITY CODE

GOVPLACE
[redacted]
11111 SUNSET HILLS RD
SUITE 200
RESTON VA 201905373

TELEPHONE NO. [redacted]

□ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE

As Indicated On Each Call

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED □ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	GSA Contract #: GS-35F-0179X DUNS Number: 957050883+0000 ----------- USCIS Commercial Cloud Hosting BPA ----------- PSC: D305 BASE CLIN 0001 for USCIS Cloud Hosting (IaaS/PaaS, and SaaS) POP: 07/30/2019 - 07/29/2020				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA
As Indicated On Each Call

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* $0.00

□ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA □ ARE □ ARE NOT ATTACHED.

□ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA □ ARE □ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: Govplace Quotation OFFER DATED 06/16/2019. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

[redacted]

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
Salvatore Saraceno

31b. NAME OF CONTRACTING OFFICER *(Type or print)* SALVATORE SARACENO

31c. DATE SIGNED 16 Jul 2019

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Firm Fixed Price (FFP) - Fixed Unit Price (FUP) Option Year CLIN 1001 for USCIS Cloud Hosting (IaaS/PaaS, and SaaS) POP: 07/30/2020 - 07/29/2021 Firm Fixed Price (FFP) - Fixed Unit Price (FUP) Option Year CLIN 2001 for USCIS Cloud Hosting (IaaS/PaaS, and SaaS) POP: 07/30/2021 - 07/29/2022 Firm Fixed Price (FFP) - Fixed Unit Price (FUP) Option Year CLIN 3001 for USCIS Cloud Hosting (IaaS/PaaS, and SaaS) POP: 07/30/2022 - 07/29/2023 Firm Fixed Price (FFP) - Fixed Unit Price (FUP) AAP Number: N/A Period of Performance: 07/30/2019 to 07/29/2023 Sections: Section I - Line Item Structure, Clauses, and Additional BPA Requirements Section II - Description of Requirement Section III - [redacted] [redacted]				

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: ____________________

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MA LING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MA L OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

□ PARTIAL □ FINAL

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

□ COMPLETE □ PARTIAL □ FINAL

37. CHECK NUMBER

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

41b. SIGNATURE AND TITLE OF CERTIFY NG OFFICER

41c. DATE

42a. RECEIVED BY *(Print)*

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

Line Item Structure

The estimated total NTE amount of the BPA is $109,747,689.10 and the estimated base period NTE amount is $23,833,676. The government understands cloud hosting is an IT consumption-based service; therefore, monthly invoices will fluctuate based on government usage along with fixed unit price (FUP) fluctuations from commercial cloud hosting services. The contractor shall be responsible for invoicing the government at the most current market prices from the commercial cloud hosting service on an hourly basis (including any discount quoted at time of award) for the duration of the BPA, to include any promotional pricing. In addition, at no point shall the contractor exceed its GSA Schedule rates. The government will verify the invoicing is accurate with current market rates using CloudCheckr, a third party cost-tracking tool.

The contractor shall track the spend rates to ensure the government does not exceed the NTE amounts on each CLIN. Should the NTE amount be expended, the government reserves the right to modify the BPA to satisfy the increased need.

BPA Clauses

This BPA is subject to the terms and conditions of the GSA Schedule Contract.

Federal Acquisition Regulation (FAR) Clauses incorporated by reference

52.252-2 **Clauses Incorporated by Reference** (Feb 1998)
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses: http://www.acquisition.gov/far.

(End of clause)

Federal Acquisition Regulation (FAR) clauses incorporated by reference

FAR 52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)
FAR 52.204-2	Security Requirements (AUG 1996)
FAR 52.204-4	Printed/Copied Double-Side on Postconsumer Fiber Content Paper (MAY 2011)
FAR 52.212-4	Alternate 1- Contract Terms and Conditions – Commercial items (JAN 2017)
FAR 52.224-1	Privacy Act Notification (APR 1984)
FAR 52.224-2	Privacy Act (APR 1984)
FAR 52.232-39	Unenforceability of Unauthorized Obligations (JUN 2013)
FAR 52.237-3	Continuity of Services (JAN 1991)
FAR 52.242-13	Bankruptcy (JUL 1995)

Federal Acquisition Regulation (FAR) Clauses incorporated in full text

52.217-9 **Option to Extend the Term of the Contract** (Mar 2000)

(a) The government may extend the term of this contract by written notice to the contractor within **15 days of BPA expiration**; provided that the government gives the contractor a preliminary written notice of its intent to extend at least **30 days** before the contract expires. The preliminary notice does not commit the government to an extension.

(b) If the government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **48 months**.

(End of clause)

52.224-3 **Privacy Training – Alternate I (DEVIATION)**

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

52.232-40 **Providing Accelerated Payment to Small Business Subcontractors** (Dec 2013)

(a) Upon receipt of accelerated payments from the Government, the contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

52.252-4 **Alterations in Contract** (Apr 1984)

Portions of this contract are altered as follows:

Use of the word “contract” is understood to mean “Blanket Purchase Agreement” wherever such application is appropriate. Use of the word “solicitation” is understood to mean “Request for Quote” wherever such application is appropriate.

(End of clause)

52.252-6 **Authorized Deviations in Clauses** (Apr 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(b) The use in this solicitation or contract of any clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) Clauses incorporated by reference

The full text of HSAR clauses and provisions may be accessed electronically at the following internet address: www.acquisition.gov

3052.203-70	**Instructions for Contractor Disclosure of Violations**	(Sep 2012)
3052.205-70	**Advertisements, Publicizing Awards, and Release**	(Sep 2012)
3052.242-72	**Contracting Officer's Representative**	(Dec 2003)

Homeland Security Acquisition Regulation (HSAR) Clauses incorporated in full text

3052.204-71 **Contractor Employee Access, Alternate I** (Sep 2012)
(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:
(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting

Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

Safeguarding Of Sensitive Information (Mar 2015)
(HSAR Class Deviation 15-01)
(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the

sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS*

Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

Information Technology Security and Privacy Training (Mar 2015)
(HSAR Class Deviation 15-01)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer’s Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

General Services Administration Regulation (GSAR) Clauses incorporated in full text

552.238-82 Special Ordering Procedures for the Acquisition of Order-Level Materials (Jan 2018)

(a) Definitions.

“Order-level materials” means supplies and/or services acquired in direct support of an individual task or delivery order placed against a Federal Supply Schedule (FSS) contract or

FSS blanket purchase agreement (BPA), when the supplies and/or services are not known at the time of Schedule contract or FSS BPA award. The prices of order-level materials are not established in the FSS contract or FSS BPA. Order-level materials acquired following the procedures in paragraph (d) are done so under the authority of the FSS program, pursuant to 41 U.S.C. 152(3), and are not open market items, which are discussed in FAR 8.402(f).

(b) FAR 8.403(b) provides that GSA may establish special ordering procedures for a particular FSS.

(c) The procedures in FAR subpart 8.4 apply to this contract, with the exceptions listed in this clause. If a requirement in this clause is inconsistent with FAR subpart 8.4, this clause takes precedence pursuant to FAR 8.403(b).

(d) Procedures for including order-level materials when placing an individual task or delivery order against an FSS contract or FSS BPA.

(1) The procedures discussed in FAR 8.402(f) do not apply when placing task and delivery orders that include order-level materials.

(2) Order-level materials are included in the definition of the term “material” in FAR clause 52.212-4 Alternate I, and therefore all provisions of FAR clause 52.212-4 Alternate I that apply to “materials” also apply to order-level materials. The ordering activity shall follow procedures under the Federal Travel Regulation and FAR Part 31 when order-level materials include travel.

(3) Order-level materials shall only be acquired in direct support of an individual task or delivery order and not as the primary basis or purpose of the order.

(4) The value of order-level materials in a task or delivery order, or the cumulative value of order-level materials in orders against an FSS BPA awarded under a FSS contract shall not exceed 33.33%.

(5) All order-level materials shall be placed under the Order-Level Materials SIN.

(6) Prior to the placement of an order that includes order-level materials, the Ordering Activity shall follow procedures in FAR 8.404(h).

(7) To support the price reasonableness of order-level materials,

(i) The contractor proposing order-level materials as part of a solution shall obtain a minimum of three quotes for each order-level material above the simplified acquisition threshold.

(A) One of these three quotes may include materials furnished by the contractor under FAR 52.212-4 Alt I (i)(1)(ii)(A).

(B) If the contractor cannot obtain three quotes, the contractor shall maintain its documentation of why three quotes could not be obtained to support their determination.

(C) A contractor with an approved purchasing system per FAR 44.3 shall instead follow its purchasing system requirement and is exempt from the requirements in 552.238-82(d)(7)(i)(A)-(B).

(ii) The Ordering Activity Contracting Officer must make a determination that prices for all order-level materials are fair and reasonable. The Ordering Activity Contracting Officer may base this determination on a comparison of the quotes received in response to the task or delivery order solicitation or other relevant pricing information available.

(iii) If indirect costs are approved per FAR 52.212-4(i)(1)(ii)(D)(2) Alternate I), the Ordering Activity Contracting Officer must make a determination that all indirect costs approved for payment are fair and reasonable. Supporting data shall be submitted in a form acceptable to the Ordering Activity Contracting Officer.

(8) Prior to an increase in the ceiling price of order-level materials, the Ordering Activity Contracting Officer shall follow the procedures at FAR 8.404(h)(3)(iv).

(9) In accordance with GSAR clause 552.215-71 Examination of Records by GSA, GSA has the authority to examine the Contractor's records for compliance with the pricing provisions in FAR clause 52.212-4 Alternate I, to include examination of any books, documents, papers, and records involving transactions related to the contract for overbillings, billing errors, and compliance with the IFF and the Sales Reporting clauses of the contract.

(10) OLMs are exempt from the following clauses:

(i) 552.216-70 Economic Price Adjustment - FSS Multiple Award Schedule Contracts.
(ii) 552.238-71 Submission and Distribution of Authorized FSS Schedule Pricelists.
(iii) 552.238-75 Price Reductions.

(11) Exceptions for travel.

(i) Travel costs are governed by FAR 31.205-46 and therefore the requirements in paragraph (d)(7) do not apply to travel costs.

(ii) Travel costs do not count towards the 33.33% limitation described in paragraph (d)(4).
(iii) Travel costs are exempt from clause 552.238-74 Industrial Funding Fee and Sales Reporting.

(End of clause)

Additional BPA Requirements

C-1. ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR Part 52.212-4(g), all invoices submitted to USCIS for payment shall include the following:

(1) Name and address of the contractor.
(2) Invoice date and invoice number.
(3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
(4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.
(5) Shipping and payment terms.
(6) Name and address of contractor official to whom payment is to be sent.
(7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
(8) Taxpayer Identification Number (TIN).

(b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

(d) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495
(802) 288-7600

C-2. PERFORMANCE REPORTING

The government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor will need to enroll at www.cpars.gov to participate in this process.

C-3. POSTING OF ORDER IN FOIA READING ROOM

(a) The government intends to post the order resulting from this notice to a public FOIA reading room.

(b) Within 30 days of award, the contractor shall submit a redacted copy of the executed order (including all attachments) suitable for public posting under the provisions of the

Freedom of Information Act (FOIA). The contractor shall submit the documents to the USCIS FOIA Office by email at **foiaerr.nrc@uscis.dhs.gov** with a courtesy copy to the contracting officer.

(c) The USCIS FOIA Office will notify the contractor of any disagreements with the contractor's redactions before public posting of the contract or order in a public FOIA reading room.

C-4. FINAL PAYMENT

As a condition precedent to final payment, a release discharging the government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out of or under this order shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

C-5 SCOPE

This requirement is for commercially available cloud hosting, an information technology (IT) consumption-based service. This requirement includes Infrastructure as a Service (IaaS) / Platform as a Service (PaaS) and Software as a Service (SaaS). The current requirement is based on historical usage, but it is reasonably expected that the usage of this service will continue to grow. The scope of this requirement includes new IaaS / PaaS and SaaS offerings that meet the DOR requirements, as they become available on the contractor's GSA Federal Supply Schedule.

C-6 CONTRACTOR TEAM ARRANGEMENT (CTA)

CTAs are permissible under this RFQ and shall be specifically identified as such. Offerors shall submit a copy of the CTA document if quoting a CTA. This document shall address the items listed under "Elements of a CTA Document" which is accessible through the link http://www.gsa.gov/contractorteamarrangements.

C-7 TECHNOLOGY REFRESH – NEW ITEMS

Based on the underlying GSA Schedule contract(s), the BPA issued as a result of this RFQ may be modified to include items (services or software) if the following conditions are met:

1) The items are within the scope of the BPA as solicited;
2) The items are commercially available;
3) The items are approved through the FedRamp process or eligible for an agency ATO, (if applicable); and
4) The items are on the underlying GSA Schedule contract(s).

The Contracting Officer may issue a "Tech Refresh" modification to add relevant items that are on the GSA Schedule contract(s) and to delete items that are no longer available. Tech Refresh modifications may be issued each quarter of the BPA year, or sooner, if USCIS requires an item that is not currently offered under these BPAs. Item pricing shall be at discounts from Schedule list price equal to or better than the discounts for items already on the BPA, or for items being replaced.

Description of Requirements (DOR)

1. Title of Project

The U.S. Citizenship & Immigration Services (USCIS) Office of Information Technology has a continued requirement for a reseller to provide access to FedRAMP Authorized true On-Demand Commercial Cloud Service Providers (CCSP's) for our Commercial Cloud Hosting Services (CCHS). This includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

2. Background

USCIS has built and is currently operating 26 major mission critical systems that are being hosted in the Amazon Web Services (AWS) commercial cloud. These applications are deployed in AWS and designed to leverage programmatic provisioning capabilities offered by the AWS commercial cloud.

This requirement supports the delivery of USCIS systems via Continuous Integration/Continuous Delivery (CI/CD) DevOps methodologies for building quality software that is developed, built, tested and implemented into production quickly and in rapid succession using the CI/CD pipeline.

USCIS programs and systems supported by this DOR serve both public and private stakeholders and can range broadly in terms of size, complexity and importance. In order to support this architecture in CCSP's, USCIS requires a true on-demand secure, scalable, flexible, automated and cost effective cloud computing environment that provides a developer access to Web Graphical User Interface (GUI) Console and Application Programming Interfaces (APIs) to programmatically provision all hosting services, hardened images, formation templates, auto scaling of infrastructure, large scalable databases as a service, large scalable storage as a service, development services, monitoring services, containerization services, automated configuration control services, and automated scalable networks services that provide for rapid provisioning and de-provisioning of entire system environments in minutes.

3. Scope

USCIS requires reseller services to access multiple FedRAMP Authorized true on-demand CCSP's. The scope of this Blanket Purchase Agreement (BPA) includes the ability to access new CCSP's as they become FedRAMP Authorized and available through the reseller. The access provided by this BPA shall support USCIS' CI/CD DevOps Information Technology (IT) systems development model and provide SaaS options. The types of cloud services required by this BPA are IaaS, PaaS and SaaS (see definitions section for additional details). The BPA is for reseller services only to provide access to and a payment mechanism for consumption based true On-demand Commercial Cloud service providers. Any services are administrative only as described in the DOR for providing the unfettered access and assisting in any service outages or issues with the CCSP's. Development, migration, or managed service provider services are not part of this procurement and will not be considered if proposed.

This BPA shall include access to the AWS US East/West CCSP to continue to host existing USCIS systems that are currently deployed in AWS (approximately 85% of the total requirement). This BPA shall also include access to at least one other FedRAMP Impact Level Moderate, FedRAMP Authorized true on-demand IaaS/PaaS CCSP and at least one FedRAMP Impact Level High, FedRAMP Authorized, true on-demand IaaS / PaaS CCSP that meets the salient characteristics listed below. Additionally, this

BPA shall include access to several different SaaS options, including at least one SaaS option that meets the salient characteristics listed for each of the SaaS offerings identified in Section 4.2. The scope of this BPA encompasses the ability to add additional SaaS requirements as needed.

The decision about where to place new programs, systems and IT capabilities being implemented by the agency, and additional legacy information systems migrating to cloud based IT support models, will be made by the government based on an analysis of the technical architecture and cost effectiveness of each CCSP, depending on the system.

4. Systems Requirements

All services shall be provided by a consumption based True On-demand Commercial Cloud Service Provider which provides real-time hardware resources to support the Governments virtual infrastructure without any need to estimate or procure those hardware resources. The hardware resources underlying the virtual infrastructure shall become available in real time at the launch of the virtual instance and the virtual instances shall be billed in increments no larger than one hour. There shall be no requirement for any interaction between the contractor and the USCIS DevOps teams in order to configure any of the infrastructure and platform cloud services and the hardware to operate those resource shall be instantly available to support the performance specifications for that service. For example, there shall be no ticketing system to a third party to configure the infrastructure. The DevOps teams shall have direct access to the GUI and API to launch and configure resource instances, and these resource instances shall be available within 5 minutes after the DevOps Teams execute script API calls, via automated infrastructure code that executes API calls, or initiating the configuration from the GUI console.

a) Scalability – Each CCSP shall be both horizontally and vertically scalable to two thousand virtual instances in less than 10 minutes. It shall support hundreds of petabytes of storage, a minimum of six terabytes of storage for databases, and be able to scale across two or more data centers as a selectable option in the API or web console.

b) Reliability – Each CCSP shall provide redundancy across multiple data centers, geographically dispersed from each other, to prevent natural and man-made disasters from impacting operational status. All services shall be scaled over multiple data centers and provide for real-time automatic failover without interruption to the service the systems are supporting, should a disaster occur. Launching resources in multiple data centers shall be a selectable option within the API and web console.

c) Availability – Each CCSP shall provide a minimum availability level of 99.9% for each of their services unless otherwise stated for a particular service. And each service shall meet their commercially advertised Service Level Agreements (SLA's). Resources launched in multiple data centers shall continue to operate and be available when one of the data centers is offline for 100% uptime redundancy.

d) Direct Access to the Console and APIs – Each CCSP shall provide for direct and unfettered access to the cloud management and configuration console and APIs by Government personnel to control all the resources and configuration within the cloud.

e) Cloudcheckr (brand name) Integration – All IaaS and PaaS clouds must be integrated with the Cloudcheckr cloud reporting tool as this is how the Government manages its cloud environments for cost, configuration management, and security compliance.

f) Twilio (brand name) Third Party Messaging Service – USCIS requires Twilio, a three tiered authentication mechanism to validate and verify an end user's identity. The authentication shall be done through the (1.) username, (2.) password, and a (3.) security code transmitted to the user via text message, email, or voicemail.

4.1 IaaS and PaaS True On-Demand Commercial Cloud Services – In order to support USCIS's objective and architectures and provide cloud diversity, the contractor shall provide three or more CCSP's for the IaaS and PaaS offerings. All offerings must be FedRAMP Authorized and FedRAMP Impact Level moderate at a minimum; additionally, at least one offering must be FedRAMP Impact Level high. Each offering shall include **<u>all</u>** of the following services:

4.1.1 Virtual Compute Service (VCS) –Virtual compute resources shall be configurable in real-time. In addition, VCS's must:

a) Be able to instantiate and resize on demand without the need to rebuild the virtual instance,
b) Provide scalable, on demand sizing to support additional load or reduction in load via programmatic scripting through an API.
c) Allow the automated configuration of memory, CPU, instance storage, and the boot partition size that is optimal for the Government's choice of operating system and application. The VCS shall support the latest versions of operating systems such as Red Hat Linux, Ubuntu Linux, CentOS Linux, and Microsoft Windows Server 2012 or newer. These shall be updated over the life of the BPA as new operating system technologies emerge and are supported by each CCSP'.

4.1.2 Scaling Automation Service (SAS) – Each CCSP shall provide a Virtual Computer scaling service that provides for programmatic launching and shutdown of compute instances based on load of the instances in the compute pool. Load shall be based on an increase or decrease in processor or memory utilization of a period of time to trigger the launch or shutdown action.

4.1.3 Database Management Services (DBMS) – Each CCSP shall provide a minimum of three database services that do not require any management or administration on the part of the customer (USCIS) for the underlying DBMS. It shall provide for automatic backups that can be configured by the user to save the data in cloud storage for data recovery purposes in the event of a system failure. All database configuration commands and options shall be available via the GUI or API.

4.1.3.1 Relational Database Services (RDS) – Each CCSP shall provide a highly available relational database service for large scalable databases without USCIS having to manage the servers or DBMS. This service must be geographically redundant over more than 500 miles. The database creation, modification, deletion and management on this service must be available via API's and scale on demand to 20000 IOPS and 6 TB. The RDS shall provide a minimum of two of the following databases: Oracle, MySQL, PostgreSQL, and Microsoft SQL Server.

4.1.3.2 NoSQL (NSDS) – Each CCSP shall provide a fast and flexible NoSQL database service for applications that need consistent, single-digit millisecond latency at any scale. It shall be a fully managed cloud database that supports both document and key-value store models. It shall provide a flexible data model, reliable performance, and automatic scaling of throughput capacity, providing response times from milliseconds to microseconds up to millions of requests per second.

4.1.3.3 Data Warehouse Service (DWS) – Each CCSP shall provide a fully managed, petabyte-scale data warehouse service in the cloud, which allows for a100GB of data to stability and the ability to scale to a petabyte or more. This service shall allow the user to run Business Intelligence tools against the data source to use the data to acquire new insights for the business. Complex query datasets shall be returned within minutes using SQL based tools to analyze the data.

4.1.4 Storage – All storage shall be highly available and replicated automatically across multiple data centers to prevent outages or loss of data.

4.1.4.1 Scalable Block Storage (SBS) – Each CCSP shall provide persistent high speed, low latency block storage for the virtual compute instances that remain even when the virtual compute instance is turned off or decommissioned. The storage shall be scalable up or down within 15 minutes of an API call or administration console change.

4.1.4.2 Highly Scalable Network Storage Service (HSNSS) – Each CCSP shall provide access to reliable, fast, and inexpensive network data storage infrastructure. It shall provide web-scale computing by allowing storage and retrieve any amount of data, at any time, from within CCSP or anywhere on the web. It shall store data objects redundantly on multiple devices across multiple facilities and allows concurrent read or write access to these data objects by many separate clients or application threads. The redundant data stored shall be usable to recover reliably and quickly from instance or application failures. This storage shall also allow for the storage and recovery of machine images, snapshots, and data backups programmatically. It shall provide for programmatic recovery from these snapshots and backups in the case of a system failure. The data stores shall be logically organized in buckets and be accessible to the systems that are providing permission to that data. The data shall have HTTPS URL pointers that address the data by the logical buckets in which it is stored.

4.1.4.3 Highly Scalable (Glacial) Network Storage Service (GNSS) – Each CCSP shall provide slower speed network storage for data that is less frequently accessed. This storage has the same redundancy requirements as the Highly Scalable Network Storage, but with higher latency disk to provide for more cost effective storage of long term, infrequently accessed data.

4.1.4.4 Auto-Scaling File Storage (AFS) – Each CCSP shall provide for automatic scaling File Storage that allows the expansion and contraction of the file system as data is added to and removed from the File Store. The file store shall be mountable by the Virtual Compute Instances and provide file storage as needed based on the storage amount that is needed.

4.1.5 Server Containerization Services (SCS) – Each CCSP shall provide a highly scalable, high performance, container management service that supports a standard container format such as Docker, Kubernetes, or Pivotal Cloud Foundry and allows applications to easily run on a CCSP managed cluster of Virtual Computer instances.

a) This service shall eliminate the need to install, operate, and scale the cluster management infrastructure.
b) The service shall, via the API, be able to launch and stop container enabled applications, query the complete state of the cluster, and access many features like security groups, Virtual Load Balancing, SBS volumes, and IAM roles.
c) The system teams shall be able to schedule the placement of containers across the cluster service based on resource needs and availability requirements.
d) This service shall support third-party schedulers to meet business or application specific requirements.

4.1.6 Network Services – Each CCSP shall provide the following network services:

4.1.6.1 Private Virtual Cloud Network (PVCN) – Each CCSP shall provide a Private Virtual Cloud Network segment that is a logically isolated section of the CCSP where resources can be launched in a virtual network that USCIS defines. USCIS shall have complete control over the virtual networking environment, including selection of its own IP address range, creation of subnets, and configuration of route tables and network gateways. The PVCN shall support both IPv4 and IPv6. The service shall support a minimum 100 PVCN's per account. The PVCN shall support multiple layers of security:

a) The PVCN shall support a minimum of 1000 Security/Firewalling rules per PVCN to control traffic flow.
b) The PVCN shall support a minimum of 1000 Access Control Rules to control traffic flow.
c) The PVCN shall support a hub and spoke networking model to allow traffic flow inside the CCSP to a central point that can be connected back to the DHS data centers or an external MTIPS service via an encrypted Virtual Private Network (VPN) connection between the DHS datacenters to act as an extension of these datacenters.

4.1.6.2 Virtual Load Balancing (VLB) – Each CCSP shall provide an auto-scalable virtual load balancing capability that automatically distributes incoming application traffic across multiple targets, such as VCS instances or SCS containers. It shall handle the varying load of application traffic locally or across data centers. VLB shall offer three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make the applications fault tolerant.

a) Application Load Balancing – An Application Load Balancer shall support load balancing of HTTP and HTTPS traffic and provide advanced request routing targeted at the delivery of modern application architectures, including micro services and containers, operating at the individual request level (Layer 7).
b) Network Load Balancing – Network Load Balancer shall provide load balancing of Transport Control Protocol (TCP) traffic where extreme performance is required. It shall

operate at the connection level (Layer 4) and handle millions of requests per second while maintaining ultra-low latencies.

c) Classic Load Balancing – Classic Load Balancer shall provide basic load balancing across multiple VCS instances and operates at both the request level and connection level.

d) All Virtual Load balancing services shall adhere to the following performance characteristics:

1. High Availability – Automatically distribute incoming traffic across multiple targets in multiple data centers and only to healthy targets that can process the traffic.

2. Security – Provide robust security features, including integrated certificate management and SSL termination and decryption. Centrally manage SSL settings and offload CPU intensive workloads from the applications.

3. Auto Scalability – Virtual Load Balancing shall be capable of handling rapid changes in network traffic patterns. Additionally, integration with auto scaling capabilities shall ensure sufficient application capacity to meet varying levels of application load without requiring manual intervention.

4. Flexibility – Virtual Load Balancing shall provide the capability to use IP addresses to route requests to application targets. This shall provide the capability using application load balancing to run multiple applications on the same virtual compute instance using the same network port to also simplify inter-application communication in micro services based architecture.

5. Monitoring – Virtual Load Balancing shall provide monitoring of applications and their performance in real time with metrics, logging, and request tracing exportable to Splunk to improve visibility into the behavior of your applications, uncovering issues and identifying performance bottlenecks in your application stack at the granularity of an individual request.

6. Hybrid Load Balancing – Virtual Load Balancing shall provide the ability to load balance across the CCSP and on-premise resources using the same load balancer.

7. DNS Services (DNSS) – Each CCSP shall provide a DNS service that integrates with the customers on premise DNS service to provide programmatic add, update, and deletion of DNS records via GUI or API.

4.1.6.3 Direct Connection Service (DCS) – The ability to bypass the public Internet and provide a direct connection to the commercial cloud service provider from the DHS Data Center over a secure scalable on-demand cloud interconnection, providing a secure connection over a private link that improves performance, reduces costs, increases security, and ensures consistent throughput. This connection shall support network speeds up to 10Gbps. This service shall be charged by the amount of data throughput consumed. The service shall support the following criteria:

a) Ability to move large volumes of data in and out of the cloud faster and more securely than over a public internet connection.

b) Ability to achieve predictable network performance and deliver a consistent end user experience.
c) Ability to provide flexible bandwidth options below one Gbps enabling bursts up to two times the committed access rate at no additional cost.
d) Ability to handle workloads that require occasional bandwidth bursts, such as backups, allowing a benefit from higher performance when bandwidth needs spike and from reduced connection costs when bandwidth needs are low.
e) Ability to provide infrastructure components such as Compute, Storage, Database Services, Monitoring, Network, Cloud Automation, and middleware services via programmatic interfaces.

4.1.7 Development Platforms – Each CCSP shall provide PaaS development platforms that provide for loading code and running a workload through a managed CI/CD pipeline and all infrastructure is handled by the development and infrastructure code. This service shall support, at a minimum, .Net, Java, Ruby, Node JS, and PHP development platforms.

4.1.8 Artificial Intelligence Platforms – Each CCSP shall provide a PaaS capability that supports machine learning and artificial intelligence based on algorithms that can parse data, find patterns and learn from that data make determinations/predictions about the world based on the data, and update settings without relying on a human to change the rules-based programming.

4.1.9 Cloud Service Monitoring (CSM) – Each CCSP shall provide a monitoring service for cloud resources and the applications run in the cloud. This service shall collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in the cloud resources. This service shall monitor all forms of cloud service resources (e.g. virtual compute, storage, network, database, containerization, etc.), application logs, and provide that data via an automated interface to external logging tools such as Splunk.

4.1.10 Content Delivery Services (CDS) – The commercial cloud service shall provide a global CDS that securely provides the following capabilities:

a) Cached static data content – secured delivery of cached static data content across the internet outside of the direct CCSP network connection to provide for fast delivery of content to the end user.
b) Video Streaming – secured delivery of streaming video content over the internet to the end user. This service shall support streaming for video, pre-recorded files and live events with sustained, high throughput to support high definition video. On-demand streaming, shall support multi-bitrate adaptive streaming in Microsoft Smooth, HLS, HDS, or MPEG-DASH formats to any device.
c) Security against Distributed Denial of Service (DDoS) – All CDS services shall provide security against DDoS attacks and prevent attacks that alter or affect the content that is being provided by this service.
d) Secure Delivery methods – The CDS shall deliver content in a secure manner compliant with PCI, DSS, HIPAA, and ISO to ensure secure delivery of the most sensitive data. It shall provide secure delivery against DDoS attacks. Secure APIs for applications shall be delivered via SSL/TLS, and advanced SSL features are available automatically.

e) Commercial Third Party Key Support – The service shall be able to utilize commercially available third party certificates from major provider to secure content. This shall include for example: Symantec, Comodo, Entrust, Verizon, Digicert, etc.

4.1.11 Key Management Service (KMS) – Each CCSP shall provide a fully managed secure key management service where the CCSP handles the availability, physical security, and hardware maintenance of the underlying infrastructure. This service shall store keys in hardware security modules (HSMs). This service shall provide the following:

a) Support for import of internal US Treasury or commercially available encryption certificates keys into the HSMs.
b) Each CCSP shall patch, and maintain HSMs and key management software. USCIS shall be able to provision new vaults and keys in minutes and centrally manage keys, secrets, and policies.
c) The applications and USCIS developers shall be granted permissions to the keys, but shall never have direct access to the keys. USCIS developers shall have access to manage Dev and Test Keys, but once transitioned to production, production security and operations personnel shall be the only ones with access to production keys.
d) The production key stores shall support SSL/TLS certificates and automatically renew certificates with public certificate authorities.
e) Keys shall be created, imported, and rotated via commands from the API.
f) All Key management events shall be logged and provided via the CMS to an external security tool, in this instance the USCIS Splunk tool.

4.1.12 Server-less Compute Service (SCS) – The SCS shall provide compute services to execute code that does not require the customer to first provision virtual servers or container services to execute code. The compute instances instantiated by the CCSP to execute the code shall be continuously scalable for parallel code execution. The service shall be on-demand based on the compute resources used for the period of time the code execution consumes.

4.1.13 Identity and Access Management Service (IAMS) – Each CCSP shall provide an IAMS that is fully configurable by customer that integrates with customer three factor authentication systems. This service shall support the Government three factor authentication standard.

4.1.14 Cloud Formation Service (CFS) – Each CCSP shall provide a cloud formation capability via its API calls which can build an entire system computing environment from script. This shall include all networking components, routing, firewalling, security, keys, certificates, users, roles, virtual computing instances, containers, micro-services, storage, databases, load balancers, messaging services, monitoring, and content delivery to establish an entire environment.

4.1.15 Messaging Services – Each CCSP shall deliver the following messaging services:

a) Message Queueing Service (MQS) – Each CCSP shall provide a fully managed MQS that easily enables the decoupling and scaling of micro-services, distributed systems, and server-less applications. This service shall support the building of applications from individual components that each performs a discrete function which improves scalability and reliability and is fault tolerant. This service shall allow the sending, storage, and receipt of messages between software components at any volume, without losing messages or requiring other services to always be available. The queues shall be manageable via the API just like any other service in the cloud. The queueing services shall provide at least one of the following two choices for methods of delivery:

1. Best Effort – The Best Effort method of deliver shall provide for maximum throughput, best-effort ordering, and at-least-once delivery.

2. First In First Out (FIFO) – The FIFO method shall guarantee that messages are processed exactly once, in the exact order that they are sent.

4.1.16 Publish/Subscribe Notification – Each CCSP shall provide a fully managed pub/sub messaging service that makes it easy to decouple and scale micro-services, distributed systems, and server-less applications. This service shall support communications to the messaging queues, desktop architectures, and mobile devices including Android and Apple iOS. This service shall support event driven computing workflows based on topics and triggers.

4.2 <u>SOFTWARE AS A SERVICE</u> – The contractor shall provide access to at least one offering of each of the following FedRAMP Authorized SaaS services:

4.2.1 Customer Management Services – The reseller shall provide a SaaS Customer Relationship Management service that has the following capabilities:

a) A dedicated document library for creating, storing, and retrieving documentation on each customer, standards for call protocols, and the customer's application status with USCIS.
b) Role based user access that integrates with the DHS Active Directory service.
c) Workflow automation for handling the calls that is customizable by USCIS personnel to match the workflow patterns of the Agency.
d) Integration with the DHS Exchange Email system to manage communications within the agency.
e) API calls to allow for automation of work patterns.
f) Standard and Customizable reports to get status on calls such as, call volume, call patterns, call hang-ups, call wait states, call resolutions, and call volumes by topic.

4.2.2 Service Desk Management Services – The reseller shall provide a SaaS Service Desk Management service that supports Asset Management, customizable ticketing workflows, knowledge base management, smartphone apps for the user, web based user portal, customizable, user role based permissions that integrate with the DHS Active Directory Services, and integration with the Microsoft Exchange email system.

4.2.3 Unified Communications Services – The reseller shall provide a SaaS unified communications service that is cloud based and meets government-level security standard to allow organizations to collaborate with internal government and external commercial entities from any device, mobile, computer, or desk phone. This service shall include the capability to delivering mobility, voice, video conferencing, web, chat, presence, audio conferencing, voicemail, textual chat.

4.2.4 Video Conferencing Services – The reseller shall provide access to Video Conferencing SaaS that allows for using the call connection hardware completely hosted in the cloud. It shall be capable of supporting between 2-1,000 participant connections supporting small to large Town Hall type conferencing capabilities. This service shall also include shared whiteboard, computer application and screen sharing, calls, and text chat.

4.2.5 Mobile Device Management Services – The reseller shall provide a SaaS to deploy, configure, secure, manage and support smartphones, tablets, laptops and other devices across multiple mobile applications and operating systems. It shall support line-of-business devices the Government can implement in a containerized solution or as a comprehensive solution based on device type, use case and user role in the organization.

4.2.6 Office Application Services – The reseller shall provide the Office Suite as SaaS to support the USCIS enterprise deployment of the Office Suite in a FedRAMP commercial cloud, FedRAMP Impact Level moderate.

5. Contract Administration

5.1 The contractor shall directly provide contract administration in support of the IaaS / PaaS / SaaS services. Such professional services may include, but are not limited to:

a) Provisioning of accounts, including collection of USCIS user information; Management of the Master Payer Account. Organization of the accounts in the console and reporting/analysis tools.

b) Collection, analysis, and synthesis of Agency usage data for all services provided by a contractor, whether non-labor or professional, to ensure configuration and accurate billing through the CloudCheckr tool, when compatible with a CCSP, and a functionally similar tool with other CCSP that are not compatible with CloudCheckr.

6 Acronyms and Definitions

6.1 API – Application Programming Interface

6.2 CCHS – Commercial Cloud Hosting Services – A USCIS program within the Enterprise Cloud Services branch that manages the services provided by the Commercial Cloud Service Providers to the organization.

6.3 CCSP – Commercial Cloud Service Provider – a commercial entity that provides for virtualized IaaS and PaaS resources which are launched and managed via a programmatic interface to support fully automated CI/CD pipelines and system environments. It is a consumption based on-demand cloud hosting model that is billed in increments no larger than one hour.

6.4 CI/CD Pipeline – Continuous Integration/Continuous Delivery Pipeline – an automated method of software and infrastructure integration, testing, and deployment that is accomplished through programmatic interfaces. The pipeline usually includes several system environments including development, functional testing, unit testing, performance testing, pre-production, and production. The programmatic scripting is based on triggers and testing tools to validate the new code and move the code through the pipeline from one environment to the next until it has passed all the tests and is deployed to production.

6.5 **DHS –** Department of Homeland Security

6.6 **GUI –** Graphical User Interface

6.7 **IaaS –** Infrastructure as a Service – a virtualized set or resources that are programmatically instantiated and managed by the customer from the operating system through to the application layers.

6.8 **IOPS** – This is the input/output operations per second used to measure disk performance.

6.9 **PaaS –** Platform as a Service – a virtualized set or resources that are programmatically instantiated and managed by the customer from the operating system through to the application layers.

6.10 **SaaS –** Software as a Service – a virtualized set or resources that are programmatically instantiated and managed by the customer from the operating system through to the application layers.

6.11 **Services -** The term "services," in the context of this document, does not mean services performed by personnel. It is service analogous to telephone, cable, electrical, or cell phone service. There are no personnel involved in these services other than commercial cloud hosting resellers provisioning cloud accounts and providing data reports to verify CloudCheckr billing. It is a compute service function that allows USCIS to build and host system in a virtualized public cloud infrastructure environment.

6.12 **True On-Demand Commercial Cloud** – a Commercial Cloud that features completely virtualized infrastructure and services where the customer has direct unfettered programmatic access to launch and manage resources on-demand in real-time. The underlying hardware resources are managed by the CCHS and always have sufficient processing to deliver the performance specified by the service offerings. It is a consumption based model where each service is billed in increments no larger than one hour.

6.13 **USCIS –** United States Citizenship and Immigration Services

70SBUR19A000000012 - Section III - [redacted]

[redacted]

[redacted]

[redacted]