

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. Contract ID Code
Firm Fixed Price

Page 1 Of 7

2. Amendment/Modification No. P00005	3. Effective Date 2015DEC16	4. Requisition/Purchase Req No. SEE SCHEDULE	5. Project No. (If applicable)
---	--------------------------------	---	--------------------------------

6. Issued By ARMY CONTRACTING COMMAND - RI JENNIFER S. TYLER ROCK ISLAND, IL 61299-8000 BLDGS 60 & 62 EMAIL: JENNIFER.S.TYLER.CIV@MAIL.MIL	Code W52P1J	7. Administered By (If other than Item 6)	Code
---	----------------	---	------

8. Name And Address Of Contractor (No., Street, City, County, State and Zip Code) FOUR POINTS TECHNOLOGY, L.L.C. 14900 CONFERENCE CENTER DR STE 100 CHANTILLY, VA 20151-3813	<input type="checkbox"/>	9A. Amendment Of Solicitation No.
	<input type="checkbox"/>	9B. Dated (See Item 11)
	<input checked="" type="checkbox"/>	10A. Modification Of Contract/Order No. W52P1J-12-A-0018
	<input type="checkbox"/>	10B. Dated (See Item 13) 2012AUG03
Code 1YS78	Facility Code	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in item 14. The hour and date specified for receipt of Offers

is extended, is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendments; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. **FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER.** If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. Accounting And Appropriation Data (If required)

NO CHANGE TO OBLIGATION DATA

**13. THIS ITEM ONLY APPLIES TO MODIFICATIONS OF CONTRACTS/ORDERS
It Modifies The Contract/Order No. As Described In Item 14.**

<input type="checkbox"/>	A. This Change Order is Issued Pursuant To: The Contract/Order No. In Item 10A.	The Changes Set Forth In Item 14 Are Made In
<input type="checkbox"/>	B. The Above Numbered Contract/Order Is Modified To Reflect The Administrative Changes (such as changes in paying office, appropriation data, etc.) Set Forth In Item 14, Pursuant To The Authority of FAR 43.103(b).	
<input checked="" type="checkbox"/>	C. This Supplemental Agreement Is Entered Into Pursuant To Authority Of:	52.212-4(c)
<input type="checkbox"/>	D. Other (Specify type of modification and authority)	

E. IMPORTANT: Contractor is not, is required to sign this document and return _____ copies to the Issuing Office.

14. Description Of Amendment/Modification (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

SEE SECOND PAGE FOR DESCRIPTION

Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. Name And Title Of Signer (Type or print)	16A. Name And Title Of Contracting Officer (Type or print) JILL M. SOMMER JILL.M.SOMMER.CIV@MAIL.MIL (309)782-3582		
15B. Contractor/Offeror (Signature of person authorized to sign)	15C. Date Signed	16B. United States Of America By _____ /SIGNED/ (Signature of Contracting Officer)	16C. Date Signed 2015DEC16

CONTINUATION SHEET**Reference No. of Document Being Continued****Page 2 of 7****PIIN/SIIN** W52P1J-12-A-0018**MOD/AMD** P00005**Name of Offeror or Contractor:** FOUR POINTS TECHNOLOGY, L.L.C.

SECTION A - SUPPLEMENTAL INFORMATION

Buyer Name: JENNIFER S. TYLER
Buyer Office Symbol/Telephone Number: CCRC-TA/(309)782-7833
Type of Contract 1: Firm Fixed Price
Kind of Contract: Service Contracts
Kind of Modification: G
Type of Business: Other Small Business Performing in U.S.
Surveillance Criticality Designator: C
BPA Expiration Date: 2016MAR02

Paying Office: HQ0303
DFAS-COLUMBUS
DFAS-CO/JAIQBAC
ATTN: ROCK ISLAND
P. O. BOX 182316
COLUMBUS OH 43218-2316

*** End of Narrative A0000 ***

1. The purpose of this modification to W52P1J-12-A-0018 is to add DFARS Clause 252.204-7012 entitled Safeguarding Covered Defense Information and Cyber Incident Reporting.
2. See also Attachment 0013 Chain of Contact for Government Personnel. Please note that communication with the Government should start at the lowest level possible.
2. Except as provided herein, all other terms and conditions remain unchanged.

*** END OF NARRATIVE A0007 ***

CONTINUATION SHEET	Reference No. of Document Being Continued		Page 3 of 7
	PIIN/SIIN W52P1J-12-A-0018	MOD/AMD P00005	
Name of Offeror or Contractor: FOUR POINTS TECHNOLOGY, L.L.C.			

SECTION I - CONTRACT CLAUSES

<u>Status</u>	<u>Regulatory Cite</u>	<u>Title</u>	<u>Date</u>
I-1 ADDED	252.204-7012 (DEV 2016- 00001)	SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEVIATION 2016-00001)	OCT/2015

(a) Definitions. As used in this clause--

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified information that--

(i) Is--

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) Controlled technical information.

(B) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

"Cyber incident" means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or

CONTINUATION SHEET	Reference No. of Document Being Continued	Page 4 of 7
	PIIN/SIIN W52P1J-12-A-0018	MOD/AMD P00005

Name of Offeror or Contractor: FOUR POINTS TECHNOLOGY, L.L.C.

other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum--

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government--

(A) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and

(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract; or

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause--

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," (see <http://dx.doi.org/10.6028/NIST.SP.800-171>) that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer with the exception of the derived security requirement 3.5.3 Use of multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts, which will be required not later than 9 months after award of the contract, if the Contractor notified the contracting officer in accordance with paragraph (c) of the provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (DEVIATION 2016-00001)(OCT 2015); or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the DoD Chief Information Officer (CIO) prior to contract award; and

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractors ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall--

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractors network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractors ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <http://dibnet.dod.mil>.

CONTINUATION SHEET	Reference No. of Document Being Continued	Page 5 of 7
	PIIN/SIIN W52P1J-12-A-0018	MOD/AMD P00005

Name of Offeror or Contractor: FOUR POINTS TECHNOLOGY, L.L.C.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <http://dibnet.dod.mil>.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <http://iase.disa.mil/pki/eca/Pages/index.aspx>.

(d) Malicious software. The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (recipient) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Governments use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractors responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) Subcontracts. The Contractor shall--

(1) Include the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items; and

(2) Require subcontractors to rapidly report cyber incidents directly to DoD at <http://dibnet.dod.mil> and the prime Contractor. This

CONTINUATION SHEET	Reference No. of Document Being Continued PIIN/SIIN W52P1J-12-A-0018 MOD/AMD P00005	Page 6 of 7
---------------------------	---	---------------------------

Name of Offeror or Contractor: FOUR POINTS TECHNOLOGY, L.L.C.

includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

CONTINUATION SHEET**Reference No. of Document Being Continued****Page 7 of 7****PIIN/SIIN** W52P1J-12-A-0018**MOD/AMD** P00005**Name of Offeror or Contractor:** FOUR POINTS TECHNOLOGY, L.L.C.

SECTION J - LIST OF ATTACHMENTS

<u>List of</u> <u>Addenda</u>	<u>Title</u>	<u>Date</u>	<u>Number</u> <u>of Pages</u>	<u>Transmitted By</u>
Attachment 0013	CHAIN OF CONTACT FOR GOVERNMENT PERSONNEL	18-NOV-2015	001	EMAIL