REQUEST FOR QUOTATION

RFQ NO. INTERNET AND TELEPHONE SATELLITE SERVICES
FOR
FBI LOS ANGELES FIELD OFFICE

Date: 02/14/2024

From: Federal Bureau of Investigation/ Finance Division

Subject: Request for Quotation (RFQ) for Internet and Telephone Satellite Services for FBI Los Angeles Field Office

Solicitation Number: **TBD**

The Federal Bureau of Investigation (FBI) Procurement Section is issuing this Request for Quotation (RFQ) for the purpose of procuring internet and telephone satellite services for per the below specs for the FBI Los Angeles Division. This RFQ falls under FAR Part 12 and 8.4. This requirement will be awarded based on Lowest Price Technically Acceptable (LPTA).

NAICS Code: 517410, Satellite Telecommunications

Size Standard: $40,000,000.00

The period of performance for this requirement will be: from March 1st, 2024 to February 28th, 2025.

Contractors interested in competing for this effort may participate by submitting quotes in accordance with the procedures set forth in this RFQ. **All quotes shall be firm fixed priced**.

Questions To the Contracting Officer Are Due: 02/20/2024 at 12:00pm EST/EDT

Quotes Must Be Submitted No Later Than: 02/28/2024 at 12:00pm EST/EDT

ALL QUESTIONS SHALL BE EMAILED TO THE CONTRACTING OFFICER AT HNGUYEN2@FBI.GOV, ALL QUOTES SHALL BE SUBMITTED TO HNGUYEN2@fbi.gov.

1.0 SUPPLIES OR SERVICES AND PRICES

1.1 GENERAL DESCRIPTION

The FBI has a requirement for internet and telephone satellite service.

2.0 DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

2.1 PURPOSE

The purpose of this RFQ is to receive Firm Fixed Price quotes from small businesses vendors for the internet and telephone service via satellite. The vendor shall provide a detail quote based on the requirement listed in 2.6.1.

2.2 BACKGROUND

The Los Angeles Electronics Technician program has a requirement for internet and telephone service via satellite for the FBI Mobile Command Center (MCC).

2.3 SCOPE OF WORK

This RFQ is for internet and telephone service via satellite. No Scope of Work is provided.

2.4 DELIVERABLES

SEE 2.6.1 CLINS

2.5 TERM OF CONTRACT

- All quotes shall be firm fixed price
- Delivery shall occur on or before 5 days after receipt of purchase order.
- By submitting a quote the vendor agrees to all terms and conditions found in this RFQ.
- **All vendors shall complete and submit with their quote the vendor determination of responsibility document.**

2.6 SERVICES AND PRICES/COSTS

The following abbreviations are used in this price schedule: **Firm Fixed Price (FFP)**

2.6.1 BILL OF MATERIALS (Shall include all costs associated with delivery, products, profit, and any additional categories not listed)

FBI LOS ANGELES SATELLITE SPECS LIST
The Los Angeles Electronics Technician program has a requirement for internet and telephone service via satellite for the FBI Mobile Command Center (MCC). This requirement includes the need for one vehicle mount and one portable satellite units, both having iDirect modems. Service requirements: Duel satellite GEO connectivity with complete IP portability, 20Mx5M, minimum acceptability 10:1 contention ratio, all voice services included, Redphone included, 100 days of simplex 500k streaming, 1 Cradlepoint NetCloud license for one year. Hardware compatibility: The service being requested is for satellite based internet service/WI-FI with full IP address portability for direct connection and the option of 24 hours multiple satellite connections for redundancy. This satellite service would also require telephone service compatibility based on the existing installed Panasonic 'Advanced Hybrid System' telephone switch KX-TA1232 with Panasonic KX-T7731 land-line type phone hardware already installed in the MCC. Required hardware compatibility is due to lack of funds for system hardware upgrades. This telephone service requires dial in/out access to fixed numbers. An additional Requirement is access to the Red PHONE service and directory, allowing the ability to connect to all agencies who participate.

GRAND TOTAL: $_____

2.7 TERMS AND CONDITIONS

Incorporated by Reference:

52.212-1 Instructions to Offerors

52.212-4 Contract Terms and Conditions

52.212-2 Evaluation—Commercial Items. Evaluation—Commercial Items.

As prescribed in 12.301(c), the Contracting Officer may insert a provision substantially as follows: EVALUATION—COMMERCIAL ITEMS (OCT 2014)

(a) The Government will award a contract resulting from

this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

x Total Small Business Set Aside _____

Past Performance_____

Lowest Price Technically

Acceptable_____ Technical and past performance, when combined, are Equal, *when compared to price*.

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)

52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders— Commercial Items.

As prescribed in 12.301(b)(4), insert the following clause: CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS— COMMERCIAL ITEMS (JUN 2016)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of

law or Executive orders applicable to acquisitions of commercial items:

(1) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)

(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004)(Public Laws 108-77 and 108-78 (19

U.S.C. 3805 note)).

The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

___ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (SEPT 2006), with Alternate I (OCT 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

___ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509)).

X___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUNE 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

___ (4) 52.204-10, Reporting Executive Compensation

and First-Tier Subcontract Awards (OCT 2015) (Pub. L. 109- 282) (31 U.S.C. 6101 note).

___ (5) [Reserved].

___ (6) 52.204-14, Service Contract Reporting Requirements (JAN 2014) (PUB. L. 111-117, section 743 OF DIV. C).

___ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (JAN 2014) (PUB. L. 111-117, section 743 OF DIV. C).

___ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (OCT 2015) (31 U.S.C. 6101 note).

___ (9) 52.209-9, Updates of Publicly Available

Information Regarding Responsibility Matters (JUL 2013) (41 U.S.C. 2313).

___ (10) [Reserved].

___ (11)(i)52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

___ (ii) Alternate I (NOV 2011) of 52.219-3.

___ (12)(i)52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

___ (ii) Alternate I (JAN 2011) of 52.219-4.

___ (13) [Reserved]

_**X**_ (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

___ (ii) Alternate I (NOV 2011).

___ (iii) Alternate II (NOV 2011).

___ (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (JUNE 2003) (15 U.S.C. 644).

___ (ii) Alternate I (OCT 1995) of 52.219-7.

___ (iii) Alternate II (MAR 2004) of 52.219-7.

___ (16) 52.219-8, Utilization of Small Business Concerns (OCT 2014) (15 U.S.C. 637(d)(2) and (3)).

___ (17)(i) 52.219-9, Small Business Subcontracting Plan (OCT 2015) (15 U.S.C. 637(d)(4)).

___ (ii) Alternate I (OCT 2001) of 52.219-9.

___ (iii) Alternate II (OCT 2001) of 52.219-9.

___ (iv) Alternate III (OCT 2015) of 52.219-9.

___ (18) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

___ (19) 52.219-14, Limitations on Subcontracting (NOV 2011) (15 U.S.C. 637(a)(14)).

___ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (JAN 1999) (15 U.S.C. 637(d)(4)(F)(i)).

___ (21) 52.219-27, Notice of Service-Disabled Veteran- Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657 f).

___ (22) 52.219-28, Post Award Small Business Program Representation (JUL 2013) (15 U.S.C. 632(a)(2)).

___ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women- Owned Small Business Concerns (DEC 2015) (15 U.S.C. 637(m)).

___ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (DEC 2015) (15 U.S.C. 637(m)).

_**X**_ (25) 52.222-3, Convict Labor (JUNE 2003)

(E.O. 11755).

_**X**_ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (FEB 2016) (E.O. 13126).

_**X**_ (27) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

_**X**_ (28) 52.222-26, Equal Opportunity (APR 2015)

(E.O. 11246).

_**X**_ (29) 52.222-35, Equal Opportunity for Veterans (OCT 2015)(38 U.S.C. 4212).

_**X**_ (30) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

___ (31) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212).

___ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

_**X**_ (33)(i) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O. 13627).

___ (ii) Alternate I (MAR 2015) of 52.222-50 (22

U.S.C. chapter 78 and E.O. 13627).

___ (34) 52.222-54, Employment Eligibility Verification (OCT 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

___ (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items

(MAY 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable

to the acquisition of commercially available off-the-shelf items.)

___ (ii) Alternate I (MAY 2008) of 52.223-9

___ (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).

___ (38)(i)52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (JUN 2014) (E.O.s 13423 and 13514).

___ (ii) Alternate I (OCT 2015) of 52.223-13.

___ (39)(i)52.223-14, Acquisition of EPEAT®-Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).

___ (ii) Alternate I (JUN 2014) of 52.223-14.

___ (40) 52.223-15, Energy Efficiency in Energy- Consuming Products (DEC 2007) (42 U.S.C. 8259b).

___ (41)(i) 52.223-16, Acquisition of EPEAT®-

Registered Personal Computer Products (OCT 2015) (E.O.s 13423 and 13514).

___ (ii) Alternate I (JUN 2014) of 52.223-16.

__ (42) 52.223-18, Encouraging Contractor Policies to

Ban Text Messaging While Driving (AUG 2011) (E.O. 13513).

___ (43) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).

___ (44) 52.223-21, Foams (JUN 2016) (E.O. 13693).

___ (45) 52.225-1, Buy American—Supplies (MAY 2014) (41 U.S.C. chapter 83).

___ (46)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (MAY 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19

U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182,

108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-

283, 110-138, 112-41, 112-42, and 112-43.

___ (ii) Alternate I (MAY 2014) of 52.225-3.

___ (iv) Alternate III (MAY 2014) of 52.225-3.

_X__ (47) 52.225-5, Trade Agreements (FEB 2016) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

___ (48) 52.225-13, Restrictions on Certain Foreign Purchases (JUNE 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

___ (49) 52.225-26, Contractors Performing Private

Security Functions Outside the United States (JUL 2013) (Sec-tion 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

___ (50) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (NOV 2007) (42 U.S.C. 5150).

___ (51) 52.226-5, Restrictions on Subcontracting

Outside Disaster or Emergency Area (NOV 2007) (42 U.S.C. 5150).

___ (52) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 4505,

10 U.S.C. 2307(f)).

___ (53) 52.232-30, Installment Payments for Commercial Items (OCT 1995) (41 U.S.C. 4505,

10 U.S.C. 2307(f))

_**X**_ (54) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (JUL 2013) (31 U.S.C. 3332).

___ (55) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (JUL 2013) (31 U.S.C. 3332).

___ (56) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).

___ (57) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

___ (58)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006)

(46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

___ (ii) Alternate I (Apr 2003) of 52.247-64.

(b) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items: [*Contracting Officer check as appropriate*.]

___ (1) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014)(E.O. 13495).

__ (2) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

___ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 2014) (29 U.S.C. 206 and

41 U.S.C. chapter 67).

___ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (MAY 2014) (29 U.S.C. 206 and

41 U.S.C. chapter 67).

___ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment— Requirements (MAY 2014) (41 U.S.C. chapter 67).

___ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter

67).

___ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

___ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792).

___ (10) 52.237-11, Accepting and Dispensing of $1 Coin (SEPT 2008) (31 U.S.C. 5112(p)(1)).

(c) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an Authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type

and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (OCT 2015) (41 U.S.C. 3509).

(ii) 52.219-8, Utilization of Small Business Concerns (OCT 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(iv) 52.222-21, Prohibition of Segregated Facilities (APR 2015)

(v) 52.222-26, Equal Opportunity (APR 2015) (E.O. 11246).

(vi) 52.222-35, Equal Opportunity for Veterans (OCT 2015) (38 U.S.C. 4212).

(vii) 52.222-36, Equal Opportunity for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).

(viii) 52.222-37, Employment Reports on Veterans (FEB 2016) (38 U.S.C. 4212)

(ix) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(x) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(xi) ___ (A) 52.222-50, Combating Trafficking in Persons (MAR 2015) (22 U.S.C. chapter 78 and E.O 13627).

___ (B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O 13627).

(xii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiv) 52.222-54, Employment Eligibility Verification (OCT 2015) (E.O. 12989).

(xv) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

(xvi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (JUL 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xvii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xviii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C.

Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor

---

NOTICE OF CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.

1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term2 contractor employee whose background investigation (BI) process begins on or after October 27, 2005:

a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form 1-9, OMB No. 1615-0047, " Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

•High Risk - Background Investigation (5-year scope)

•Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)

•Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;3
4) Waiver request memorandum, including both the Office of Personnel

Management schedule date and position sensitivity/risk level; and 5) Favorable review of the National Agency Check (NAC)4 portion of the applicable BI that is determined by position sensitivity/risk level.

A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM' s scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).

e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.

2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items la. and lb. above. The pre-appointment waiver requirements for short-term contractors are:

a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;
c.Favorable credit report, if required;5 and
d.Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.

A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve-month period. This will ensure that any consecutive short-term appointments are subject to the full PFV-I identity proofing process.

For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve- month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.

3. Intermittent Contractors:

An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5.The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.

NOTES:

1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201 /FIPS-201-22505.pdf.
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre- appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM 's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block "B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre- appointment waiver package.

(End of Clause)

Every effort must be made to ensure that supplies are provided and integrated and services are performed using sound security components, practices, and procedures. Acquisition of supplies or services from concerns under Foreign Ownership, Control, or Influence (FOCI) or of supplies developed, manufactured, maintained, or modified by concerns under FOCI (any or all of which shall be referred to herein as "Use of FOCI source") is of serious concern and must be approved prior to contract award. Approval decisions will be made on a case by case basis after the source or technology has been identified by the Offeror and subjected to a risk assessment. The risk assessment process will vary depending on the acquisition type and proposed use of a FOCI source, available risk mitigation measures, and the information/justification provided by the Offeror. Any Offeror responding to this Request for Proposal (RFP), Request for Quotation (RFQ), or Sealed Bid acknowledges the Government's requirements to secure services or equipment from firms which are not under Foreign Ownership, Control, or Influence (FOCI), or where any FOCI, in the opinion of the Government, adversely impacts on National Security or security requirements. The Offeror understands and agrees that the Government retains the right to reject any response to this RFP, RFQ, or Sealed Bid made by the Offeror, without any further recourse by or explanation to the Offeror, if the FOCI for that Offeror is determined by the Government to be an unacceptable security risk. Risk assessments will be on a case by case basis and will be used to determine whether the use of a FOCI source poses an unacceptable security risk. If an unacceptable security risk is determined, the Government retains the right to reject the use of a FOCI source or to require that certain risk mitigation measures be taken by the Offeror. Similarly, the Government retains the unilateral right to approve the use of a FOCI source when the risk assessment indicates that such use would be in the Governments' best interests. If the use of a FOCI source is not approved, no classified information will be disclosed to the Offeror as part of the Government's rationale for non-approval. The Offeror (prime and subs) may not seek reimbursement from the Government for any costs associated with responding to this RFP, RFQ or Sealed Bid, as a result of a FOCI non#approval decision.

In Section K, Offerors shall complete the Acquisition Risk Questions and Key Management Personnel Listing (KMPL) for the prime contractor and all proposed subcontractors. Provision of false information shall be cause for default under the Default Clause of this contract. The information in Section K regarding Key Management Personnel, which may identify U.S. persons, is being requested pursuant to the National Security Act of 1947, as amended, Executive Order 12829, National Industrial Security Program, and Director of Central Intelligence Directive 7/6, Community Acquisition Risk Center, or superseding Acts, Orders or Directives. The FBI will use this information to conduct the acquisition risk determination and may share the information internally and externally with members of the Intelligence Community and other U.S. Government entities, if necessary, consistent with appropriate routine uses for its Central Records System (CRS), Justice/FBI-002, last published in full in the Federal Register on February 20, 1998 (63 Fed. Reg. 8671), or any updates thereto. In the absence of proof of death of any of the Key Management Personnel, their consent, or an overriding public interest, the information will not otherwise be disseminated except pursuant to the routine uses for the CRS. The Government reserves the right to prohibit individuals who are not U.S. citizens from all or certain aspects of the work to be performed under this Contract. Foreign Ownership, Control, or Influence (FOCI) For purposes of this clause, a U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company. Changed conditions, such as change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating, or, alternatively, that different FOCI mitigation measures be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI. There is a continuing obligation of the Selected Offeror to advise the Government of such changed conditions. Failure to abide by this obligation shall be cause for default under the Default Clause of this contract.

Factors: The following factors will be used as the basis for making an acquisition risk determination. If the Offeror, or its proposed subcontractors, meet any of the following factors, they must identify themselves as a potential FOCI company and submit themselves for a Government FOCI evaluation and risk assessment: (1) Ownership or beneficial ownership, direct or indirect, of 5 percent or more of the Offeror's company's voting securities by a foreign person. (2) Ownership or beneficial ownership, direct or indirect, of 25 percent or more of any class of the Offeror's company's non- voting securities by a foreign person. (3) Management positions, such as directors, officers, or executive personnel of the Offeror's company held by non-U.S. citizens. (4)

Foreign person power, direct or indirect, to control the election, appointment, or tenure of directors, officers or executive personnel of the Offeror's company or other decisions or activities of the Offeror's company. (5) Contracts, agreements, understandings, or arrangements between the Offeror's company and a foreign person. (6) Loan arrangements between the Offeror's company and a foreign person if the Offeror's company's (the borrower) overall debt to equity ratio is 40:60 or greater; or financial obligations that are subject to the ability of a foreign person to demand repayment. (7) Annual total revenues or net income in excess of 5 percent from a single foreign person or in excess of 30 percent from foreign persons in the aggregate. (8) Ten percent or more of any class of the Offeror's voting securities held in "nominee shares", in "street names", or in some other method that does not disclose the beneficial ownership of equitable title. (9) Interlocking directors with foreign persons and any officer or management official of the Offeror's company who is also employed by a foreign person. (10) Any other factor that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of the Offeror's company. (11) Ownership of 10 percent or more of any foreign interest. Every effort must be made to ensure that supplies are provided and integrated and services are performed using sound security components, practices, and procedures. Acquisition of supplies or services from concerns under Foreign Ownership, Control, or Influence (FOCI) or of supplies developed, manufactured, maintained, or modified by concerns under FOCI (any or all of which shall be referred to herein as "Use of FOCI source") is of serious concern and must be approved prior to contract award and evaluated during contract performance. Approval decisions will be made on a case by case basis after the source or technology has been identified by the Offeror and subjected to a risk assessment.

Any Offeror responding to this Request for Proposal (RFP), Request for Quotation (RFQ), or Sealed Bid acknowledges the Government's requirements to secure services or equipment from firms which are not an acquisition risk; are not under Foreign Ownership, Control, or Influence (FOCI); or where any FOCI, in the opinion of the Government, adversely impacts on National Security or security requirements. The Offeror understands and agrees that the Government retains the right to reject any response to this RFP, RFQ, or Sealed Bid made by the Offeror, without any further recourse by or explanation to the Offeror, if the acquisition risk for that Offeror is determined by the Government to be an unacceptable security risk. The risk assessment process will vary depending on the acquisition type and proposed use of a FOCI source, available risk mitigation measures, and the information/ justification provided by the Offeror. Risk assessments will be on a case by case basis and will be used to determine whether the use of a FOCI source poses an unacceptable security risk. If an unacceptable security risk is determined, the Government retains the right to reject the use of a FOCI source or to require that certain risk mitigation measures be taken by the contractor. Similarly, the Government retains the unilateral right to approve the use of a FOCI source when the risk assessment indicates that such use would be in the Governments' best interests.

If the use of a FOCI source is not approved, no classified information will be disclosed to the Offeror as part of the Government's rationale for non-approval. The Offeror (prime and subs) may not seek reimbursement from the Government for any costs associated with responding to this RFP, RFQ, or Sealed Bid, as a result of a FOCI non#approval decision.

DJAR-PGD-02-02B Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems

The Department of Justice (DOJ) will no longer permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction with respect to all new employees utilized directly to perform duties on the contract.

Non-U.S. citizens currently employees under this contract or commitment may continue performance unless otherwise directed by the Department of Justice. No new, replacement, or additional Non-U.S. citizens may be added to the contract without the express approval of the Department of Justice. [In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.].

(End of Clause)

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the

U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E- Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800- 37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to- date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ;

and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has
(a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ- CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by theDOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO),

acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

FBI-0010 Warrantless Search - Contract Security Requirements from Acquisition Security Unit (ASU)

All cleared personnel accessing information within FBI controlled space are required to execute an FBI Form FD 1001 Consent for Warrantless Searches of Department of Justice (DOJ) Workplaces as a condition of working at FBI facilities. The FBI's Director implemented the Attorney General's policy subjecting employees to warrantless physical searches of their offices or immediate workplaces within DOJ premises when authorized by the Attorney General (AG) or the Deputy Attorney General (DAG) based upon a determination that information the Department deems credible indicates that the employee: 1) is, or may be, disclosing classified information in an unauthorized manner; 2) has incurred excessive indebtedness or has acquired a level of affluence that can not be reasonably explained by other information; 3) had the capability and opportunity to disclose classified information that is believed to have been lost or compromised to a foreign power or an agent of a foreign power; or 4) has repeatedly or significantly mishandled or improperly stored classified information. The search may extend to the entire office or workplace and anything within it that might hold classified information, including locked containers (such as briefcases) and electronic storage media (such as computer disk

and handheld computers), whether owned by the government, by the employee, or by a third party. The search may be conducted by appropriate FBI personnel and/or law enforcement officers, on an announced or unannounced basis, during the workday or after hours. If discovered during a search, evidence of misconduct - whether related to storage or classified information, storage of sensitive but unclassified information, or a crime - will be collected and reported to appropriate authorities. Contractor personnel who will meet the above criteria will be required to sign Form FD 1001 Consent for Warrantless Searches of Department of Justice (DOJ) Workplaces (attached) upon award and forward the executed form(s) to the assigned Contracting Officer's Representative designated in Section G of the solicitation if this is a formal solicitation or listed below. All forms will be retained by the FBI during the period the individual is providing services and two years after that individual's departure before final disposition is taken.

FBI-0002 Classified Contracts - Contract Security Requirements from Acquisition Security Unit (ASU)

The FBI has determined that performance of this effort requires that the Contractor have access to classified National Security Information (herein known as classified information). Classified information is Government information, which requires protection in accordance with Executive Order 12356, Classified National Security Information, and supplementing directives. Executive Order 13292, dated 28 March 2003, "Further Amendment to Executive Order 12356, as amended, "Classified National Security Information" and implementation directives, provides principles and procedures for the proper classification and declassification of material. These principles and procedures are applicable to classified documents or materials generated by the contractor in performance of this contract. This clause applies to the extent that this contract involves access to information classified (select either "Confidential", "Secret" or "Top Secret"). The contractor shall comply with: (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M) (2) Any revisions to that manual, notice of which has been furnished to the contractor. The Contractor shall abide by the requirements set forth in the DD Form 254 and the National Industrial Security Program Operating Manual (NISPOM), DoD 5200.22-M) for the protection of classified information at its cleared facility, if applicable, as directed by the DSS. If the Contractor has access to classified information at a FBI or other Government facility, it shall abide by the requirements set by the agency. No classified document or material provided by the FBI, or generated by the contractor pursuant to the contract, may be downgraded or declassified unless authorized in writing by the CO. The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual shall interface with the FBI Security Office on all security matters, to include physical, personnel and protection of all Government information and data accessed by the Contractor. Contractor personnel will require access to classified information and have access to classified areas. Contractor personnel shall possess at least an active and transferable Government Secret clearance at the time of proposal submission. Contractors who will have access to FBI facilities, systems or data shall possess an active and transferable Top Secret clearance at the time of proposal submission. The Government reserves the right to waive this requirement for any portion of the work that deals with technologies or data that is in the public domain. Contractor personnel assigned to this project shall be subject to routine criminal and credit checks by the FBI. Contractor personnel shall be subject to counterintelligence focused polygraph examinations at the Government's discretion. The polygraph examinations may be required prior to acceptance or at any time during the task order, without notice. The contractor shall maintain an overall security program in accordance with the requirements of the NISP. All automated information systems utilized to process FBI information will be operated in accordance with the requirements of the NISPOM, NISPOM Supplement, dated February 1995, DCID 6/3 and/or FBI certification and accreditation policies and procedures, as appropriate. Revisions to these documents, when published, will be provided to the contractor and will become a part hereof upon such issuance. If subsequent to the date of this contract, the security classification or security requirements under this contract are caused to be changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract. The contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph, but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information. The contractor is obligated to comply with all relevant clauses and provisions incorporated into this contract and with the Contractor Nondisclosure Agreement, and as referenced therein, the NISPOM, dated January 1995, and all applicable FBI security policies and procedures, including the DCIDs. As applicable, the contractor shall maintain a security program that meets the requirements of these documents. Security requirements are a material conduction of this contract. This contract shall be subject to immediate termination for default, without the requirement for a 10-day cure notice, when it has been determined by the CO that a failure to fully comply with the security requirements of this contract resulted from the willful misconduct or lack of good faith on the part of any one of the Contractor's directors or officers, or on the part of any of the managers, superintendents, or equivalents of the contractor who have supervision or direction of: a. All or substantially all of the contractor's business, or b. All or substantially all of the contractor's operations at any one plant or separate location in which this contract is being performed, or c. A separate and complete major industrial operation in connection with the performance of this contract. When deficiencies in the contractor's security program are noted which do not warrant immediate default, the contractor shall be provided a written notice of the deficiencies and be given a period of 90 days in which to take corrective action. If the contractor fails to take the necessary corrective action, the CO may terminate the whole or any part of this contract, for default. The contractor shall maintain and administer, in accordance with all relevant clauses and provisions set forth or incorporated into this contract, a security program that meets the requirements of these documents.

1.1 Financial Disclosure Requirements: Financial considerations and foreign travel have been identified as significant elements in recent espionage cases. In response to these threats, Executive Order 12968 established a requirement that all Executive Branch personnel who are granted access to "particularly sensitive classified information" as a condition of such access, file with the agency head an annual financial disclosure report. With the continuous dependency on contractors to support the FBI, to include access to classified information, if a procurement is expected to result in the acquisition of services involving the assignment of contractor personnel to FBI locations, access to Sensitive Compartmented Information (SCI) and access to the FBI's Secret Network (FBINET) the Program Management Officer/Contracting Officer's Representative (COR), in coordination with the assigned Chief Security Officer, are required to identify during procurement planning stages, whether an acquisition will require the anticipated contract to include the Special Security Requirement identified below.

1.2 Special Security Requirement: Security Requirements Applicable to Contractor Personnel Assigned to FBI Locations, with Access to Sensitive Compartmented Information (SCI) and the FBI Secret Network (FBINET), or those selected by the Director or Deputy Director of the FBI. Requirements are applicable to all individuals to be assigned to FBI locations, to include those identified as "Key Personnel", if specified in the contract, who will require access to FBI locations, SCI and FBINET, or those selected by the Director or Deputy Director of the FBI. Award of this contract is anticipated to result in the assignment of contractor personnel to FBI controlled or occupied space with access to SCI and the FBINET. As such, all contractor personnel assigned to such space with access to SCI and FBINET, or those selected by the Director or Deputy Director of the FBI, are required to file an annual Security Financial Disclosure Form (SFDF). Information collected through these filings is used to help make personnel security determinations including whether to allow access to classified information, sensitive areas, and equipment; or to permit assignment to sensitive national security positions. The data may be subsequently used as part of a review process to evaluate continued eligibility for access to classified information or as evidence in legal proceedings. Upon request, contractor employees required to file must:

a. Submit an annual financial disclosure form electronically using the SFDF. The SFDF is a web-based form that is accessible only through the FBI Intranet. Every form submitted undergoes automated analysis, and is stored in a secure database;

b. Sign and submit two consent forms: Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act, (DOJ-555) and Personnel Consent to Release Information, (FD-979) to the assigned FBI Chief Security Officer. (These consent forms are used only if deemed necessary by the FBI in the event of a financial review. If a filer submitted the consent forms in a previous year, he/ she would be required to resubmit only the form if requested to do so by the assigned FBI Chief Security Officer);

c. Include all requested information pertaining to the filer, his or her spouse, and any dependent children. A filer whose spouse or dependent(s) refuse to provide financial information should explain the circumstances of this refusal in the Comments Section of the SFDF.

The filer may be subject to penalties, including having access to classified information suspended, revoked, or denied. Individual circumstances are reviewed on a case by case basis. d. Not omit or provide false or misleading information on an SFDF. Filings are reviewed for accuracy and completeness, and filers may be contacted by FBI employees/contractors assigned the responsibility of the Financial Disclosure Program regarding any potential discrepancies and/or omissions. Contractor employees who meet the sited criteria are required to file and are responsible for the successful completion of the SFDF process. Refusal to submit financial disclosure information could result in the immediate removal of the employee from FBI space, restricted access to FBI information or denial of unescorted access to FBI facilities. Exceptions will be resolved on a case-by-case basis. If contract performance is impacted as a result of removal of the employee, the contractor may be found in default of the contract. If a contractor employee terminates employment and/or assignment to the FBI prior to the reporting requirement, the contractor employee is not required to file.

(a) None of the funds made available by the Department's current Appropriations Act may be used to enter into a contract, memorandum of understanding, or cooperative agreement with a corporation -

(1) convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government, or

(2) that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability ,
unless an agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(b) By submitting a response to this solicitation, the offeror represents that, as of the date of this offer -

(1) the offeror is *not* a corporation convicted of a felony criminal violation under any Federal or State law within the preceding 24 months; and,

(2) the offeror is *not* a corporation that has any unpaid Federal or State tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

(End of Provision)

FBI-0003 Contracting Officer's Security Representative (COSR) - Contract Security Requirements from Acquisition Security Unit (ASU)

COSR are the designated representatives of the CO and derives their authorities directly from the CO. They are responsible for certifying the contractor’s capability for handling classified material and ensuring that customer security policies and procedures are met. The COSR is the focal point for the contractor, CO, and COR regarding security issues. The COSR cannot initiate any course of action that may alter the terms of the contract. The COSR is UC Saunders and can be reached on (202) 220-9230. The provisions of this clause shall apply to the extent that any aspect of this contract requires the contractor to access classified, of Sensitive But Unclassified and/or Law Enforcement Sensitive information. If, subsequent to the date of this contract, the security requirements under this contract are changed by the FBI, as provided in this clause, and the security costs or time required for delivery under this contract are thereby increased or decreased, the contract price, delivery schedule, or both, and any other provision of this contract which may be affected shall be subject to an equitable adjustment in accordance with the procedures in the Changes clause of this contract.

DJAR-PGD-07-12 Maintaining Contractor Performance During a Pandemic or Other Emergency

---

Continuing Contract Performance During a Pandemic Influenza or otherNational Emergency

During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce.

Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

The types of actions a federal contractor should reasonably take to help ensure performance are:

Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.

Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.

• Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.

• Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.

Establish communication processes to notify employees of activation of this plan.

• Integrate pandemic health crisis response expectations into telework agreements. With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.

• Determine how all employees who may telework will communicate with one another and with management to accomplish work.

Practice telework regularly to ensure effectiveness.

• Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.

• Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractors notification.

The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

(End of Clause)

DJAR-PGD-02-02A Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems

The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contractor commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction. [In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.].

(End of Clause)

FBI-0013 e-QIP - Contract Security Requirements from Acquisition Security Unit (ASU), Procurement Section Directive (PSD): 09-22.18

Performance under this contract may require access to FBI locations to provide some service, product, or perform some other official function of interest to the FBI. Requirements, as identified below, to include approval by the FBI's Security Division, must be satisfied prior to access. Contractors who will require escorted access, to include short-term, intermittent, or infrequent access, to an FBI facility must complete an "Access of Non-FBI Personnel to FBI Facilities, Background Data Information Form," (FD 816), a "Privacy Act of 1974 Acknowledgment Form" (FD 484) and two Fingerprint Cards (FD 258). Completed forms should be provided to the assigned Contracting Officer's Technical Representative (COTR) at least 10 days prior to required access. Individuals requiring unescorted access to an FBI facility must complete the Standard Form 86 (SF-86), Questionnaire for National Security Positions, using the Office of Personnel Management's Electronic Questionnaires for Investigations Processing (e-QIP) and provide two Fingerprint Cards (FD 258). e-QIP is a secure website that can be accessed from any computer system which has an Internet connection. Only the signed release forms and FD 258 will need to be mailed to the identified Chief Security Officer, the SF-86 itself will be transmitted to the FBI electronically. To complete the SF-86 using e-QIP, the individual requiring unescorted access to the FBI facility must contact (insert Chief Security Officer, Division, and telephone number) in order to be initiated into e-QIP. Once this action has been accomplished, the individual should be able to access e-QIP at the following link in order to initiate and complete the electronic process: http://www.opm.gov/e-qip/browser-check.asp. Thoroughly read and follow the instructions for completing the SF-86. NOTE: To fully address suitability/security issues, the FBI requires individuals to provide responses to questions on the SF-86 for the last ten years. Failure to complete the application as instructed may lead to significant delays in processing the required investigation and approval for unescorted access. Upon logging onto e-QIP, there will be a prompt to answer three "Golden" security questions to establish the user account. After completing the electronic SF-86, please print and sign the (1) Certification Form (CER) - Certify Completeness and Accuracy of your Investigation Request; (2) Medical Release Form (MEL) - Authorization for Release of Medical Information; and (3) Release Form (REL) - Authorization for Release of Information. In addition to these SF 86 release forms, the completion of a Non-Personnel Consent to Release Information (FD-979a), the United States Department of Justice Disclosure and Authorization Pertaining to Consumer Reports (DOJ 555) are required. Annotation of the assigned e-QIP Investigation Request Number on the upper right corner of each document transmitted to the identified Chief Security Officer is required for coordination with the electronic transmission and to facilitate the investigative process. The e-QIP Investigation Request Number, automatically generated by e-QIP, is located on both the header and footer of the signature forms. These release forms (five total) and FD 258 should be mailed via Federal Express or UPS Express mail directly to the following address: (insert name and address of Chief Security Officer). The use of regular U.S. mail channels may cause significant delays in processing the unescorted access request. Upon completion of processing the facility access request, the individual will be required to execute a non-disclosure agreement suitable for their approved access.

FBI-0006 (U) Contractor Suitability Special Security Requirement (SSR)

Access to FBI facilities and information is subject to specific security and suitability requirements. The FBI reserves the right and prerogative to deny and/or restrict facility and information access of any contractor employee determined by the FBI, at any time prior to or during performance, to be unsuitable for access and/or present a risk of compromising sensitive government information to which he or she would have access to under this contract. Contractors will be allotted a reasonable amount of time, determined by the government, to replace the employee found not suitable for contract performance. Failure to replace the employee may result in a no cost termination by the government.

FBI-0011 CARS Clause: Clauses for Contracts Involving Access to Classified Information - Contract Security Requirements from Acquisition Security Unit (ASU)

The Government intends to secure services or equipment from firms which are not deemed to be an acquisition risk. The Government reserves the right to contract with such Offerors under appropriate arrangements, when it determines that such contract will be in the best interest of the Government. Accordingly, all Offerors responding to this proposal or initiating performance of a contract are required to answer the acquisition risk questions located in Section K. All answers are to be reflective of the parent and subsidiary levels of an organization. Offerors are also required to request, collect, and forward to the Government answers to these acquisition risk questions from all subcontractors undertaking classified work under the Offeror's direction and control. Offerors are responsible for the thoroughness and completeness of each subcontractor's submission. Responses should specify, where necessary, the identity, nature, degree, and impact of any Foreign Ownership, Control, or Influence (FOCI) on their organization or activities, or the organization or activities of a subcontractor.

Additionally, a Key Management Personnel Listing (KMPL) must be submitted for each entity for which acquisition risk information is required. The KMPL must identify senior management by full legal name, position, social security number, date/place of birth, and citizenship status. The Offeror shall, in any case in which it believes that foreign influence exists or is being sought over its affairs, or the affairs of any subcontractor, promptly notify the Contracting Officer's Security Representative of all pertinent facts.

The Selected Offeror shall promptly disclose to the Contracting Officer's Security Representative any information pertaining to any interest of a FOCI nature in the Selected Offeror or subcontractor that has developed at any time during the Selected Offeror's duration or has subsequently come to the Selected Offeror's attention. Written notification to the Contracting Officer is required of the Selected Offeror or any subcontractor whenever there is a change in response to any of the acquisition risk questions. The Offeror is responsible for initiating the submission of the required risk acquisition information and KMPL for all subcontractors undertaking classified work during the entire period of performance of the contract. Failure to comply shall be cause for default under the Default Clause of this contract.

In Section K, Offerors shall complete the Acquisition Risk Questions and Key Management Personnel Listing (KMPL) for the prime contractor and all proposed subcontractors. Provision of false information shall be cause for default under the Default Clause of this contract. The information in Section K regarding Key Management Personnel, which may identify U.S. persons, is being requested pursuant to the National Security Act of 1947, as amended, and Director of Central Intelligence Directive 7/6, Community Acquisition Risk Center, or superseding Acts or Directives. The FBI will use this information to conduct the acquisition risk determination and may share the information internally and externally with members of the Intelligence Community and other U.S. Government entities, if necessary, consistent with appropriate routine uses for its Central Records System (CRS), Justice/FBI-002, last published in full in the Federal Register on February 20, 1998 (63 Fed. Reg. 8671), or any updates thereto. In the absence of proof of death of any of the Key Management Personnel, their consent, or an overriding public interest, the information will not otherwise be disseminated except pursuant to the routine uses for the CRS. The Government reserves the right to prohibit individuals who are not
U.S. citizens from all or certain aspects of the work to be performed under this Contract.

Foreign Ownership, Control, or Influence (FOCI) - For purposes of this clause, a U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company. Changed conditions, such as change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating, or, alternatively, that different acquisition risk mitigation measures be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be an acquisition risk. There is a continuing obligation of the Selected Offeror to advise the Government of such changed conditions. Failure to abide by this obligation shall be cause for default under the Default Clause of this contract.

Factors: The following factors will be used as the basis for making an acquisition risk determination. If the Offeror, or its proposed subcontractors, meet any of the following factors, they must identify themselves as a potential FOCI company and submit themselves for a Government acquisition risk evaluation and assessment:
(1) Ownership or beneficial ownership, direct or indirect, of 5 percent or more of the Offeror's company's voting securities by a foreign person. (2) Ownership or beneficial ownership, direct or indirect, of 25 percent or more of any class of the Offeror's company's non- voting securities by a foreign person. (3) Management positions, such as directors, officers, or executive personnel of the Offeror's company held by non-U.S. citizens.(4) Foreign person power, direct or indirect, to control the election, appointment, or tenure of directors, officers, or executive personnel of the Offeror's company or other decisions or activities of the Offeror's company. (5) Contracts, agreements, understandings, or arrangements between the Offeror's company

and a foreign person.(6) Loan arrangements between the Offeror's company and a foreign person if the Offeror's company's (the borrower) overall debt to equity ratio is 40:60 or greater; or financial obligations that are subject to the ability of a foreign person to demand repayment. (7) Annual total revenues or net income in excess of 5 percent from a single foreign person or in excess of 30 percent from foreign persons in the aggregate. (8) Ten percent or more of any class of the Offeror's voting securities held in "nominee shares", in "street names", or in some other method that does not disclose the beneficial ownership of equitable title. (9) Interlocking directors with foreign persons and any officer or management official of the Offeror's company who is also employed by a foreign person. (10) Any other factor that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of the Offeror's company. (11) Ownership of 10 percent or more of any foreign interest. Every effort must be made to ensure that supplies are provided and integrated and services are performed using sound security components, practices, and procedures.

Acquisition of supplies or services from concerns under Foreign Ownership, Control, or Influence (FOCI) or of supplies developed, manufactured, maintained, or modified by concerns under FOCI (any or all of which shall be referred to herein as "Use of FOCI source") is of serious concern and must be approved prior to contract award and evaluated during contract performance. Approval decisions will be made on a case bycase basis after the source or technology has been identified by the Offeror and subjected to a risk assessment. Any Offeror responding to this Request for Proposal (RFP), Request for Quotation (RFQ), or Sealed Bid acknowledges the Government's requirements to secure services or equipment from firms which are not an acquisition risk; are not under Foreign Ownership, Control, or Influence (FOCI); or where any FOCI, in the opinion of the Government, adversely impacts on National Security or security requirements. **The Offeror understands and agrees that the Government retains the right to reject any response to this RFP, RFQ, or Sealed Bid made by the Offeror, without any further recourse by or explanation to the Offeror, if the acquisition risk for that Offeror is determined by the Government to be an unacceptable security risk.**

The risk assessment process will vary depending on the acquisition type and proposed use of a FOCI source, available risk mitigation measures, and the information/justification provided by the Offeror. Risk assessments will be on a case by case basis and will be used to determine whether the use of a FOCI source poses an unacceptable security risk. If an unacceptable security risk is determined, the Government retains the right to reject the use of a FOCI source or to require that certain risk mitigation measures be taken by the contractor. Similarly, the Government retains the unilateral right to approve the use of a FOCI source when the risk assessment indicates that such use would be in the Governments' best interests. If the use of a FOCI source is not approved, no classified information will be disclosed to the Offeror as part of the Government's rationale for non approval. The Offeror (prime and subs) may not seek reimbursement from the Government for any costs associated with responding to this RFP, RFQ, or Sealed Bid, as a result of a FOCI non#approval decision.

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)

DJAR-PGD-15-02-2C Contractor Certification of Compliance with Federal Tax Requirements – Award (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that, to the best of its knowledge and belief, the contractor has (a) filed all Federal tax returns requires during the three years preceding the certification, (b) not been convicted of a criminal offense under the Internal Revenue Code of 1986, and (c) not been notified, more than 90 days before the subject certification, of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a non-frivolous administrative or judicial proceeding.

(End of Clause)

2.8 REQUIREMENTS FOR QUOTE PREPARATION

1. All vendors shall have an Active UEI number in SAM.GOV
2. Quote shall be firm fixed price
3. Quote shall be submitted to the Contracting Officer via e-mail at hnguyen2@fbi.gov before closing date and time.

QUOTE SHALL ALSO INCLUDE:
Please be sure the quote clearly indicates the following information:
Company Name
Address
Contract Name
Phone/FAX/E-mail
TIN

DUNS&UEI:
Company Size: **small**
Payment Terms: **NET 30**
FOB: **Destination**

2.9 EVALUATION AND AWARD PROCESS

This will be awarded based on the Lowest Price Technically Acceptable. To be considered technically acceptable the vendor shall quote all required services, be able to meet the required completion date, complete and submit the vendor responsibility determination sheet with their quote. The award will be based on the firm fixed price quote with NET 30 payment terms. All invoices shall be submitted through IPP for payment after delivery has been completed.

2.10 PROCESS SCHEDULE

The FBI anticipates awarding this contract within 5 days after the RFQ closes. But all quotes shall be good for **60 days.**

2.11 POINTS OF CONTACT

All questions shall be directed to the Contracting Officer Hong Nguyen.
U.S. Department of Justice
Federal Bureau of Investigation
Regional Contracting Officer Program
4000 W. Metropolitan Drive
Suite 200
Orange, California 92686
E-mail: hnguyen2@fbi.gov

2.12 ATTACHMENTS

1. Vendor Determination of Responsibility Document- SHALL BE SUBMITTED WITH VENDORS QUOTE TO BE CONSIDERED TECHNICALLY ACCEPTABLE

IPP.GOV INFORMATION:

FBI IMPLEMENTATION OF INVOICE PROCESSING PLATFORM (IPP) ELECTRONIC INVOICING SYSTEM

The Federal Bureau of Investigation (FBI) is implementing an electronic invoicing system, the Invoice Processing Platform (IPP), to comply with the Office of Management and Budget's 2018 electronic invoicing mandate.
IPP is a secure, web-based electronic invoicing system provided by the U.S. Department of the Treasury's Bureau of the Fiscal Service in partnership with the Federal Reserve Bank of St. Louis (FRSTL). IPP is available at no cost to any commercial vendor or independent contractor doing business with a participating government agency. To learn more about IPP, please visit IPP.gov.

Beginning in January 2021, the FBI will progressively increase the number of contracts that it transmits to IPP. To prepare for this transition, please review the transition schedule and actions below.

Action to take:

If you are already enrolled in IPP:

If your company is already registered in IPP, you will not be required to re-register. Please contact your organization's IPP account administrator so that he/she may add you as an additional user to your company's vendor profile. If necessary, update and/or correct relevant user data in your company's IPP collector account. Additionally, please ensure that your company is registered in SAM.gov. Your company's Electronic Business POC in SAM.gov will be designated as an IPP administrator by default. This REQUEST FOR QUOTATION RFQ NO. DJF-21-3440-PR-0004406, SECURITY ACCESS EQUIPMENT (BRAND NAME ONLY FOR ME Page | 40 individual will be responsible for initial account registration as well as creating and managing your company's IPP users and permissions.

Upon notification by a Contracting Officer (signed purchase order, signed purchase order modification, etc.), please submit your invoices via the IPP system. The cover pages of applicable purchase orders and purchase order modifications will contain the following advisory: "Send all invoices via IPP, NOT central_invoices@fbi.gov."

If you are NOT already enrolled in IPP:

If your company is not registered to use IPP, no action in IPP is required at this point in time. The FBI will enroll your company by using the provided contact information relevant to your company in SAM.gov. Please ensure that your company is registered in SAM.gov. Your company's Electronic Business POC in SAM.gov will be designated as an IPP administrator by default. This individual will be responsible for initial account registration as well as creating and managing your company's IPP users and permissions. Please note that due to U.S. Department of the Treasury guidelines, IPP cannot set up User IDs using a shared email address.

1. To begin the IPP enrollment process, your company's designated Electronic Business POC in SAM.gov will receive two emails from IPP Customer Support (ipp.noreply@mail.eroc.twai.gov):

   - The first email contains the initial administrative IPP User ID
   - The second email, sent within 24 hours of receipt of the first email, contains a temporary password
   - You must log in with the temporary password within 30 days

2. Registration is complete when the initial administrative user logs into the IPP web site with the User ID and password provided and accepts the IPP rules of behavior. Additional user accounts, including administrators, can be created after initial login.

3. Upon notification by a Contracting Officer (signed purchase order, signed purchase order modification, etc.), please submit your invoices via the IPP system. The cover pages of applicable purchase orders and purchase order modifications will contain the following advisory: **"Send all invoices via IPP, NOT central_invoices@fbi.gov."**

Training:

Vendor training materials, including a first-time login tutorial, are available on the IPP.gov website. Once you have logged in to the IPP application, you will have access to user guides that provide step-by-step instructions for all IPP capabilities ranging from creating and submitting an invoice to setting up email notifications.
Live webinars are held monthly and provide a great opportunity to learn the basics of the system. See IPP.gov for more details.

Additional Support

IPP Customer Support Team is available Monday through Friday from 8:00 am to 6:00 pm EST

- Phone: (866) 973-3131
- Email: IPPCustomerSupport@fiscal.treasury.gov
- For answers to frequently asked questions, visit the Vendor FAQ page on the IPP.gov web site.

For general questions related to the FBI's transition to IPP, please send an email to IPP@fbi.gov.

For contract-specific questions, please contact the designated contracting officer for your contract.

We appreciate your patience and participation as we make this transition.