Section I – BPA Terms and Conditions

1.0 General

This section presents the general requirements applicable to the BPA Contractor.

It is the responsibility of the Contractor to notify the Contracting Officer of GSA Schedule price changes affecting services listed in this BPA prior to award of any order. Contractors may offer further price reductions in accordance with their commercial practice and are encouraged to offer additional discounts at the BPA level and the order level. The relationship between the current price in the GSA Schedule and the price offered in the Contractor's quotation shall remain constant; i.e., the discount shall remain the same throughout the term of the BPA. All orders placed against this BPA are subject to the terms and conditions of the GSA Schedule contract, except as specifically noted in this BPA.

2.0 Services

At the BPA order level, the BPA Contractor shall provide the estimated labor categories and hours to perform the requirements identified.

3.0 Types of Orders

This BPA provides for Firm-Fixed-Price (FFP), Labor-Hour (LH), and Time-and-Materials orders with options. The type of order will be identified at the BPA order level.

4.0 BPA Estimated Value

The estimated dollar value of the total BPA orders placed under the BPA is $7.3 million over five (5) years.

5.0 Obligation

This BPA does not obligate any funds. Each individual order placed against this BPA will obligate funds.

6.0 Referenced Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR) Clauses

The Contractor's GSA Professional Services Schedule contract clauses are incorporated into this BPA.

This BPA 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 this address: https://www.acquisition.gov/?q=browsefar or for DHS specific clauses at http://farsite.hill.af.mil/vmhsara.htm.

Clause	Title	Date
DHS Clauses/Provisions		
HSAR 3052.203-70	Instructions for Contractor Disclosure of Violations	SEP 2012
HSAR 3052.205-70	Advertisements, Publicizing Awards, and Release – Alternate I	SEP 2012
HSAR 3052.242-72	Contracting Officer's Technical Representative	DEC 2003
Additional FAR Clauses/Provisions		
FAR 52.204-2	Security Requirements	AUG 1996

HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 45 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause).

HSAR 3052.204-71 Contractor Employee Access (SEP 2012) with 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.

When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of

work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020)

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are

covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

7.0 Term of the BPA

7.1 The BPA shall remain in effect for a maximum ordering period of five (5) years from the date of award or until the expiration or termination of the BPA Contractor's GSA Schedule contract, whichever is sooner. The period of performance for each individual BPA order shall be specified at the BPA order level.

7.2 BPA orders may be issued at any time during the five-year period. The performance period will be specified in the BPA order and may include option periods which extend the BPA order up to 12-months beyond the expiration date of this BPA.

8.0 Ordering Officers

DHS warranted Contracting Officers within the Management Directorate and at DHS Components are authorized to place orders under this BPA. DHS Components include:

- Cybersecurity and Instructure Security Agency (CISA)
- Federal Emergency Management Agency (FEMA)
- Federal Law Enforcement Training Center (FLETC)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Customs and Border Protection (CBP)
- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Secret Service (USSS)

9.0 Orders

Orders that will be placed against this BPA by the DHS Contracting Officers shall be in accordance with the Ordering Procedures identified in the BPA.

10.0 Ordering Procedures

The DHS order-level Contracting Officer shall award and administer orders in accordance with the ordering procedures and ordering guidelines set forth in this BPA and the procedures outlined in FAR 8.405-3(c)(1), Ordering from single-award BPAs.

10.1 Each order issued under this BPA will include the following information, as applicable:

(1) BPA number and order number;
(2) Date of the order;
(3) Description of the work to be performed;
(4) The work schedule, period of performance, or required completion date (include the requiring office typical hours of operation);
(5) Place of performance;
(6) Deliverables;
(7) CLIN number and description, quantity, unit price, and extended total;
(8) The firm-fixed-price to complete the requirements or labor-mix table with labor categories and rates identified;

(9) The security requirements;
(10) The payment schedule; and
(11) Accounting and appropriation data.

10.2 BPA orders shall be within the scope of the BPA. Only the Contracting Officer for the BPA may modify the BPA.

11.0 Invoicing
Invoicing procedures shall be specified in each individual order.

12.0 Order of Precedence
The terms and conditions included in this BPA apply to all orders pursuant to it. In the event of an inconsistency between the provisions of this BPA and the terms and conditions of the Contractor's Schedule contract, the GSA contract will take precedence.

13.0 Annual Review of the BPA
In accordance with FAR 8.405-3(e), DHS OPO, which has established this BPA, will conduct an annual review to determine whether the underlying Schedule contract is still in effect, whether the BPA still represents best value, and whether the estimated quantities/amounts have been exceeded and additional price reductions can be obtained.

14.0 Nonconformance
The Government will remedy nonconformance in accordance with FAR 8.406-3 Remedies for Nonconformance, 8.406-4 Termination for Cause, 8.406-5 Termination for the Government's Convenience, and 8.406-6 Disputes.

15.0 Disclosure of Information

15.1 BPA Holder is reminded that information furnished under this solicitation may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked. Marking of items will not necessarily preclude disclosure when DHS determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.

15.2 Any information made available to the BPA Holder by the Government must be used only for the purpose of carrying out the provisions of this BPA and all subsequent orders and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the order.

15.3 In performance of this BPA, the BPA Holder assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the BPA Holder or the BPA Holder's responsible employees.

15.4 Each officer or employee of the BPA Holder or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the BPA

Holder that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. 641.

16.0 Contractor Team Arrangement (CTA)

16.1 It is anticipated that the awarded contractor will be termed "BPA Holder" or "BPA Contractor" and considered the Prime Contractor. The BPA Holder shall hold a GSA MAS Schedule 541620, Environmental Consulting Services, contract and may have teaming arrangements/agreements with other contractors termed "CTA Partners" for purposes of meeting the requirements of the BPA. Any BPA Holder utilizing a CTA Partner is required to submit the teaming agreement document and to identify, in its quotation, the lead CTA Partner and the participating members, their corresponding GSA Schedule contract numbers, the work to be performed by each team member, team members' responsibility for all services and related tasks.

16.2 For purposes of the BPA and order administration, all Government communications, ordering, and scheduling flows through the BPA Holder. Furthermore, all invoices shall be submitted by the BPA Holder and all payments will be made to this BPA Holder who, in turn, will be responsible for payment to each CTA Partner. Any disputes involving the distribution of payment between the BPA Holder and CTA Partner shall be resolved without any involvement by the Government.

16.3 The BPA Holder shall also provide the DHS Contracting Officer with a primary and alternate administrative points of contact (POC) after BPA award. The BPA Holder shall notify the DHS BPA Contracting Officer and Contracting Officer's Representative (COR) of any changes in contact information as expeditiously as possible.

17.0 BPA Prices and Price Adjustments

17.1 At no time shall order prices exceed awarded prices on the Contractor's GSA Schedule contract or the BPA. The discount pricing relationship established for the BPA Holder (including all CTA Partners) shall be maintained throughout the life of the BPA unless modified by the DHS Contracting Officer.

17.2 The BPA Holder may request a price increase on the BPA only after there has been an approved GSA Schedule price increase. The DHS Contracting Officer will make the final decision on any request for price increases under this BPA via a bilateral modification. For any price decreases made to the GSA Schedule contract, the BPA discounted price shall be immediately identified to the DHS Contracting Officer and be immediately effective. There will be no retroactive price increases allowed on existing orders.

18.0 508 REQUIREMENTS ACCEPTANCE

Before accepting information and communications technology (ICT) required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims

provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.