Request for Quotation #15JA0526Q00000066

This is a combined synopsis/solicitation for Grand Jury & Deposition Court Reporting Services (commercial items) for the U.S. Attorney's Office, Eastern District of Michigan, prepared in accordance with the format in FAR 12.202(b), as supplemented with additional information included in this notice. This announcement constitutes the only solicitation; quotes are being requested and a written solicitation will not be issued.

This acquisition is being conducted as a Small Business Set-Aside. All offerors are required to verify their small business status under NAICS code 561492 in their quote. Any quotes from offerors that do not meet the socioeconomic requirement and small business size standard will not be considered for award.

Specific instructions to offerors and minimum quote submission criteria are located in Section 7, *Addendum to 52.212-1- Instructions, Conditions and Notices to Offerors (Mar 2023)*

Questions in regard to this solicitation are due July 7, 2026 at 1:00 PM Eastern to the Contracting Officer via email at brandon.wish@usdoj.gov. Questions submitted after this deadline may not be responded to.

Quotes are due July 21, 2026 at 1:00 PM Eastern to the Contracting Officer via email at brandon.wish@usdoj.gov.

For further information regarding this solicitation, contact:

Brandon Wish
Contracting Officer
Executive Office for United States Attorneys
brandon.wish@usdoj.gov
803-297-2111

Section 1 - Supplies or Services and Prices/Costs

1.1 General

a) The Contractor shall provide Grand Jury & Deposition Court Reporting Services for the United States Attorney's Office (USAO), Eastern District of Michigan.

b) The period of performance for this contract will include a base year and four (4) one-year options as follows:

Base Year:	09/15/2026 – 09/14/2027
Option Year I:	09/15/2027 – 09/14/2028
Option Year II:	09/15/2028 – 09/14/2029
Option Year III:	09/15/2029 – 09/14/2030
Option Year IV:	09/15/2030 – 09/14/2031

Contract may be extended an additional six months pursuant to FAR 52.217-8, Option to Extend Services. In the event the contract is extended pursuant to FAR clause 52.217-8, Option to Extend Services, the prices for the most recent period shall apply.

c) The contract will be an Indefinite Delivery Indefinite Quantity (IDIQ) contract. Contract type will be Time-and-Materials (T&M).

d) No Government Furnished Property shall be provided.

e) Department of Labor wage rates are applicable. Specifically, Wage Determination #2015-4837 is applicable. See Attachment 3 – Wage Determination.

f) The Government requires the following for this effort:
- Minimum of two (2) court reporters
- One (1) videographer

g) All Contractor personnel who will have access to Grand Jury material will need to be cleared.

1.2 Minimum Guarantee, Order Limits, & Ceiling

a) The USAO will order a minimum guaranteed amount of $1,000.00 during the life of this contract. The minimum amount is not re-established with each option year.

b) The minimum order limit is $100.00 and the maximum order limit is TBD.

c) The contract ceiling is TBD.

d) Each order ceiling is established in the individual task order and in accordance with FAR 52.212-4 Alt I (i), the Contractor shall provide requisite notification in the event expenditures are expected to exceed 85% of current funding ceiling.

1.3 Pricing

a) All unit prices are fixed and includes, but are not limited to, labor (including supervision), material, equipment, facilities, fringe benefits, overhead, G&A, and profit necessary to provide the Grand Jury & Deposition Court Reporting services required. Travel is priced separately and referenced in Section 2.

b) For planning purposes only, the following general information is provided:

i. Under normal circumstances, Grand Jury at the Bay City location is scheduled on a recurring basis, commencing on a Wednesday, and then recurring every three weeks thereafter. It will not be scheduled for any specific Wednesday of each month, but instead, will be scheduled for the Wednesday occurring three weeks after each prior Grand Jury session.
ii. Historically, the average number of Grand Jury daily sessions per year has been 13-15.
iii. Under normal circumstances, Depositions occur usually only twice annually on no set schedule. Each session generally lasts about 2 hours.
iv. Historically, the average number of depositions per year has been 1-2.

Section 2 - Statement of Work

2.1 Overview

a) The Contractor shall provide all labor (including supervision), material, equipment, facilities, and whatever else may be needed to record and transcribe Grand Jury testimony and Depositions, on an "as needed" basis for the USAO specified in Section 1 in accordance with the terms, conditions, and Statement of Work set forth herein.

b) The location(s) where services may be requested and take place are listed below:

Grand Jury: U.S. District Court
1000 Washington Ave.
Bay City, MI 48708

Depositions: Anywhere within 50 miles of Bay City, MI.

2.2 Grand Jury Transcripts

a) **Scheduling of Grand Jury:** The USAO will notify the Contractor of the requirements for attendance at a Grand Jury no later than one business day before the scheduled session. Each request will set forth the date, place and time of the session. The Contractor shall reply stating they have received the work order by returning the signed work order form or other form of written acceptable as may be agreed upon by the USAO and Contractor and communicate the name of the reporter who will be in attendance. The same individual reporter shall be available for the whole duration of the day as opposed to splitting daily services between two or more (e.g. one reporter for morning and another for afternoon) to provide continuity and consistency of services. Any change will be communicated by the Contractor to the USAO prior to the session. In the event a Grand Jury session is continued for more than one day, the Contractor will make reasonable efforts to assign the same court reporter for each continued segment of that given Grand Jury session. Should the Contractor not be able to provide the same court reporter, it will notify the USAO authorized Point of Contact before the Grand Jury session that another court reporter will be providing the court reporting services.

b) **Original Transcripts.** Unless otherwise stated, Grand Jury testimony shall be typed in an original and delivered within the turnaround times as set forth below. All Grand Jury transcripts shall contain (at a minimum) a title page stating the witness's name, Grand Jury date, time of the commencement of the proceeding for that particular witness, name, title and address of the attorney appearing for the Government. The title page should also include the Grand Jury number of the case, i.e., 07 GJ 999, and the name of the Federal Grand Jury that the witness is appearing before. Transcripts may be ordered by the USAO within the following timeframes. Billing rates for these turnaround times are set forth in the Pricing Schedule of this contract.

i. **10 Business Day Transcripts:** Transcripts will be completed and delivered on or before the 10th business day after the Contractor receives a request from the USAO. Transcripts shall be delivered to the USAO of each witness's testimony, only when requested by the USAO. Colloquy will not be transcribed unless requested by the USAO, in which case the transcript shall be completed and delivered on or before the 10th business day after the Contractor receives a request from USAO.

ii. **5 Business Day Transcripts:** Transcripts shall be completed and delivered on or before the 5th business day after the Contractor receives a request from the USAO. This request will sometimes be made the same day as the proceedings.

iii. **3 Business Day Transcripts:** Transcripts shall be completed and delivered on or before the 3rd business day after the Contractor receives a request from the USAO. This request will sometimes be made the same day as the proceedings.

iv. **Next Business Day Transcripts**: Transcripts shall be delivered before 9:30am of the following business day after conclusion of each day's proceedings. This may require performance after normal business hours. The Contractor may not be notified in advance of the testimony of this requirement.

v. **Additional Copies of Transcripts:** The Government has the right to copy and distribute transcripts acquired under this contract, however, the Government may order additional copies of any transcript. Additional copies of transcripts shall be provided to the USAO, as ordered, within the same turnaround times as set forth above.

vi. **Attendance Fee.** The Contractor is entitled to an Attendance Fee as set forth in the Pricing Schedule of this contract. The fee is payable for each hour the Contractor's reporter appears at a scheduled proceeding. The minimum charge for any single day is three (3) hours total for the Contractor, not for each individual reporter. Attendance fees will be paid for each hour the Contractor's reporter appears for a scheduled proceeding. Proceedings are presently scheduled for 9:30am to 1:30pm, but may go to 4:30pm. The Contractor is not paid during any lunch break. These hours are subject to change. The Contractor will generally be asked to report at 9:00am and be dismissed after the session concludes. A shorter day may be scheduled. The Government guarantees payment of a minimum of three (3) hours. In the event that there are time periods during the day during which no testimony is taken, and the reporter is required to remain available for testimony later in the day, the Contractor will be paid the hourly attendance fee during those time periods. In the event that a reporter's presence is required for a whole day and no testimony is recorded, the Contractor will be paid one (1) cancellation fee or the number of hours the reporter was available, whichever is higher.

vii. **Cancellation Fee.** The Contractor may wish to charge a cancellation fee. The Government will notify the contractor by telephone of any cancellations no later than 5:00pm the day before the scheduled proceedings. If the USAO does not notify the contractor within the designated time, the contractor may request a cancellation fee.

viii. **Other Requirements.** As follows:

- A transcript of all witness testimony shall be produced only when the USAO makes a specific request that a transcript be produced. Some witness testimony may never be transcribed. Colloquy will not be transcribed unless the USAO requests it.
- Each witness' testimony shall be in a separate transcript.
- If the USAO does not request that a transcript be produced, charging for estimated pages shall NOT be allowed. Only the Attendance fee will be paid.
- Grand Jury transcripts shall not be sold nor provided to anyone other than the Government under any circumstances.

ix. **Delivery.** See Section "EOUSA AI-10-1E Federal Grand Jury Court Reporter Security Requirements (December 2015)." The Government will request that deliverables be sent via USAfx.

c) **Grand Jury Travel and Per Diem Reimbursement Restrictions:**

The Contractor(s), when Grand Jury sessions are located within a 50-mile radius of the locations identified in Section 2.1(b), shall not be entitled to travel reimbursements. Travel required outside the 50-mile radius is allowable and shall be pre-approved in writing by the Contracting Officer's Representative or Contracting Officer prior to traveling. Travel expenses shall be reimbursed in accordance with the Federal Travel Regulations (FTR). The FTR can be found at this address: https://www.ecfr.gov/current/title-41/subtitle-F.

Travel reimbursement restrictions: Travel exceptions may be considered on a case-by-case basis at the sole discretion of the Contracting Officer's Representative (COR), or the Contracting Officer and these exceptions will be reimbursed in accordance with the Federal Travel Regulations (FTR). Travel expenses shall be reimbursed in accordance with the FTR, which can be found at this address: https://www.ecfr.gov/current/title-41/subtitle-F. All exceptions made for travel reimbursement must be pre-approved, in writing, by the Contracting Officer or Contracting Officer's Representative (COR) or the Contractor risks non-reimbursement

of travel expenses. The Contractor shall submit an itemized list of all estimated expenses to be claimed for each trip for pre-approval for any exceptions made.

d) **Certification.** Each reporter shall attach his/her official certification to the original transcript so recorded as follows:

CERTIFICATE

(I, We) hereby certify that the foregoing is a true and accurate transcript, to the best of (my, our) skill and ability, from my stenographic notes of this proceeding.

Date Court Reporter

There shall be no charge for either this certification page or any index page if used.

2.3 Deposition Transcripts

a) **Scheduling of Depositions:** The USAO will notify the Contractor of the requirements for attendance at a deposition no later than two business days before the scheduled session. Each request will set forth the date, place and time of the session. The Contractor shall reply stating they have received the work order by returning the signed work order form or other form of written acceptance as may be agreed upon by the USAO and communicate the name of the reporter who will be in attendance. The same individual reporter shall be available for the whole duration of the day as opposed to splitting daily services between two or more (e.g. one reporter for morning and another for afternoon) to provide continuity and consistency of services. Any change will be communicated by the Contractor to the USAO prior to the session. In the event a deposition is continued for more than one day, the Contractor will make reasonable efforts to assign the same court reporter for each continued segment of that given deposition. Should the Contractor not be able to provide the same court reporter, it will notify the USAO before the scheduled session that another court reporter will be providing the court reporting services.

b) **Original Transcripts**. Unless otherwise stated, depositions shall be typed in an original and delivered within the turnaround times as set forth below. Transcripts may be ordered by the USAO within the following timeframes. Billing rates for these turnaround times are set forth in the Pricing Schedule of this contract.

i. **10 Business Day Transcripts:** Transcripts will be completed and delivered on or before the 10th business day after the Contractor receives a request from the USAO. Transcripts shall be delivered to the USAO of each witness's testimony, only when requested by the USAO. Colloquy will not be transcribed unless requested by the USAO, in which case the transcript shall be completed and delivered on or before the 10th business day after the Contractor receives a request from USAO.

ii. **5 Business Day Transcripts:** Transcripts shall be completed and delivered on or before the 5th business day after the Contractor receives a request from the USAO. This request will sometimes be made the same day as the proceedings.

iii. **3 Business Day Transcripts:** Transcripts shall be completed and delivered on or before the 3rd business day after the Contractor receives a request from the USAO. This request will sometimes be made the same day as the proceedings.

iv. **Additional Copies of Transcripts:** Even though the Government has the right to copy and distribute transcripts acquired under this contract, the Government may order additional copies of any transcript. Additional copies of transcripts shall be provided to the USAO, as ordered, within the same turnaround times as set forth above.

v. **Videographer Attendance Fee.** The Contractor is entitled to a Videographer Attendance Fee as set forth in the Pricing Schedule of this contract. This fee is payable for each hour the Contractor's videographer records a scheduled deposition. The minimum charge for any single day is three (3) hours. The

videographer is not paid during a lunch break. This hourly fee shall account for the price of the recording itself and submission.

vi. **Attendance Fee.** The Contractor is entitled to an Attendance Fee in the amount set forth in the Pricing Schedule of this contract**.** The minimum charge for any single day is three (3) hours total for the Contractor, not for each individual reporter. Attendance fees will be paid for each hour the Contractor's reporter appears for a scheduled deposition. The Contractor is not paid during a lunch break. The Government guarantees payment of a minimum of three (3) hours. In the event that there are time periods during the day during which no work is performed, and the reporter is required to remain available for later in the day, the Contractor will be paid the hourly attendance fee during those time periods. In the event that a reporter's presence is required for a whole day and no deposition is recorded, the Contractor will be paid either one (1) cancellation fee or the number of hours the reporter was available, whichever is higher. The Contractor shall allow the Government ten (10) working days to request deposition transcripts before assessing an attendance fee.

vii. **Cancellation Fee.** The contractor may wish to charge a cancellation fee. The Government will notify the contractor by telephone of any cancellations no later than 5:00pm the day before the scheduled deposition. If the Government does not notify the contractor within the designated time, the contractor may request a cancellation fee.

viii. **Other Requirements**. As follows:

- A transcript shall be produced only when the USAO makes a specific request that a transcript be produced. Colloquy outside the presence of the witness will not be transcribed unless requested by the USAO.
- Each deposition shall be in a separate transcript.

ix. **Delivery.** See Section "EOUSA AI-10-1E Federal Grand Jury Court Reporter Security Requirements (December 2015)." The Government may request that transcripts be submitted via USAfx.

c) **Depositions Travel and Per Diem Reimbursement Restrictions:**

The Contractor(s), when depositions are located within a 50-mile radius of the locations identified in Section 2.1(b), shall not be entitled to travel reimbursements. Travel required outside the 50-mile radius is allowable and shall be pre-approved in writing by the Contracting Officer's Representative or Contracting Officer prior to traveling. Travel expenses shall be reimbursed in accordance with the Federal Travel Regulations (FTR). The FTR can be found at this address: https://www.ecfr.gov/current/title-41/subtitle-F.

Travel reimbursement restrictions: Travel exceptions may be considered on a case-by-case basis at the sole discretion of the Contracting Officer's Representative (COR), or the Contracting Officer and these exceptions will be reimbursed in accordance with the Federal Travel Regulations (FTR). Travel expenses shall be reimbursed in accordance with the FTR, which can be found at this address: https://www.ecfr.gov/current/title-41/subtitle-F. All exceptions made for travel reimbursement must be pre-approved, in writing, by the Contracting Officer or Contracting Officer's Representative (COR) or the Contractor risks non-reimbursement of travel expenses. The Contractor shall submit an itemized list of all estimated expenses to be claimed for each trip for pre-approval for any exceptions made.

d) **Certification**. Each reporter shall attach his/her official certification to the original transcript so recorded as follows:

CERTIFICATE

I, (NAME OF REPORTER), a Shorthand Reporter and a Notary Public, do hereby certify that the foregoing witness, (NAME OF WITNESS), was duly sworn on the date indicated, and that the foregoing is a true and accurate transcription of my stenographic notes and is a true record of the testimony given by the foregoing witness.

I further certify that I am not employed by or related to any party to this action by blood or marriage and that I am in no way interested in the outcome of this matter.

In witness whereof, I have hereunto set my hand this day of , 20 .

There shall be no charge for either this certification page or any index page if used.

2.4 Recording Requisites

a) Recording hereunder shall be taken by reporters qualified in the operation of Steno-type equipment, Real Time recording, Computer Aided Transcription (CAT), Shorthand and/or monitored Multi-Microphone recording systems, and when permitted by the Presiding Official, by Steno mask. At the request of the USAO, recording shall also be taken by videotape. Regardless of the type of equipment used, it is mandatory that there be an accurate read back capability and that a back-up system be utilized. It is also mandatory that tape recording devices shall have a separate monitor head which shall allow the reporter to monitor the recorded tape.

i. **Monitored Multi-microphone Recording Systems**. The mandatory requirements follow:

- The Contractor's personnel shall operate and monitor the recording equipment at all times.
- The operating personnel shall provide to the USAO, prior to the commencement of each proceeding, a certification that the equipment is turned on and operating.
- The recording equipment utilized shall provide for the instant playback of testimony.
- The equipment shall be capable of recording as many as twenty-three grand jurors together in one room with the prosecutor and the witness.
- The system utilized shall have a back-up system to allow continuous recording of speakers. The Grand Jury hearings shall not be stopped for any reason such as the changing of a tape.
- The media shall be of such quality that there shall be no instances of inaudibility because of accents or words used by the speakers.
- The system shall be portable to allow for transportation of media to another location when an immediate decision is required by a Federal District Court Judge.
- The recording monitor shall be able to identify speakers.
- A back-up system shall be available so as not to delay the proceedings.
- The equipment utilized shall not pose any safety hazards due to exposed wires, cords, or for any other reason.

ii. **Steno Mask Recording**. The mandatory requirements in the event steno mask recording is permitted are as follows:

- The respective systems shall be of such quality as to ensure against error, misinterpretation, or loss of voice.
- The equipment shall contain simultaneous playback, listening, and pre-amplification.

iii. **Real Time Recording**. The steno machine is attached to the computer. As the steno types the strikes/words are translated into English onto the screen.

iv. **Computer Aided Transcription (CAT).** With this type of system, the steno strikes a key which is written onto a disk. The disk is inserted into an attachment to the computer and the information is brought up on the computer screen. Also, a back-up voice tape is made so that a re-verification can be made of the transcript.

v. **Video Recording.** Video recordings shall be submitted digitally via USAfx.

b) The Contractor, or the duly authorized employee, agent, or representative of the Contractor, shall present himself/herself to the person in charge of the proceedings and he/she shall at all times be governed by the

instructions of the Presiding Official in matters affecting the composition of the record, adjournment to other times or places, and matters of like character.

c) The Contractor shall give the Government its copy prior to the witness being presented their testimony. The Government may choose to present to the witness. In the event further information is desired, the above referenced volume is a part of the United States Code, Title 28 and may be found at any public library.

d) Everything spoken pertaining to the subject matter shall be reported, unless the Presiding Official otherwise directs. No part of any proceedings, of which notes have been taken as required, shall be omitted from the record, unless the Presiding Official so directs.

e) All notes, records, documentary exhibits, and any other material which is a part of, or relates to, any action recorded by the Contractor shall be the property of the United States and shall be delivered to the ordering office, together with furnished transcript, if requested.

f) Right to Remove Individual Reporter - It shall be an absolute right of the USAO to inform the Contractor through the Contracting Officer of the unacceptability of specific court reporters for Grand Jury work. The failure of the Contractor to provide a court reporter other than one designated unacceptable by the USAO shall provide a basis for the USAO's decision to obtain court reporting services from another source.

2.5 Transcript Format

a) All transcripts shall be provided to the USAO utilizing USAfx and be in searchable PDF format.

b) A separate transcript shall be provided for each witness/deponent. The title page shall show the name of the witness, Grand Jury date, time of the commencement of the proceeding for that particular witness, docket number, the date of proceedings, the name, title and address of the attorney appearing for the Government, caption of matter, etc. and shall be followed by a page of distinctive color indexing the exhibits where applicable.

c) The paging of the transcripts shall be in a single series by consecutive numbers regardless of the number of days consumed in the hearings, proceeding, etc., and the paging of the transcript in a hearing shall follow consecutively the paging of the last previous hearing in the same case.

d) Each copy of the transcript furnished to the USAO shall be bound with covers of good quality, white or colored 140 pound index paper, #1 sulphite paper, heavy weight transparent plastic, or similar material approved by the ordering office. Transcripts shall be punched with three holes at the left side; the upper and lower holes to be two inches from top and bottom of the page, third hole in the center of the resulting interval, and shall be secured with a suitable fastener of permanent nature.

e) All transcripts shall be typed with black ribbon or reproduced by regular office type duplicating machines on white linen unglazed paper of good quality, #30 white bond paper or similar stock, to be approved by the ordering office. Transcripts shall be typed on paper 8 ½ inches x 11 inches in size, with a ruled margin of 1 3/4 inches at the left side and 3/8 inch at the right side. Typing shall be 10 spaces to the inch, double spaced, and shall not be less than 25 lines to the page exclusive of the line containing the witness name, date of testimony, and page number. The lines of testimony are to be numbered on each page beginning with #1. These numbers will appear just to the left of the left ruled margin. Whenever testimony is continuous, requiring more than one line, the typing shall begin one blank space after the left hand ruled margin and shall continue to the right hand ruled margin, with no blank spaces. The distance between the left hand ruled margin and the right hand ruled margin will be 6 3/8 inches. Therefore, there will be no less than 60 characters per line available. No word should wrap to the next line that would properly fit within the 60 count. Pages necessarily containing less than 25 lines shall be charged and paid for at the full-page rate. No payment will be made for lines in excess of 25 lines to the page. The first line of Q and A's will be indented 5 spaces, then followed by a period and 3 blank spaces. The second line will return to one blank space after the left hand ruled margin. The first line of colloquy will be indented 10 spaces, followed by a period and 3 blank spaces. The second line will return to one blank space after the left hand ruled margin. No extraneous words should be used on the title page or at the

beginning of a witness' testimony. No statement that can properly fit on a line should be extended to an additional line. There should be no unnecessary blank lines unless absolutely necessary for readability. The USAO will be the sole judge of this format.

Reduced page transcripts (Condensed Transcripts) shall include four transcript pages in reduced format on a single 8 ½ x 11 inch page.

f) Exhibits admitted in evidence, identified in Grand Jury proceedings, when requested by the Government attorney shall be stamped, marked, numbered by the Contractor, and arranged in numerical order, as directed by the individual Assistant U.S. Attorney (AUSA) and shall be annexed to the transcript. The marking shall indicate clearly whether the exhibit is offered by the complainant, protestant, intervener, defendant, respondent, applicant, the ordering office, or other party of record. The numbering of exhibits shall be in a single series of consecutive numbers, regardless of the number of days consumed in the hearing, unless otherwise directed by the Presiding Official. The number of exhibits introduced at a hearing or in a reopened case shall follow consecutively the number on the last previous exhibit introduced by such party. Exhibits shall not be copied into the record nor shall photo static copies of exhibits for inclusion in the record be made by the reporter unless the Presiding Official so directs.

2.6 Availability/Sale of Transcripts

a) Recording of proceedings shall be transcribed by the Contractor only when directed by the USAO. In the handling of transcripts, the Contractor shall observe and comply with security requirements stipulated herein. Transcripts will not be made available to the public by the Contractor.

b) Pursuant to Public Law 92-463, the Government reserves the right to make Grand Jury transcripts available to the public at the actual cost of duplication.

2.7 Reports

The Contractor shall submit immediately, in writing, to the Contracting Officer and the USAO the following reports:

- Unauthorized Entry. A report on any information coming to his attention concerning unauthorized entry (actual, attempted, or threatened) at his facilities where work for the USAO is performed.
- Loss, Compromise or Suspected Compromise. A report on any loss, compromise or suspected compromise of transcripts, notes or other related material.
- Any change of ownership, including stock transfers that affect the control of the corporation.
- Change of operating or address of the facility.
- A report of any change during the performance of the contract in location of closed or restricted areas as established, including the creation of any new areas requiring approval of the United States Attorney (USA).
- A report of any change in the storage capability which would affect the information which the Contractor is required to safeguard.

The Contractor shall also maintain and keep available for review by the USAO a master index of the Grand Jury sessions, including the date, name of Grand Jury, name of case, name of AUSA(s), case number, name of witnesses and pages from those witnesses, and the name of the court reporter.

2.8 Orders

a) The Contracting Officer will provide funding at the Task Order level on Optional Form 347, which will state the amount of funding available for each ordering period. Services to be furnished will subsequently be ordered by the issuance of work orders (see Attachment 1) signed by the Contracting Officer's Representative (COR) or Authorized Individual(s) of the USAO (see Attachment 1).

b) All work orders issued hereunder are subject to the terms and conditions of this contract which shall take precedence in the event of conflict with any work order.

c) All work orders placed under this contract must contain the following information:

i. Date of Order
ii. Order Number
iii. Description of Service
iv. Place of Performance
v. Primary Point of Contact of the work order

A sample Court Reporting Ordering Form is located in Attachment 1.

d) In accordance with FAR 52.212-4 Alt I (i), the Contractor shall provide requisite notification in the event expenditures are expected to exceed 85% of current funding ceiling.

2.9 Key Personnel

a) The key personnel whom the Contractor shall furnish for the performance of this contract are as follows:

Name: TBD	Title: Court Reporter
Name: TBD	Title: Court Reporter
Name: TBD	Title: Videographer

b) The personnel specified above is/are considered to be essential to the work being performed hereunder. Prior to replacing any of the specified individuals, the Contractor shall immediately notify both the Contracting Officer and COR reasonably in advance and shall submit written justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the program. No replacement of personnel shall be made by the Contractor without the written consent of the Contracting Officer.

2.10 Notice to Proceed

Within ten (10) calendar days after the contract award, the USAO will furnish the Contractor with personnel security application forms. The Contractor shall complete and return to the COR all personnel security application forms within seven (7) calendar days after receipt. After a sufficient number of Contractor Personnel are cleared by the Government, a notice to proceed will be issued by the Contracting Officer or the Contracting Officer's Representative specifying a performance start date.

Section 3 - Packaging and Marking

All information and submittals, including receipts, forms, reports, and other materials provided to the CO or the COR shall be clearly marked with the IDIQ contract number and applicable task order number:

EOUSA IDIQ CONTRACT NUMBER: TBD

Section 4 - Inspection and Acceptance

Final inspection and acceptance of work performed, reports, and other deliverables shall be performed by the COR.

Section 5 - Deliveries or Performance

5.1 Period of Performance:

See Section 1

5.2 Place of Performance:

See Section 2

5.3 Performance Standards

Evaluation of the Contractor's overall performance in accordance with the performance standards set forth in this Statement of Work shall be conducted jointly by the COR and the Contracting Officer and shall form the basis of the Contractor's permanent performance record with regard to this contract.

Section 6 - Contract Administration Data

6.1 Contracting Officer

The Contracting Officer for this contract is: **Brandon Wish, Executive Office for U.S. Attorneys**

Written communications shall make reference to the contract number and shall be emailed to brandon.wish@usdoj.gov or mailed to the above address.

6.2 Payment/Invoice Requirements

Payment for actual work and services rendered under this contract will be made in accordance with the Prompt Payment Act. Invoices shall be submitted monthly at a minimum, preferably the first Monday of each month for work done in the preceding month. All invoices should reference the appropriate call number assigned at the time of ordering, the IDIQ number, the applicable annual Task Order number, and applicable CLINS. To constitute a proper invoice, the invoice must be submitted in accordance with FAR 52.212-4(g). In addition, the following information must appear on the invoice:

- Date service was performed
- Location service was performed
- Attorney's Name
- Grand Jury Number (for Grand Jury only)
- Name of witness
- Number of pages
- Cost per page
- Call Number

Invoices shall be submitted to: USAMIE.Invoices@usdoj.gov. All follow-up invoices shall be marked "Duplicate of Original."

6.3 Accounting and Appropriation Data

Accounting and Appropriation Data is assigned with each task order.

Section 7 – Clause & Provision Addendums

Addendum to 52.212-1 - Instructions, Conditions and Notices to Offerors

The Government plans to award a contract to the Offeror whose quote represents the best value solution. The CO may reasonably determine that the superior solution/approach merits a higher price, and therefore represents the best value to the Government. The CO, using sound business judgment will base the selection decision on the integrated assessment of the Statement of Work and the Offeror's capability as measured against the below evaluation factors. Quotation shall be prepared in accordance with and comply with the instructions contained within this RFQ. The technical submission will be evaluated separately from the price submission. The quote will be evaluated in accordance with the evaluation factors listed herein.

This acquisition is being conducted as a small business set aside. All offerors are required to verify their small business status under NAICS code 561492 in their quote. Any quotes from offerors that do not meet the socioeconomic requirement and small business size standard will not be considered for award.

Cover Page

Quote(s) shall be submitted with a cover page to include the following information:

- Company Name and Address
- Phone Number
- Point of Contact Name and E-Mail Address
- SAM UEI Code
- Small Business Qualification
- Contractor personnel location
- GSA Contract Number (if applicable)

In addition to the Cover Page, quotes(s) shall consist of three (3) separate volumes and contain the following information. The following factors shall be used to evaluate offerors, and the evaluation criteria for award are listed in order of importance as follows:

Volume I: Technical

Proposed Key Personnel (Section 2.9) - Offerors shall provide resumes of prospective key personnel. The proposed key personnel are:

- Minimum of two (2) court reporters
- One (1) videographer

The key personnel will perform the tasks identified in the Statement of Work. The resume(s) shall demonstrate the key personnel's qualifications to provide the requested services and demonstrate experience in projects of similar size, scope, complexity and results. The resumes shall list the Key Personnel's location, education, experience, security clearance level, and training, if any.

Proposed key personnel shall be available up to, and at the time of award. If, at any time after a quote is submitted, a proposed key personnel candidate is no longer available, the offeror shall notify the Government immediately. Quotes may be found technically unacceptable if the key personnel candidate is no longer available prior to the time of award.

Volume II: Past Performance

The Offeror will be evaluated based on their past performance experience. The Offeror shall submit up to three (3) past performance references of similar work and scope completed within three (3) years of this solicitation closing. Evaluation will be based on the relevancy of recent efforts accomplished by the Offeror.

Past performance information will also be accessed by the Government from available online databases, including sources such as the Contractor Performance Assessment Rating System (CPARS) and Systems for Award Management.

Volume III: Price

Offerors shall submit a complete price proposal as reflected in Attachment 2 - Pricing Schedule, to be evaluated. Do not include asterisks with exceptions or comments on these pages. Only state the unit price and total CLIN amount for each CLIN item except travel CLINs. Any additions to the pricing page other than the CLIN price in the space provided will not be considered. Quotes providing partial pricing may be considered non-responsive and subsequently, ineligible for award. If a CLIN is no charge, state N/C (instead of stating zero) in Unit Price Column. N/A's are not acceptable. All CLINs with an estimated quantity must have a unit price or state N/C.

All pricing and costs associated to provide the requisite services stated in this SOW herein shall be included within the pricing proposal. No additional line items nor additional charges will be added or considered post-award.

The Government may require additional pricing information to assist in determining the extent to which the price is fair and reasonable, and the pricing information shall be provided if requested. The Government will evaluate quotes for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

(End of addendum)

Addendum to 52.212-2 - Evaluation-Commercial Items (Nov 2021)

1 (Technical)
2 (Past Performance)
3 (Price)

Technical and past performance, when combined, are significantly more important than price.

(End of addendum)

2852.212-4 Contract Terms and Conditions, Commercial Items (FAR Deviation) (NOV 2020)

When a commercial item is contemplated (using FAR part 12 procedures or otherwise) and the contract will include FAR 52.212-4, the following replaces subparagraph (g)(2); paragraph (h); subparagraph (i)(2); paragraph (s); and paragraph (u), Unauthorized Obligations, of the basic FAR clause, and adds paragraph (w), as follows:
(g)(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment act regulations at 5 CFR part 1315, as modified by subparagraph (i)(2), *Prompt payment,* of this clause.
* * * * *
(h) *Patent indemnity.* Contractor shall indemnify and hold harmless the Government and its respective affiliates, officers, directors, employees, agents, successors and assigns (collectively, “Indemnities”) from and against any and all liability and losses incurred by the Indemnities that are (i) included in any settlement and/or (ii) awarded by a court of competent jurisdiction arising from or in connection with any third party claim of infringement made against Indemnities asserting that any product or service supplied under this contract constitutes infringement of any patent, copyright, trademark, service mark, trade name or other proprietary or intellectual right. This indemnity shall not apply unless Contractor shall have been informed within a reasonable time by the Government of the claim or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. This indemnity also shall not apply to any claim unreasonably settled by the Government which obligates Contractor to make any admission or pay any amount without written consent signed by an authorized officer of Contractor, unless required by final decree of a court of competent jurisdiction.
* * * * *
(i)(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations (5 CFR part 1315), with the following modification regarding the due date: For the sole purpose of computing an interest penalty due the Contractor, the Government agrees to inspect and determine the acceptability of any supply delivered or service performed specified in the invoice within thirty (30) days of receipt of a proper invoice from the Contractor, after which time, if no affirmative action has been taken by the Government to accept such supply or service, the supply or service will be deemed accepted and payment due thirty (30) days from the date of deemed acceptance. If the Government makes the determination that the item delivered or service performed is deficient or otherwise unacceptable, or the invoice is otherwise determined not to be a proper invoice, the terms and conditions of this paragraph regarding prompt payment will apply to the date the Contractor corrects the deficiency in the item delivered or service performed or submits a proper invoice. If actual acceptance occurs within the constructive acceptance period, the Government will base the determination of an interest penalty on the actual date of acceptance. The constructive acceptance requirement does not, however, compel Government officials to accept supplies or services, perform contract administration functions, or make payment prior to fulfilling their responsibilities.
* * * * *
(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:
(1) The schedule of supplies/services.
(2) The Assignments, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts provisions of the basic FAR clause at 52.212-4, and the Unauthorized Obligations and Contractor's Commercial Supplier Agreements—Unenforceable Clauses provisions of JAR 2852.212-4.
(3) FAR 52.212-5.
(4) Other paragraphs of the basic FAR clause at 52.212-4, with the exception of paragraph (o), Warranty, and those paragraphs identified in this deviation of 52.212-4.
(5) Addenda to this solicitation, contract, or order, including contractor's Commercial supplier agreements incorporated into the contract.
(6) Solicitation provisions if this is a solicitation.
(7) Paragraph (o), Warranty, of the basic FAR clause at 52.212-4.
(8) The Standard Form 1449.
(9) Other documents, exhibits, and attachments.
(10) The specification.
* * * * *
(u) *Unauthorized obligations.*
(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract or order is subject to any Commercial supplier agreement that includes any language, provision, or clause requiring the Government

to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (see 31 U.S.C. 1341), the following shall govern:
(i) Any such language, provision, or clause is unenforceable against the Government.
(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an "I agree" click box or other similar mechanism (*e.g.,* "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.
(iii) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement and have no effect.
(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.
* * * * *
(w) *Commercial supplier agreements—unenforceable clauses.* When any supply or service acquired under this contract or order is subject to a contractor's commercial supplier agreement, the following shall be deemed incorporated into such agreement and modifies and replaces any similar language, provision, or clause in such agreement. As used herein, "this agreement" means any contractor commercial supplier agreement:
(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:
(i) *Applicability.* This agreement is a part of a contract between commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR part 12).
(ii) *End user.* This agreement shall bind the Government as end user but shall not operate to bind the Government employee or person acting on behalf of the Government in his or her personal capacity.
(iii) *Law and disputes.* This agreement is governed by Federal law.
(A) Any language, provision, or clause purporting to subject the U.S. Government to the laws of any U.S. state, territory, district, or municipality, or the laws of a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted and shall have no effect.
(B) Any language, provision, or clause requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted and shall have no effect.
(C) Any language, provision, or clause prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted and shall have no effect.
(iv) *Continued performance.* Notwithstanding any other provision in this agreement, if the Contractor believes the Government to be in breach of this contract, order, or agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in subparagraph (d), Disputes, of FAR 52.212-4.
(v) *Arbitration; equitable or injunctive relief.* In the event of a claim or dispute arising under or relating to the contract, order, or this agreement, (A) binding arbitration shall not be used unless otherwise specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the Government only when explicitly provided by statute.
(vi) *Updating terms.*
(A) After award, the contractor may unilaterally revise terms if they are not material. Material terms are defined as:
(1) Terms that change Government rights or obligations;
(2) Terms that increase Government prices;
(3) Terms that decrease the overall level of service; or
(4) Terms that limit any other Government right addressed elsewhere in this contract.
(B) For revisions that materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.
(C) Any agreement terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provisions of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.
(vii) *Order of precedence.* Any Order of Precedence clause in any commercial supplier agreement is not enforceable against the Government. The applicable Order of Precedence for this contract, order, or agreement is FAR 52.212-4(s), as revised by JAR 2812.302 and 2852.212-4(s).
(viii) *No automatic renewals.* If any license or service tied to period payment is provided under this agreement (*e.g.,* annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by a properly warranted contracting officer, and any provision or term of any license or service purporting to provide for automatic renewal is unenforceable against the Government.
(ix) *Indemnification by the Government or end-user.* Any language, provision, or clause of this commercial supplier agreement requiring the Government or End-user to indemnify the commercial supplier or licensor is not enforceable against the Government.

(x) *Indemnification by the commercial supplier or licensor.* Any clause of this agreement requiring or permitting the commercial supplier or licensor to defend the Government as a condition of indemnifying the Government for any claim of infringement is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.
(xi) *Audits.* Any language, provision, or clause of this commercial supplier agreement permitting Contractor to audit the end user's compliance with this agreement is not enforceable against the Government. To the extent any language, provision or clause of this agreement permits Contractor to audit the Government's compliance under this contract, order, or agreement, such language, provision, or clause of this agreement is hereby stricken and replaced as follows:
"(A) If Contractor reasonably believes that the Government has violated the terms of this agreement with regard to the restrictions on authorized use and/or the number of authorized users, upon written request from Contractor, including an explanation of the basis for the request, DOJ will provide a redacted version of the Government's most recent Security Assessment and Authorization package (SAA) to Contractor on a confidential basis, so that Contractor may reasonably verify the Government's compliance with its obligations under this agreement. Contractor understands and agrees that the Government will remove or redact any information from the SAA that it reasonably believes may compromise (a) the security of the Government's information technology environment; (b) the confidentiality of any third-party proprietary or confidential information; (c) any confidential, sensitive law enforcement information; and (d) any other information that the Government believes may compromise a past, current, or prospective investigation, prosecution, or litigation. Notwithstanding the preceding, and subject to the Government's policies and procedures for such review, including but not limited to complying with all Government security requirements prior to being granted access to the Government's facilities, including the execution of appropriate confidentiality and/or non-disclosure agreements, the Government will arrange, upon Contractor's written request, for Contractor to view an un-redacted version of the SAA on Government premises. Contractor understands that Contractor will be provided a copy of the un-redacted SAA on Government premises only and that no un-redacted copy of the SAA, or any medium containing information relating to it, will be permitted to be removed from Government premises.
(B) The Contractor also understands and agrees that the Contractor shall make a request under this paragraph no more than on an annual basis and only during the period of the contract, and that any activities performed by Contractor under this clause will be performed at Contractor's expense, without reimbursement by the Government.
(C) Discrepancies found with regard to the restrictions on authorized use and/or the number of authorized users may result in a charge by Contractor to the Government. Any resulting invoice must comply with the proper invoicing and payment requirements specified in the contract. This charge, if disputed by the Government, will be resolved through the Disputes clause at 52.212-4(d); no payment obligation shall arise on the part of the Government until the conclusion of the dispute process."
(xii) *Taxes or surcharges.* Any taxes or surcharges which the Contractor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.
(xiii) *Non-assignment.* This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under FAR 52.212-4 (b), Assignment.
(xiv) *Confidential information.*
(A) During the term of this contract or order, either party may identify information as "confidential information," and there shall be no disclosure, dissemination, or publication of any such information except to the extent required for the performance of this contract or order and otherwise provided in this clause or by statute or regulation. Specifically, the parties agree that the party receiving confidential information may only disclose such information to its employees and contractors on a "need-to-know" basis to carry out the obligations of this contract or order, and that subcontractors performing under this Agreement are subject to the same stipulations provided in this provision. The parties also agree that this provision shall survive the termination of this contract or order, and any confidential information obtained or received which comes within these restrictions shall remain confidential, provided that the obligation to treat information as confidential shall not apply to information which is or becomes publicly available through no improper action of the receiving party; is or comes to be in the receiving party's possession independent of its relationship with the disclosing party; is developed by or becomes known to the receiving party without use of any confidential information of the disclosing party; or is obtained rightfully from a third party not bound by an obligation of confidentiality. Additionally, nothing in this contract or order shall restrict disclosure by the receiving party pursuant to any applicable law, including but not limited to the Freedom of Information Act, 5 U.S.C. 552, *et seq.,* or an order of any court of competent jurisdiction, provided that in either such case the receiving party gives prompt notice to the disclosing party to allow the disclosing party to interpose an objection to such disclosure, take action to assure confidential handling of the confidential information, or take such other action as it deems appropriate to protect its confidential information.
(B) The Government considers and hereby identifies as confidential any and all information related to any inquiries and/ or searches performed by the Government or by contractor at the Government's direction under this contract or order, including the subject of any such inquiry or search and any and all search terms, regardless of whether provided in writing or orally to Contractor, and Contractor agrees that it may only disclose such information to its employees and contractors

on a “need-to-know” basis to carry out the obligations of this contract or order and that it will not share, reveal, divulge, disclose, disseminate, or publicize any such information to any third party except as provided in this provision without the prior written approval of the Contracting Officer. Contractor also understands and agrees that any subcontractors performing under this contract or order are subject to the same stipulations and that Contractor may be held responsible for any violations of confidentiality by a subcontractor.
(C) These provisions are consistent with and do not supersede, conflict with, or otherwise alter an employee's obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by Executive orders and statutory provisions relating to whistleblower protection are incorporated into this contract and are controlling.
(D) The Government may share the terms, conditions and prices set forth in this Order with, and provide a copy of the Order to, other Executive branch agencies of the U.S. Government, provided that the Government shall ensure that other Executive branch agencies to which it provides such information will be required to treat all such information consistent with terms and conditions set forth in this Order.
(E) Notwithstanding anything in this agreement, the Government may retain any confidential information as required by law, regulation, or its internal document retention procedures for legal, regulatory, or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this Order.
(xv) *Authorized users.* Authorized users may include full and part-time employees of the Government, including those working at or from remote locations, and contractors and contractor employees working within the scope of their contract with the Government, including those at or from remote locations.
(xvi) *Authorized use.* Authorized users are authorized to use the product or service acquired under this contract in performing business on behalf of the Government. Any information obtained or acquired by the Government under this contract may be used by the Government in the performance of Government business.
(2) If any language, provision, or clause of this agreement conflicts or is inconsistent with the preceding paragraph (w)(1), the language, provisions, or clause of paragraph (w)(1) shall prevails to the extent of such inconsistency.

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)		
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov		
Clause	Title	Fill-ins (if applicable)
52.203-17	Contractor Employee Whistleblower Rights (Nov 2023)	
52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements--Representation (Jan 2017)	
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)	

Clause	Title	Fill-ins (if applicable)
52.204-7	System for Award Management (Nov 2024)	
52.204-13	System for Award Management Maintenance (Oct 2018)	
52.209-6 (DEV)	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (Jan 2025) (DEVIATION NOV 2025)	
52.209-10 (DEV)	Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015) (DEVIATION NOV 2025)	
52.212-1	Instructions, Conditions and Notices to Offerors	
52.212-2	Evaluation-Commercial Products and Commercial Services (Nov 2021)	
52.212-4 Alt I	Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2023) - Alternate I (Nov 2021)	
52.219-6 (DEV)	Notice of Total Small Business Set-Aside (Nov 2020) (DEVIATION DEC 2025)	
52.222-3 (DEV)	Convict Labor (June 2003) (DEVIATION DEC 2025)	
52.222-36 (DEV)	Equal Opportunity for Workers with Disabilities (Jun 2020) (DEVIATION DEC 2025)	
52.222-50 (DEV)	Combating Trafficking in Persons (Oct 2025) (DEVIATION DEC 2025)	
52.224-1	Privacy Act Notification (Apr 1984)	
52.224-2	Privacy Act (Apr 1984)	
52.224-3	Privacy Training (Jan 2017)	
52.226-8	Encouraging Contractor Policies To Ban Text Messaging While Driving (May 2024)	
52.232-33	Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)	
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Mar 2023)	
52.233-3 (DEV)	Protest after Award (Aug 1996) (DEVIATION NOV 2025)	

Clause	Title	Fill-ins (if applicable)
52.233-4 (DEV)	Applicable Law for Breach of Contract Claim (Oct 2004) (DEVIATION NOV 2025)	
52.240-90 (DEV)	Security Prohibitions and Exclusions Representations and Certifications (DEVIATION NOV 2025)	
52.240-91 (DEV)	Security Prohibitions and Exclusions (DEVIATION NOV 2025)	
52.240-93 (DEV)	Basic Safeguarding of Covered Contractor Information Systems (DEVIATION NOV 2025)	

Clauses By Full Text

52.216-18 Ordering (Aug 2020)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from 09/15/2026 through 09/14/2031 [*insert dates*].

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) A delivery order or task order is considered "issued" when--

(1) If sent by mail (includes transmittal by U.S. mail or private delivery service), the Government deposits the order in the mail;

(2) If sent by fax, the Government transmits the order to the Contractor's fax number; or

(3) If sent electronically, the Government either--

(i) Posts a copy of the delivery order or task order to a Government document access system, and notice is sent to the Contractor; or

(ii) Distributes the delivery order or task order via email to the Contractor's email address.

(d) Orders may be issued by methods other than those enumerated in this clause only if authorized in the contract.

(End of clause)

52.216-19 Order Limitations (Oct 1995)

(a) *Minimum order*. When the Government requires supplies or services covered by this contract in an amount of less than $1.00 [*insert dollar figure or quantity*], the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order*. The Contractor is not obligated to honor--

(1) Any order for a single item in excess of TBD [*insert dollar figure or quantity*];

(2) Any order for a combination of items in excess of TBD [*insert dollar figure or quantity*]; or

(3) A series of orders from the same ordering office within 1 days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (*i.e.*, includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 1 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

52.216-22 Indefinite Quantity (Oct 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; *provided*, that the Contractor shall not be required to make any deliveries under this contract after 09/14/2031 [*insert date*].

(End of clause)

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 7 days [*insert the period of time within which the Contracting Officer may exercise the option*].

(End of clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 7 days [*insert the period of time within which the Contracting Officer may exercise the option*]; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days [*60 days unless a different number of days is inserted*] before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months (months)(years).

(End of clause)

2852.201-70 Contracting Officer's Representative (COR) (NOV 2020)

(a) Mr./Ms. TBD of TBD , TBD , TBD , is hereby designated to act as Contracting Officer's Representative (COR) underTBD , for the period of TBD (specify the performance period of the contract that the designation covers).
(b) Performance of work under this contract is subject to the technical direction of the COR identified above, or another representative designated in writing by the Contracting Officer. The term “technical direction” includes, without limitation, the following:
(i) Receiving all deliverables;
(ii) Inspecting and accepting the supplies or services provided in accordance with the terms and conditions of this contract;
(iii) Clarifying, directing, or redirecting the contract effort, including shifting work between work areas and locations, filling in details, or otherwise serving to accomplish the contractual statement of work to ensure the work is accomplished satisfactorily;
(iv) Evaluating performance of the Contractor; and
(v) Certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.
(c) The COR does not have the authority to issue direction that:
(i) Constitutes a change of assignment or work outside the contract specification/work statement/scope of work.
(ii) Constitutes a change as defined in the clause entitled “Changes” or other similar contract term.
(iii) Causes, in any manner, an increase or decrease in the contract price or the time required for contract performance;
(iv) Causes, in any manner, any change in a term, condition, or specification or the work statement/scope of work of the contract;
(v) Causes, in any manner, any change or commitment that affects price, quality, quantity, delivery, or other term or condition of the contract or that, in any way, directs the contractor or its subcontractors to operate in conflict with the contract terms and conditions;
(vi) Interferes with the contractor's right to perform under the terms and conditions of the contract;
(vii) Directs, supervises, or otherwise controls the actions of the Contractor's employees or a Subcontractor's employees.
(d) The Contractor shall proceed promptly with performance resulting from the technical direction of the COR. If, in the opinion of the Contractor, any direction by the COR or the designated representative falls outside the authority of (b) above and/or within the limitations of (c) above, the Contractor shall immediately notify the Contracting Officer.
(e) Failure of the Contractor and Contracting Officer to agree that technical direction is within the scope of the contract is a dispute that shall be subject to the “Disputes” clause and/or other similar contract term.
(f) COR authority is not re-delegable.

(End of Clause)

2852.203-70 General Non-Disclosure Agreement (AUG 2016)

The provisions of this Non-Disclosure Agreement (NDA) are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive Order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this agreement and are controlling.
(End of Provision)

2852.222-70 Domestic Violence, Sexual Assault, and Stalking (DEC 2014)

(a) It is DOJ policy to enhance workplace awareness of and safety for victims of domestic violence, sexual assault, and stalking. This policy is summarized in “*DOJ Policy Statement 1200.02, Federal Workforce Responses to Domestic Violence, Sexual Assault, and Stalking,”* available in full for public viewing at: *http://www.justice.gov/sites/default/files/ovw/legacy/2013/12/19/federal-workplacee-responses-to-domesticeviolence-sexualassault-stalking.pdf.*
Vendor agrees, upon contract award, to provide notice of this Policy Statement, including at a minimum the above-listed URL, to all Vendor employees and employees of subcontractors who will be assigned to work on DOJ premises.
(b) Upon contract award, DOJ will provide the Contractor with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking for the component or components where the Contractor will

be performing. The Contractor agrees to inform its employees and employees of subcontractors, who will be assigned to work on DOJ premises, with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking.
(End of Clause)

2852.223-70 Unsafe Conditions Due to the Presence of Hazardous Material (NOV 2020)

(a) “Unsafe condition” as used in this clause means the actual or potential exposure of Contractor or Government employees to a hazardous material.
(b) “Hazardous Material” as used in this clause includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract), any other potentially hazardous material requiring safety controls, or any other material or working condition designated as hazardous by the Contracting Officer's Representative (COR).
(c) The Occupational Safety and Health Administration (OSHA) is responsible for issuing and administering regulations that require Contractors to apprise its employees of all hazards to which they may be exposed in the course of their employment; proper conditions and precautions for safe use and exposure; and related symptoms and emergency treatment in the event of exposure.
(d) Prior to commencement of work, Contractors are required to inspect for and report to the Contracting Officer the presence of, or suspected presence of, any unsafe condition including asbestos or other hazardous materials or working conditions in areas in which they will be working.
(e) If during the performance of the work under this contract, the Contractor or any of its employees, or subcontractor employees, discovers the existence of an unsafe condition, the Contractor shall immediately notify the Contracting Officer, or designee (with written notice provided not later than three (3) working days thereafter), of the existence of an unsafe condition. Such notice shall include the Contractor's recommendations for the protection and the safety of Government, Contractor and subcontractor personnel and property that may be exposed to the unsafe condition.
(f) When the Government receives notice of an unsafe condition from the Contractor, the parties will agree on a course of action to mitigate the effects of that condition and, if necessary, the contract will be amended. Failure to agree on a course of action will constitute a dispute under the Disputes clause of this contract.
(g) Nothing contained in this clause shall relieve the Contractor or subcontractors from complying with applicable Federal, State, and local laws, codes, ordinances and regulations (including the obtaining of licenses and permits) in connection with hazardous material including but not limited to the use, disturbance, or disposal of such material.
(End of Clause)

DOJ-02 Contractor Privacy Requirements (JAN 2022)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984) and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DOJ system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.justice.gov/opcl/doj-systems-records.[1] Applicable SORNs published by other agencies may be accessed through those agencies’ websites or by searching the Federal Digital System (FDsys) available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

Except where use of Contractor networks, IT, other equipment, or Workplace as a Service (WaaS) is specifically authorized within this contract, the Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or WaaS and Government information shall remain within the confines of authorized Government networks at all times. Any handling of Government information on Contractor networks or IT must be approved by the Senior Component Official for Privacy of the component entering into this contract. Except where remote work is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

The Contractor shall complete and submit an appropriate separation checklist to the Contracting Officer before any employee or Subcontractor employee terminates working on the contract. The Contractor must submit the separation checklist on or before the last day of employment or work on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposition of personally identifiable information (PII)[2], in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to PII or other sensitive information.

In the event of adverse job actions resulting in the dismissal of a Contractor or Subcontractor employee before the separation checklist can be completed, the Prime Contractor must notify the Contracting Officer within 24 hours and confirm receipt of the notification. In the case the Contractor is unable to notify the Contracting Officer, then the Contractor should notify the Contract Officer's Representative (COR).

Contractors must complete the separation checklist with the Contracting Officer or COR by returning all Government-furnished property including, but not limited to, computer equipment, media, credentials and passports, smart cards, mobile devices, Personal Identity Verification (PIV) cards, calling cards, and keys and terminating access to all user accounts and systems. Unless the Contracting Officer requests otherwise, the relevant Program Manager or other Key Personnel designated by the Contracting Officer or COR may facilitate the return of equipment.

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

The Contractor must ensure that all employees take appropriate privacy training, including Subcontractors who have access to PII as well as the creation, use, dissemination and/or destruction of PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle PII, including heightened security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of PII. These courses, along with more information about DOJ security and training requirements for Contractors, are available at https://www.justice.gov/jmd/learndoj. The Federal Information Security Modernization Act of 2014 (FISMA) requires all individuals accessing DOJ information to complete training on records management, cybersecurity awareness, and information system privacy awareness. Contractor employees are required to sign the "Privacy Rules of Behavior," acknowledging and agreeing to abide by privacy law, policy, and certain privacy safeguards, prior to accessing DOJ information. These Rules of Behavior are made available to all new users of DOJ's computer network and to trainees at the conclusion of DOJ-OPCL-CS-0005.

The Contractor should maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required privacy and cybersecurity training.

(2) Safeguarding PII Requirements

Contractor employees must comply with DOJ Order 0904 and other guidance published to the publicly-available Office of Privacy and Civil Liberties (OPCL) Resources page[3] relating to the safeguarding of PII, including the use of additional controls to safeguard sensitive PII (e.g., the encryption of sensitive PII). This requirement flows down from the Prime Contractor to all Subcontractors and lower tiered subcontracts.

(3) Non-Disclosure Agreement Requirement

Prior to commencing work, all Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (NDA) and the DOJ IT Rules of Behavior. The Non-Disclosure Agreement:

(a) prohibits the Contractor from retaining or divulging any PII or other sensitive information, or derivatives therefrom, furnished by the Government or to which they may otherwise come in contact as a result of their performance of work under the contract/task order that is otherwise not publicly available, whether or not such information has been reduced to writing; and

(b) requires the Contractor to report any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of PII or other sensitive information to the component-level or headquarters Security Operations Center within one (1) hour of discovery.

The Contractor should maintain signed copies of the NDA for all employees as a record of compliance. The Contractor should also provide copies of each employee's signed NDA to the Contracting Officer before the employee may commence work under the contract/task order.

(4) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial or administrative records or databases is not authorized to regularly store or include any sensitive PII or other confidential government information that is created, obtained, or provided during the performance of the contract without the written permission of the Senior Component Official for Privacy (SCOP). It is acceptable to list the names, titles and contact information for the Contracting Officer, COR, or other personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Actual or Suspected Data Breach

Contractors must report any actual or suspected breach of PII within one hour of discovery.[4] A "breach" is an incident or occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The report of a breach must be made to DOJ. The Contractor must cooperate with DOJ's inquiry into the incident and efforts to minimize risks to DOJ or individuals, including remediating any harm to potential victims.

(a) The Contractor must develop and maintain an internal process by which its employees and Subcontractors are trained to identify and report the breach, consistent with DOJ Instruction 0900.00.01[5], Reporting and Response Procedures for a Breach of Personally Identifiable Information.

(b) The Contractor must report any such breach by its employees or Subcontractors to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000); Component-level Security Operations Center and Component-level Management Team, where appropriate; the COR; and the Contracting Officer within one (1) hour of the initial discovery.

(c) The Contractor must provide a written report to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000) within 24 hours of discovery of the breach by its employees or Subcontractors. The report must contain the following information:

(i) Narrative or detailed description of the events surrounding the suspected loss or compromise of information.[6] Date, time, and location of the incident.
(ii) Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.
(iii) Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.[7]
(iv) Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
(v) Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.[8]
(vi) Actions that have been or will be taken to minimize damage and/or mitigate further compromise.

(vii) Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

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

(e) At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access PII or to work on that contract based on their actions related to the loss or compromise of PII.

(6) Victim Remediation

At DOJ's request, the Contractor is responsible for notifying victims and providing victim remediation services in the event of a breach of PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose PII was lost or compromised. When DOJ requests notification, the Department Chief Privacy and Civil Liberties Officer and SCOP will direct the Contractor on the method and content of such notification to be sent to individuals whose PII was breached. By performing this work, the Contractor agrees to full cooperation in the event of a breach. The Contractor should be self-insured to the extent necessary to handle any reasonably foreseeable breach, with another source of income, to fully cover the costs of breach response, including but not limited to victim remediation.

C. <u>Government Records Training, Ownership, and Management</u>

(1) Records Management Training and Compliance

(a) The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the *DOJ Records and Information Training for New Employees (RIM)* training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. The Contractor shall maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records containing PII and those covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency information. The Contractor shall certify, in writing, the appropriate disposition or return of all Government information at the conclusion of the contract or at a time otherwise specified in the contract. In accordance with 36 CFR 1222.32, the Contractor shall maintain and manage all Federal records created in the course of performing the contract in accordance with Federal law. Records may not be removed from the legal custody of DOJ or destroyed except in accordance with the provisions of the agency records schedules.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and may be considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain an Authority To Operate (ATO) for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) If this contract requires the development, maintenance or administration of information technology[9], the Contractor shall support the completion of the Initial Privacy Assessment (IPA) document, if requested by Department personnel. An IPA is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help components assess whether additional privacy protections may be needed in designing or implementing a project[10] to mitigate privacy risks, and whether compliance work may be needed. Upon review of the IPA, the OPCL determines whether a Privacy Impact Assessment (PIA) document and/or SORN, or modifications thereto, are required. The Contractor shall provide adequate support to complete the applicable risk assessment and PIA document in a timely manner, and shall ensure that project management plans and schedules include the IPA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DOJ, including IPAs, PIAs, and SORNs, is located on the DOJ OPCL website (https://dojnet.doj.gov/privacy/), including DOJ Order 0601, Privacy and Civil Liberties. The Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor shall work with personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST 800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB Circular A-130.

[1] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).
[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), "'personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Regarding "sensitive PII," "[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information,

the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information." OMB Circular A-130, at App. II-2.
[3] The DOJ OPCL Resources page is available at https://www.justice.gov/opcl/resources.
[4] As stated in DOJ Instruction 0900, "Contractors must notify the Contracting Officer, the Contracting Officer's Representative, and JSOC (or component-level SOC) within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines."
[5] https://www.justice.gov/file/4336/download
[6] As stated in DOJ Instruction 0900, the description should include the type of information that constitutes PII; purpose for which PII is collected, maintained, and used; extent to which PII identifies a peculiarly vulnerable population; the determination of whether the information was properly encrypted or rendered partially or completely inaccessible by other means; format of PII (e.g., whether PII was structured or unstructured); length of time PII was exposed; any evidence confirming that PII is being misused or that it was never accessed.
[7] As stated in DOJ Instruction 0900, the report should include the nature of the cyber threat (*e.g.*, Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents.
[8] As stated in DOJ Instruction 0900, the report should include analysis on whether the data is accessible, usable, and intentionally targeted.
[9] As defined in 40 U.S.C. § 11101, the term "information technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.
[10] In this instance, the term "project" is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL.

(End of Clause)

DOJ-03 Personnel Security Requirements For Contractor Employees (Nov 2021)

Work performed under this contract will involve any one or more of the following: access to DOJ Information, which may include Controlled Unclassified Information (CUI), i.e., unclassified, sensitive DOJ information, and/or access to DOJ Information Technology (IT) systems, and/or unescorted access to DOJ space or facilities. Contractor employees will occupy Public Trust Positions, unless clause alternates are applied.

1. General Requirements

(a) (1) All references to "contract(or) personnel" and "contract(or) employee" in this clause means all individuals, without limitation, to include individuals employed by the contractor, team member, subcontractor, consultant, and/or independent contractor, who will have access to information of the Department of Justice (DOJ) or information that is within the custody and control of the DOJ, access to DOJ IT systems, and/or unescorted access to DOJ facilities/space in connection with the performance of this contract. "Employment" as used herein does not create nor imply an employer/employee relationship between the DOJ and contractor employees.

(b) (1) The type of security investigation required for each contractor employee will be governed by the type and risk level of information made available to the contractor employee. The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the Security Programs Manager (SPM), in consultation with the Contracting Officer's Representative if one is appointed, have received the requisite security approval.

(c) Except where specifically noted otherwise, the federal government will be responsible for the cost and conduct of the investigation.

(d) The contractor shall ensure that no contractor employee commences performance prior to receipt of a written authorization from the contracting officer, COR, or the SPM that performance by the respective contractor employee is authorized.

(e) The data and other information to which the contractor may have access as a result of this contract is the property of, and/or within the custody and control of, the Department, and its disclosure to third parties is governed by various statutes and regulations, the violation of which may subject the discloser to criminal penalties.

2. Citizenship and Residency Requirements

(a) Residency Requirement. (1) Contractor employees in Public Trust positions, both U.S. citizens and non-U.S. citizens, must meet the Department's residency requirement if they will require access to DOJ information, IT systems, or unescorted access to facilities. For three years (not necessarily consecutive years) out of the last five years immediately prior to employment under the Department contract the contractor employee must have: (i) resided in the U.S.; (ii) worked for the U.S. in a foreign country as either an employee or contractor in a federal civilian or military capacity; or, (iii) been a dependent of a federal civilian or military employee or contractor working for the U.S. in a foreign country. At the Department's sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) for contractor employees on a case-by-case basis where justified by extenuating circumstances. The residency requirement does not apply to contractor employees residing in foreign countries that are hired to work in American embassies/ consulates/missions located outside of the United States and who require access to DOJ information, IT systems, or unescorted access *provided that* an adequate background investigation can be conducted, with favorable adjudication, as determined by the DSO.

(b) Citizenship. (1) Aside from the specific exceptions set forth in Section 1.2(b)(2), for Public Trust positions, the DOJ requires that contractor employees be U.S. citizens and nationals, or lawful permanent residents seeking U.S. citizenship. Any prospective non-U.S. citizen contractor employee who requires access to DOJ information systems, DOJ information, and/or unescorted facilities access must also have been granted a waiver as described below in paragraphs 1.2(d) and/or (e). The contractor is responsible for verifying that the non-U.S. citizens working under this contract are lawful permanent residents seeking U.S. citizenship.

(2) *Exception for Certain Non-U.S. Citizen Contractor Employees*: (i) Non-U.S. citizen expert witnesses, litigative consultants, and interpreters in rare foreign languages are not required to be lawful permanent residents seeking U.S. citizenship. However, they must be granted a waiver for access to unclassified DOJ information, whether CUI or not, DOJ IT systems, and/or unescorted facility access, as described below in paragraph 1.2(d) and (e), regardless of the duration of their duties. (ii) Non-U.S. Citizen contractor employees residing in foreign countries who are hired to work for the Department of Justice in American embassies/consulates/missions outside of the United States are not required to be lawful permanent residents seeking U.S. citizenship.

(c) Dual Citizenship. (1) U.S. citizens who hold dual citizenship with a foreign country are considered U.S. citizens within the meaning of this clause, and may be considered for, but are not entitled to, contract employment as U.S. citizens consistent with this clause. The means by which the contractor employee obtained or exercises his or her dual citizenship status will be a consideration in the Public Trust Investigation (PTI) adjudication, and/or waiver approval processes discussed in this clause.

(d) Access to DOJ Information Technology Systems. Non-U.S citizens are not authorized to access DOJ information technology (IT) systems or assist in the development, operation, management, or maintenance of DOJ IT systems, including providing IT system support, unless a waiver has been granted by the Head of the DOJ component or designee, with the prior concurrence of both the DSO and the DOJ Chief Information Officer, allowing computer access by the non-U.S. citizen. Such a waiver will be granted only in exceptional and unique circumstances on a case-by-case basis. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive DOJ IT system and any contractor employee who will need access to JCON must be a U.S. citizen or have received a waiver. In order for a waiver to be considered for approval: (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; (2) The type of personnel security vetting that has been conducted on the individual, and vetting results, that would mitigate risk; and (3) The waiver must be in the best interest of the federal government.

(e) Access to Unclassified DOJ Information and Unescorted Access to DOJ Facilities or Space. (1) Except as provided under 1.2(b)(2), non-U.S. citizens are not authorized to access DOJ information and/or unescorted access to DOJ facilities or space, unless a waiver has been granted by the DSO, allowing access by the non-U.S. citizen. Such a waiver will be granted on a case-by-case basis where justified at the discretion of the DSO.

3. Background Investigation Requirements

(a) (1) Unless otherwise stated below, all contractor personnel are subject to a Public Trust Investigation (PTI). The SPM will determine the type of investigation for each contractor employee based on the risk category (i.e., the nature of the position and degree of harm that could be caused by the individual in that position) and whether the position is long-term or short-term. The PTI risk categories are listed below.

(i) High Risk Positions. The minimum background investigation required is a Tier 4 (T4) investigation, and the five-year reinvestigation required is a Tier 4R (T4R) investigation. The 2017 version of the Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.
(ii) Moderate Risk Positions. The minimum background investigation required is a Tier 2 (T2) investigation. The five-year reinvestigation required is a Tier 2R (T2R) investigation. The 2017 version of the SF-85P is required.
(iii) Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a Tier 1 (T1) investigation and the required five-year reinvestigation is also a Tier 1 (T1) investigation. The SF 85, Questionnaire for Non-Sensitive Positions, is required.

(b) *Exception for Expert Witnesses*. Expert Witnesses, litigative consultants, and interpreters in rare foreign languages may not be subject to full background investigation requirements if alternative security requirements are approved by the DSO.

(c) *Short-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), short-term contractor employees (6 months or less) who are U.S. citizens are not subject to a full background investigation, however, must receive an approved pre-employment background investigation waiver. The required forms to complete and submit are listed in Section 1.4(b) and (c)(2).

(d) *Long-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), all long-term U.S. citizen employees (longer than 6 months) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(e) *Non-U.S. Citizen Contractor Employees*. Other than the exception in 1.3(b), all non-U.S. citizen contractor employees regardless of performance duration (short or long term) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(f) *Reciprocity*. (1) A Public Trust Investigation will be accepted under reciprocity if it meets the following guidelines: (i) the investigation is current (investigations are considered current if completed within the last five years) and favorably adjudicated, or the reinvestigation has been deferred; (ii) the investigation meets or exceeds the level of investigation required for the DOJ contractual instrument; (iii) there has been no continuous (not cumulative) break in federal contract/ service employment of two years or more; (iv) there is no derogatory information since the favorable fitness determination or adjudication that calls into question the individual's fitness based on character or conduct; and (v) the investigative record does not show conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from position to position.

4. Background Investigation Process

(a) *e-QIP (or its successor)*. Public Trust background investigations/reinvestigations of contractor employees will be performed by the DCSA. The investigative process requires contractor employees to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and provide additional information as specified in paragraph 1.4(b) below. Immediately after contract award, the contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the SPM. The e-QIP Initiator must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being given access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The contractor will then be responsible for initiating investigations for all contract personnel, whose previous investigation does not meet reciprocity, in e-QIP for completion of the security questionnaire form and forwarding the electronic form with the remainder of the security package to the SPM. Subject to the prior written approval of the SPM, the contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being provided access to e-QIP.

(b) *Additional Documentation*. (1) In addition to completing the e-QIP questionnaire (see 1.4(a), above), the contractor shall ensure that each contractor employee occupying Public Trust Positions, including short-term employees, completes and submits the following information through the contractor's Corporate Security Officer:

(i) Digital Fingerprinting/FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI or other law enforcement entity, as approved by the SPM, is required to ensure the identity of the person being fingerprinted and for printing quality. All pertinent information must be completed by the individual taking the fingerprints (FBI or other). Use of the physical FD-258 Applicant Fingerprint Card should only be used in extenuating circumstances.
(ii) DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This form will be required if the Component SPM determines a credit check is necessary for its Low Risk Level 1 contractor positions.
(iii) OF-306, Declaration for Federal Employment.
(iv) Foreign National Relatives or Associates Statement. This is only required if foreign national relatives or associates were not disclosed on the security questionnaire form.
(v) Self-Reporting Requirements for All Contractor Personnel. This is an acknowledgement and acceptance statement that every contractor must sign.
(vi) Additional information as may be required based on the review of the security questionnaire form.

The contractor shall review all forms/documents to ensure each is complete, accurate and meets all DOJ requirements, including applicable residency and citizenship requirements. The contractor shall resolve any issues or discrepancies with the contractor employee, including resubmission of corrected forms or documentation. Completed forms/documents shall be submitted to the SPM (or designee, which may include the COR) within five (5) calendar days after being finalized.

(c) Adjudication and Pre-Employment Background Investigation Waivers

(1) Except as set forth in this section, background investigations must be conducted and favorably adjudicated for each contractor employee prior to commencing their work on this contract. Where programmatic needs do not permit the federal government to wait for completion of the entire background investigation, a pre-employment background investigation waiver for *public trust contractors* can be granted by the SPM, in consultation with the cognizant COR. Pre-employment waivers cannot be used to circumvent delays in clearing classified contractors through the DCSA, if access to classified information is required.

(2) As directed by the SPM, the contractor shall initiate pre-employment waivers for Public Trust Positions when necessary. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the federal government. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contractor employee's favor. When a waiver has been disapproved, the CO, in consultation with the SPM and COR, will determine (i) whether the contractor employee will no longer be considered for work on a DOJ contract or (ii) whether to wait for the completion and favorable adjudication of the background investigation before the contractor employee commences work on a Department contract. The pre-employment background investigation waiver requirements include:

1. Verification of citizenship (copy of a birth certificate, naturalization certificate, or U.S. passport);
2. Verification of compliance with the *DOJ Residency Requirement* of this Clause;
3. Favorable review of the security questionnaire form;
4. Favorable FBI fingerprint results;
5. Favorable credit report;
6. Favorable review of the OF-306 form, Declaration for Federal Employment;
7. Verification of the initiation of the appropriate background investigation (for long-term personnel); and
8. Receipt of the signed DOJ *Self-Reporting Requirements for All Contractor Personnel* (see Section 6, below).

(3) The investigating agency (DCSA) will provide the SPM with the results of each proposed contractor employee's Public Trust investigation. Upon receipt of the investigation and any other pertinent documents from the investigating agency, the SPM will determine whether each proposed contractor employee should be granted employment security approval.

(4) The COR will notify the contractor of the results of Public Trust background investigations as they are completed and adjudicated, including any individual who is found ineligible for employment security approval. For any individual found ineligible for employment on a Department contract, the contractor shall propose a replacement and initiate the background investigation process consistent with this clause.

5. Identity Proofing and Badging

(a) Access to DOJ Information, federally-controlled IT systems, and/or unescorted access to federally-controlled facilities or space (regardless of whether the contractor employee will be issued a DOJ PIV card or building access badge) shall be made available after each respective contractor employee has (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this contract.

(b) (1) Public Trust contractor employees must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking two forms of identification in original form prior to commencement of work by the contractor employee and PIV card or building access badge issuance (as applicable). Approval will be documented by the DOJ official or an official of a trusted contract company. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

(c) [Reserved]

(d) All contractor employees requiring unescorted access to a DOJ controlled facility or space shall comply with the PIV card or building access badge requirements outlined below:

(i) When any contractor employee enters a DOJ building for the first time, he/she shall allow one hour for security processing and the creation and issuance of a building access badge. PIV cards require additional processing time and will not likely be issued on the same day.
(ii) Building access badges shall be subject to periodic review by the contractor employee's supervisor and checked against his/her personal identification. The contractor employees shall present themselves for the issuance of renewed badges when required by the government as scheduled by the COR or his/her designee. The contractor shall notify the COR when contractor employee badges are lost, and must immediately apply for reissuance of a replacement badge. The contractor shall pay for reissued building access badges at no cost to the government. It is the contractor employee's responsibility to return badges to the COR or his/her designee when a contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

6. Employee Reporting Requirements

(a) All contractor employees must sign the DOJ *Self-Reporting Requirements for All Contractor Personnel* statement acknowledging and accepting the DOJ requirement that they immediately self-report certain information using the Department's iReport system. The COR or SPM will provide the Self-Reporting statement as well as a list of reportable information, which varies by position sensitivity designation, to the contractor employee before commencing work under the contract. If the contractor employee does not have access to the DOJ iReport System, the COR or SPM will provide a fillable form for the contractor employee to complete and submit.

(b) The COR and SPM will review the written report and documentation and make a determination regarding continued employment on a DOJ contract.

(c) DOJ reporting requirements are in addition to the DCSA reporting requirements and the contractor's internal reporting requirements.

7. Replacement Personnel

(a) The contractor shall make every effort to avoid costs to the government for security investigations for replacement of contractor employees, and in so doing shall ensure that otherwise satisfactorily performing and physically able contractor employees remain in contract performance for the duration of the contract. The contractor shall take all necessary steps to ensure that contractor personnel who are selected for assignment to this contract are professionally qualified and personally reliable, of reputable background and sound character, and able to meet all other requirements stipulated in the contract.

(b) The fact that the government performs security investigations shall not in any manner relieve the contractor of its responsibility to ensure that all contract personnel are reliable and of reputable background and sound character. Should a security investigation conducted by the government and/or a contractor's self-report or failure to self-report render ineligible a contractor employee, the contracting officer will determine whether the contractor has violated this clause. The contracting officer may direct the contractor, at its own expense, to remove and replace any contractor personnel who fails to comply with or violates applicable requirements of this contract. Such action may be taken at the government's direction without prejudice to its rights under any other provision of this contract, including termination for default, and the contractor may be held liable, at a minimum, for all reasonable and necessary costs incurred by the government to (i) provide coverage (performance) through assignment of individuals employed by the government or third parties in those cases where absence of contractor personnel would cause either a security threat or DOJ program disruption and (ii) conduct security investigations in excess of those which would otherwise be required.

(c) Nothing in this clause shall require the contractor to bear costs involved in the conduct of security investigations for replacement of a contractor employee who separates from the contractor of his/her own accord, is incapacitated, or is deceased.

(d) The contractor shall comply with the terms and conditions set forth under this clause and assumes all liability for failure to comply. The rights and remedies conferred upon the government by this clause are in addition to all and other rights and remedies pursuant to the contract and as established by law.

(End of Clause)

DOJ-05 Security of Department Information and Systems (OCT 2023)

I. Applicability to Contractors and Subcontractors

Section 2839.102 of the Justice Acquisition Regulation (JAR), (48 C.F.R. § 2839.102), applies to this contract. Accordingly, all contractors are obligated to comply with all applicable DOJ security policies, directives, or guidance documents, including the security requirements in the provisions in this contract clause. This contract clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of the contractors and subcontractors (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. The security requirements set forth herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), and any other applicable laws, mandates, contract clauses, DOJ policies, directives or guidance documents and Executive Orders pertaining to the development and operation of Information Systems and/or the protection of Government Information. This clause does not alter or diminish any existing rights, obligations, 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. **Authorization to Operate** ("ATO"), as defined in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-37 Revision 2, is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.

B. **Cloud Computing**, as defined in DOJ Order 0904 Cybersecurity Program, is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models in accordance with NIST SP 800-145.

C. **Covered Contract** is any contract, order or other agreement under which the contractor, or a subcontractor at any tier, including a cloud service provider, may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information (as defined below) in the course of providing a product or service to the Department, with the exception of acquisitions under the micro-purchase threshold.

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

E. **Data** means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data, computer software, and personally identifiable information (PII) (defined below). The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

F. **DOJ Information**, as defined in DOJ Order 0904, 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 the Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired to perform the contract.

G. **Information,** as defined in DOJ Order 0904, is 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. This includes any communication or representation of knowledge in an electronic format that allows it to be stored, retrieved, or transmitted.

H. **Information System**, means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

I. **Personally Identifiable Information ("PII")**, as defined in the FAR 24.101, means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. It includes but is not limited to common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers or other government-issued identifiers, precise location information, medical history, and biometric records. This definition covers all PII that is created by or becomes available to the contractor, including its employees, subcontractors, or affiliates, as a result of performing under this contract. PII, as supplementally defined in DOJ Order 0904, also includes 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.

J. **Private Cloud**, as defined in NIST SP 800-145, is the deployment model for cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

K. **Security Breach** means any security incident (as defined below) that directly relates to the loss of control, compromise, exfiltration, manipulation, unauthorized disclosure, unauthorized acquisition, unauthorized exposure or unauthorized access or any similar occurrence of any Covered Information System or any DOJ Information or any PII accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system. This includes incidents where (1) a person other than an authorized user accesses or potentially accesses PII or DOJ Information or (2) an authorized user accesses or potentially accesses PII or DOJ Information for an unauthorized purpose.

a. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed security breach (as defined above).
b. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed security breach (as defined above).

L. **Security Incident** means any occurrence that (1) may actually or imminently jeopardize, without lawful authority, the availability, integrity, authentication, confidentiality, or nonrepudiation of DOJ Information or a Covered Information System; or (2) may constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

a. **Potential Security Incident** means any suspected, but unconfirmed security incident (as defined above).
b. **Confirmed Security Incident** means any confirmed security incident (as defined above).

M. **Vulnerability,** as defined in DOJ Vulnerability Management Plan, and the OCIO Information Security Management Procedure, means a weakness or flaw discovered in the design of a system that, when exploited, may result in a loss of confidentially, integrity, or availability of DOJ Information or an Information System.

III. Confidentiality and Non-Disclosure of DOJ Information

A. Preliminary and final contract deliverables and all associated working papers and material generated by the Contractor developed using DOJ Information, product, source code, and/or methods of operations, 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 (Rights in Data-General). The Contractor will define a method of monitoring the development activity to include any activity associated with DOJ Information, product, source code, and methods of operations. The data rights and development details shall be defined within the Contract.

If the Contractor intends to utilize its existing data, for which it has a patent or copyright, to develop a contract deliverable, it is incumbent upon the Contractor to negotiate with the CO the proper FAR Part 27 clauses in the contract to protect its existing data.

B. Pursuant to FAR 52.227-14(d)(2), all documents and data produced in the performance of this contract containing DOJ Information, product code, source code, and/or methods of operations are the property of the U.S. Government and, without the prior written permission of the CO, the Contractor shall neither reproduce nor release such information to any third-party at any time, including during performance or following expiration and/ or termination of the contract.

C. Any DOJ Information made available to the 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, the Contractor assumes responsibility for the protection of the confidentiality of all DOJ Information processed, stored, or transmitted by the Contractor. The Contractor shall comply with information security responsibilities and duties throughout the contract and after expiration/termination as appropriate per contract close-out activities. When requested by the CO (typically no more than annually), the Contractor shall provide a report to the CO identifying, to the best of the 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, in addition to any other applicable requirements, as set forth in Part I, the Contractor shall comply with the security requirements of the Federal Information Security Modernization 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, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards as amended, and OMB Memoranda relating to the security of information and/or Federal Information Systems.

B. In addition, for all Covered Information Systems, the Contractor shall comply with the following requirements, which are listed here only to highlight certain specific applicable requirements from one of the sources identified in the first paragraph of this Section. This is not an exhaustive list of all such requirements with which the Contractor is obligated to comply, and the omission of a requirement from this list should not be construed as negating the materiality of that requirement. These requirements and those in the authorities in the prior paragraph should be read together.

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 at least annually to all Contractor employees and contractors involved with the Covered Contract. Such training shall include, but not be 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, in accordance with applicable requirements but in any event at least until the expiration of the contract, 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, to include but not be limited to, collecting, reviewing, and analyzing appropriate logs and timely investigating security alerts and potential security incidents.

6. Establishing and maintaining baseline configurations and current 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 Covered 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 as defined by NIST 800-63-3, *Digital Identity Guidelines* or current revision.

9. Establishing and maintaining an operational incident handling capability for Covered Information Systems that includes adequate and timely development, logging, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and timely reporting incidents to appropriate officials and authorities within the 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.

11. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media, and DOJ assets under Contractor control; protecting them from environmental impacts, access, and equipment positioning requirements defined; 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.

12. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized personnel according to DOJ 03.

13. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards including personnel background checks.

14. Continuously assessing the risk to DOJ Information in Covered Information Systems, including scanning and remediating vulnerabilities, or implementing appropriate mitigation in accordance with DOJ policy, and ensuring the timely removal of assets no longer supported by the Contractor.

15. Continuously monitoring the application of security controls of Covered Information Systems, assessing the efficacy of such controls, and developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Covered Information Systems.

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

17. 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 and timely action in response.

18. Ensuring return of Government Furnished Equipment ("GFE") and/or PIV card assets within 10 business days of notification for end of use (contract end, staff change, etc.).

19. Complying with rights in data (FAR 52.227-14) as to the development, management, and protection of DOJ Information.

20. Reporting on risks or known issues impacting DOJ Services (staffing, hardware, process, changes, etc.) through the Contractor's CO or COR, DOJ Service Owner ("SO"), and Government Technical Manager ("GTM") including risk mitigation activities.

21. Reporting through the Contractor's CO or COR on any projected or planned changes in corporate ownership, covered information system design, and/or any technical changes that could impact the confidentiality, integrity or availability of DOJ Information, data, or systems. Changes to system design must be updated through the authorization process per NIST SP 800-37 Revision 2, Step 6 ('Continuous Monitoring") or current NIST revision.

22. When, as part of operating within the DOJ environment, the Contractor's covered information system is subject to review, audit, or assessment by third parties, facilitating DOJ access to information system resources, facilities, personnel, and documentation in a timely manner as required by the auditors. Should a third-party organization conduct a review of any Covered Information System, the Contractor must provide a copy of the report to DOJ, through the CO and COR.

23. Completing an attestation that meets OMB Memorandum M-22-18 for software procurements following the template attestation form developed by NIST. The attestation form must be returned to the CO and COR for sharing with the component Chief Information Officer (CIO).

24. Reporting on outages impacting DOJ Services through the Contractor's CO, COR, and DOJ Service Owner (SO) to include event and mitigation details.

C. The Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an 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. (For Cloud Computing Systems, see Section V, below.)

D. The Contractor shall ensure compliance with DOJ-03 (Personnel Security Requirements for Contractor Employees) as to all Covered Information Systems.

E. When requested by the DOJ CO or COR as described below, the 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 the 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, the Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

F. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause or access a Covered Information System is prohibited unless the CO approves it in writing after the Contractor has provided a letter certifying compliance with the following requirements. For any requirements which include the use or storage of PII, the Senior Component Official for Privacy must also approve. Any additional requirements set forth for the use or storage of PII under DOJ-02, Contractor Privacy Requirements, are in addition to, not superseded by, the requirements set forth here.

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

2. The 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. The 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 should be treated by the Contractor as sensitive information unless specifically designated as non-sensitive by the DOJ.

5. A Rules of Behavior (ROB) form must be signed and acknowledged annually 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 users that they have no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

6. Cybersecurity Awareness Training (CSAT) shall be provided annually by Contractor for all users of Covered Information System. This training must be submitted to, and approved by, the CO or COR in advance of being provided to users. Users must complete and acknowledge having received CSAT each year. At a minimum, CSAT provided by contractors must include:

a. Insider Threat Detection and Reporting – Importance of detecting, methodologies, indicators, and reporting

b. Privacy Awareness – Privacy Act and PII

c. General Cybersecurity – Information security, trends in advance persistent threats, social engineering/phishing, appropriate use, mobile devices, remote access, basic security best practices

G. Contractors shall not store DOJ information on Contractor-owned removable IT (e.g., media such as a thumb drive or external hard drive) unless expressly authorized in writing by the DOJ CO or COR in the performance of their contract.

H. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with NIST SP 900-88, *Guidelines for Media Sanitization*.

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

J. The Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 10 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 in a format and form acceptable to DOJ. The Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 10 business days of the removal and return of all DOJ Information.

K. DOJ, at its discretion, may suspend the Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that the Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident or Security Breach (see definitions above), 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. Any termination action taken because of the Contractor's suspected failure to comply with any security requirement will be conducted in accordance with the applicable termination clause governing the awarded contract. The Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to DOJ, and that upon request by the CO, the Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at the Contractor's expense. The Contractor must comply with FAR 52.227-14 (Rights in Data), FAR 52.245-1 (Government Property), DOJ 2400.3A Chapter 1 (component property procedures), and FAR 4.804-5(a)(6) (Procedures for closing out contract files).

V. Cloud Computing

A. The Contractor may not utilize the Cloud system of any Cloud Service Provider ("CSP") unless:

1. All of the following has occurred: (a) the Cloud system and CSP have been evaluated by a Third Party Assessing Organization ("3PAO") certified under FedRAMP; (b) the Cloud system received FedRAMP authorization; (c) the Contractor has provided the most current System Security Plan ("SSP") and Security Assessment Report ("SAR") to the DOJ CO for consideration, and provides any subsequent SSPs and SARs within 30 days of issuance; and, (d) the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under the Covered Contract has issued an ATO; or,

2. In cases where the CSP or its offering is not FedRAMP authorized, the COR approves utilization of the Cloud System after the CSP has worked with the authorizing official, the DOJ OCIO, and the FedRAMP Program Management Office to determine that the CSP is likely to seek and receive Agency/ FedRAMP authorization within 1 year, or DOJ has authorized use as a Private Cloud or Contractor Owned, Contractor Operated system.

B. The 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.

C. The Contractor must ensure that the CSP provides access and information to support and enable DOJ's cloud security posture management, to include the current inventory of security management configuration data for services and information to confirm the Contractor has been monitoring accounts for compliance with security requirements. The DOJ Justice Security Operations Center (JSOC) must be able to access logs and events to investigate potential security breaches and perform security posture assessments associated with the Security Audit Identity Credential Access Management (ICAM) policies.

D. The Contractor must ensure that the CSP provides evidence of annual recertification of privileged user access management.

E. A Supply Chain Risk Management (SCRM) review is mandatory for specified acquisitions in accordance with established process in EO 14028 and NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, or superseding document. All vendor products and solutions to be used on DOJ national security systems, enterprise-wide systems, or new FIPS-199 High and Moderate systems for the purpose of accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of DOJ Information must be submitted to DOJ OCIO for a Supply Chain Risk Management review prior to contract award or ATO signature. Changes in corporate ownership or structure shall be reported to the CO for referral to SCRM. The Contractor shall notify the CO of any confirmed Supply Chain compromise affecting the Contractor's products or services within 1 hour of discovery.

__ The following SCRM requirements for acquisition of systems, hardware, or software which will be used in systems that are mission critical or process sensitive data apply to this award. **(CO check as appropriate in coordination with the Program Manager and/or System Owner)**

1. The Contractor shall develop and deliver a SCRM Plan. The SCRM Plan shall meet the format described in NIST SP 800-161, Appendix E. The SCRM plan shall address the following security controls from NIST SP 800-53 Rev 5: SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-10, and SR-11. Equivalent ISO 27000 series controls may be used if they are mapped to the NIST control(s).

2. The Contractor shall implement the required security controls as documented in the SCRM Plan. The requirements of the SCRM plan shall flow down to all subcontractors. Evidence of the certification and compliance is required.

3. The Contractor shall provide evidence of compliance with the documented SCRM Plan. **(CO select which applies**)

__ Self-assessment by a contractor security team
__ External assessment by an independent auditor

VI. Information System Security Incident or Security

A. Confirmed Security Incident. The Contractor shall immediately (and in no event later than 1 hour of discovery) report any Confirmed Security Incident to the DOJ CO and COR. If the Confirmed Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call JSOC at 1-202-357-7000 immediately (and in no event later than within 1 hour of discovery of the Confirmed Security Incident) and shall notify the CO and COR as soon as practicable.

B. Potential Security Incident.

1. If the Contractor suspects that DOJ information has been potentially disclosed or impacted, the Contractor shall promptly investigate to determine if a Security Incident has occurred. If the Contractor has not determined within 24 hours (i.e., 24 hours from detection of potential security incident and/or security breach) whether the Potential Security Incident was in fact a Security Incident, then it must immediately report the Potential Security Incident to the DOJ CO and the COR. If the time by which to report the Potential Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call or e-mail the JSOC Team at 1-202-357-7000 or JSOC@USDOJ.GOV and contact the DOJ CO and COR as soon as practicable. If the contract involves PII, the Contractor must comply with the notification requirements of DOJ-02 and Executive Order M-17-12 (Memorandum on Preparing for and Responding to a Breach of Personally Identifiable Information), Contractor Privacy Requirements, Section B.5, for an actual or suspected Security Incident.

2. The Contractor must limit sharing of Security Incident details to only those individuals involved in responding to the potential Security Incident. Any provisions of the Covered Contract regarding the citizenship or location of individuals working on the Covered Contract apply equally to individuals involved in responding to any potential Security Incidents. The Contractor may request assistance from the JSOC for advice, incident response, or FBI coordination. The Contractor must provide weekly updates to CO, COR and JSOC during the course of a Security Incident investigation.

C. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify:

1. Both the Covered 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 the Contractor to minimize, remedy, and/or investigate the Security Incident.

3. Any and all other information as required by the CISA Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and

The Contractor may request assistance from the JSOC Team for advice, incident response, or FBI coordination, and must provide weekly updates to CO, COR, and JSOC during the course of an Incident investigation.

D. Except as otherwise required by Federal, State and local laws, executive orders, rules and regulations, all determinations regarding whether and when to notify other individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials, the DOJ Core Management Team, or the COR at DOJ's discretion.

E. The Contractor must provide to DOJ full access to any facility and/or Covered Information System affected or potentially affected by any potential or confirmed Security Incident, 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.

F. DOJ, at its sole discretion, may obtain, and the Contractor will permit, the assistance of other federal agencies and/or third-party contractors or firms to aid in response activities related to any potential or confirmed Security Incident. Additionally, DOJ, at its sole discretion, may require the Contractor to retain, at the Contractor's expense, a 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 Covered Information Systems.

G. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by the 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. The 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. Pass-Through of Security Requirements to Subcontractors and CSPs

A. The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with the contract, including any CSP providing services for any other CSP under the contract, and the 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 the Contractor.

(End of Clause)

DOJ-08 Continuing Contract Performance During a Pandemic Influenza or other National Emergency (OCT 2007)

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 contractor's 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.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.

(End of Clause)

EOUSA AI-10-1E Federal Grand Jury Court Reporter Security Requirements (December 2015)

Federal Grand Jury Court Reporter Security Requirements (December 2015)
1. Grand Jury (GJ) Security.

The work to be performed under this contract will involve access to sensitive information subject to the rules of 6(e) of the Federal Rules of Criminal Procedures. The adequate and continual protection of the information (hereafter referred to as GJ information which includes GJ testimony, discussions, exhibits, etc.) and how it is used, shared, and stored, is extremely important. The secrecy and ultimate security of the GJ information and proceedings is vital to the performance of the U.S. Attorney's Office (USAO) and the Court. A failure to protect GJ information by anyone involved may be considered a breach of contract, breach of agreement, a violation of standards, and perhaps, an unlawful act. Disclosures of matters appearing before the GJ other than its deliberations, including the vote of any juror may be made available to the attorneys for the Government to use in the performance of their duties. Otherwise, a juror, attorney, interpreter, stenographer, or operator of recorded testimony may disclose matters appearing before the GJ only when so directed by the Court.

a. Violations of the Terms and Conditions. Unauthorized use of GJ information or material could subject the disclosing individual to contempt of court penalties and other applicable penalties. Sensitive information may include, but is not limited to: data found within GJ information, informant and witness information, investigative material, tax information, medical information, computer systems information, Privacy Act (as amended) information, Department of Justice proprietary information, or Federal information that is not releasable to the general public and/or under the guidelines of the Freedom of Information Act (FOIA). Unauthorized duplication or disclosure of the data and other information to which the Contractor may have access as a result of this contract is prohibited by Public Law and is subject to criminal penalties.

b. Court Reporter Security Training. The Contractor is responsible for ensuring all employees approved to work with and have access to GJ information and materials are familiar with - and required to follow - continuing responsibilities and the security requirements as outlined in the contract.

c. Failure to Meet Security Requirements. Should the Government determine that the Contractor has failed to comply with the security requirements of the contract, the Contractor may be held responsible, as a minimum, for all reasonable and necessary costs incurred by the Government to: (a) provide coverage (performance) through assignment of individuals employed by the Government or third parties in cases where absence of contract personnel would cause a delay in the proceedings, a security threat, and/or disrupt a DOJ program, and (b) conduct security investigations in excess of those which would otherwise be required. Nothing in this clause shall require the Contractor to bear costs involved in the conduct of security investigations for the replacement of an employee who becomes incapacitated, severely ill, or deceased. Any violation of this requirement subjects the Contractor, subcontractor, employees, etc., to certain penalties including, but not limited to termination of the

contract, issuance of a cure notice for less serious violations, and being held in Contempt of Court for failing to safeguard federal GJ information.

d. List of Contractor's Employees. The Contractor shall submit to the USAO a list of the names of all principals, staff members, and regular employees requiring access to the work performed under the contract. This includes personnel of the principal Contractor and any subcontractor(s).

e. Sub-Contractors. The Contractor must ensure that any sub-contractor furnishing supplies and services which will involve access to GJ materials complies with the security requirement of the contract and has been approved by the Government.

2. Personnel Security.

The USAO will process the background investigations for GJ court reporter(s) identified by the Contractor to the USAO to perform work under this contract. However, this background investigation does not replace or supersede the employer's responsibility to sufficiently screen and eliminate unsuitable applicants and to take all necessary steps to ensure only qualified persons perform services.

a. Residency Requirement. All Contractor employees assigned to this contract and working within the United States shall meet the DOJ Residency Requirement. The Residency Requirement states that, for 3 of the 5 years immediately prior to applying for a position, the individual must have: (1) resided in the United States; (2) worked for the United States overseas in a Federal or military capacity; or (3) be a dependent of a Federal or military employee serving overseas.

b. Sufficient Personnel. The Contractor must maintain a sufficient number of approved personnel to execute the contract. The Contractor is not to assign GJ court reporting duties unless, and not until, the COR or representative of the USAO provides notification in writing that the employee has been granted the necessary security approval to perform GJ court reporting duties as outlined under this contract.

c. Suspension or Revocation of Access Approval. Access to GJ information can be suspended or revoked for cause at any time by the Contractor and/or the COR.

d. Required Suitability Approval and Background Investigation. Contractor employees must receive a security approval based upon: (1) A Government conducted Moderate Background Investigation (MBI) or higher background investigation, and (2) Favorable adjudication. A security waiver may be requested by the contractor prior to completion of a background investigation when necessary and as outlined by the Government. The Contractor will ensure the required security background investigation forms are completed and submitted. The intent and purpose of the investigation is to preclude the assignment of any individual who poses a threat to the Government or successful contract completion due to past unlawful or inappropriate behavior.

e. Background Investigation Process and Forms. The USAO will initiate the Electronic Questionnaires for Investigations Processing (e-QIP) upon receipt of the Contractor's or Contractor employee applicant's name and other information. The applicant will complete sign and submit e-QIP forms to the USAO/POC on the same day the signature pages are signed. The USAO will have 5 days to forward the forms to SEMS/PERSEC. Waiver package will include the following: e-QIP package, and the following forms; Certification, General Release, Medical Release, and Fair Credit pages, DOJ-555 Disclosure & Authorization Pertaining to Consumer Reports, Standards of Conduct Form, OF-306 Declaration for Federal Employment, Foreign Nat'l Relatives or Associates Form (if applicable), employment vouchers (2 if most recent employment is less than 2 years; 1 if most recent employment is more than 2 years), and fingerprints cards (form FD 258) or results. The forms shall be submitted to the SEMS/PERSEC upon completion of e-QIP. The Government may request additional security forms, or additional information, if the contract employee's security forms contain information which requires clarification (i.e. information concerning criminal history, financial problems, citizenship of family members, etc.)

3. Protecting the GJ Information.

a. Contractor's GJ Information Processing Site. The location selected by the Contractor and approved by the Government (USAO) for the processing, storage, and preparation of GJ information must be determined in advance of commencement of work. The location for processing is not to be changed or modified without the prior consent of the USAO unless extenuating circumstances or emergencies demand relocation. In such cases, the Contractor must coordinate with the CO or COR. The means and methods for transfer or relocation of any GJ material will also be coordinated and approved by the USAO in advance.

b. Contractor Physical Security Requirements. The physical security standards are extremely important to the Government. The Contractor has a duty and legal obligation to ensure that all physical security measures, practices, and policies are strictly followed and any deviation must be coordinated and approved by the CO. If the Contractor and the CO mutually agree to only using USAO provided space in lieu of the Contractor's own space, then the physical security requirements of subparagraphs 3d, 3e, and 3f contained in this Annex do not apply.

c. Designated Room or Space. The Contractor will have and use a designated room or space to process, proofread, and store GJ material. When a dedicated room is not feasible or practical, the Contractor must ensure that the room or space used meets or exceeds the required physical security controls, protection standard, and has been pre-approved by the USAO. The requirement is to prevent unauthorized access to the GJ material. The GJ material must be protected against unauthorized disclosure and viewing by other tenants, co-business employees, and unauthorized persons (family, friends, customers, etc.)

d. Door and Locking Hardware. The designated room or space must have an operational door and lock which prevents unauthorized entry into the room or space. Doors must be closed and locked when the room is not in use and when the room is vacated for short periods of time. (The alarm is also to be set if the user is not expected to return within
5 minutes.) The Contractor must have total key control and accountability. Only persons who have been approved to access the GJ information are to possess a key to the pre-approved room or space. The Contractor must ensure that no one is allowed unsupervised and/or unrestricted access to the space where the GJ material is stored unless approved by the government.

e. Windows and Emergency Exits. Windows are allowed provided they are locked and the pre-approved room or space is alarmed and monitored. Emergency exits are allowed and if present, must be alarmed.

f. Intrusion Alarm and Monitoring Service. The designated room or workspace where the material is stored must be equipped with an Intrusion Detection System (IDS) that is connected to a central monitoring station. The Contractor will provide the USAO a copy of the call or notification list and responder protocols on alarm annunciation. The Contractor must notify the USAO within 2 business days of any alarm activation. The notification must include the time and date of the alarm activation, an explanation of cause if known, incident details including the identification of any missing GJ material (devices, storage media, paper, etc.), and a copy of the activity log from the monitoring station. The Contractor must provide the USAO with a copy of the IDS monitoring history log quarterly (every 90 days) and as requested by the USAO. Knowledge of the code number used to program, arm and/or disarm the system must be limited to those who have Government approved access to the GJ material. Remote monitoring services are not allowed to have the code number. The alarm must be set to "armed" whenever the room is not in use. Short absences of less than 5 minutes in duration do not require the alarm to be set to "armed." The alarm system is to be tested at least once per year to ensure it is functioning properly and the desired response occurs.

g. Contractor's GJ Information Storage. The GJ material must be stored only in USAO approved storage container(s). The container must be either equipped with an approved lock or locking mechanism. The combination of a lock shall be restricted to those who have a need-to-know the information and have a security approval. An entry/closure log shall be maintained to record each time a security container is opened and closed and by whom. Any combination will be changed when a person with knowledge of the combination no longer needs or is approved for access, or upon compromise of the combination. End of day security checks shall be performed within the contract facility to ensure that precautions are taken to protect GJ material. The Contractor or an approved contractor's employee is to make periodic checks to ensure all GJ material has been properly stored. The periodic security checks shall be annotated in a log or journal. The storage container must be locked when not in use. A storage container that can be easily moved or illegally removed should be mounted or anchored to the floor or wall. It is recommended that the Contractor use a GSA-approved container whenever possible. A Class 3, 4, 5, or 6 is sufficient.

h. Use and/or Sale of Grand Jury Information and Transcripts. Grand Jury transcripts may not be sold or made available to anyone other than the Government at any time under any circumstances.

i. Personal Identity Verification (PIV) of Contractor Personnel. The Contractor shall comply with agency personal identity verification procedures that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) Guidance M-05-24, and Federal Information Processing Standards Publication (FIPS Pub) Number 201. The Contractor's employees who require physical access to the USAO or to USAO controlled information technology or device may be required to be issued and use a PIV Card issued in accordance with HSPD-12. The Contractor must comply with access procedures, policies, and security requirements if and/or when physical and/or virtual access is required to a federally-controlled facility or information system(s).

4. Information Technology (IT) Equipment.

The Contractor must ensure that all devices used to process, store, record, and duplicate GJ information meet the requirements of the USAO and have been approved by the USAO for use. (IT equipment refers to computers, recording devices, scanners, printers, laptops, copiers, and all other devices used to process and/or store GJ information.) When processing GJ Information the computer/laptop must be used as standalone with internet connectivity disabled. The computer/laptop can only be the internet enabled during the timeframe of transmitting files when using file exchange software. Administrative controls over all approved IT devices and settings used for this contract are to be restricted and approved by the Government.

a. Approval and Marking Approved Devices. The Contractor will provide to the USAO the serial numbers of all IT devices used in the performance of this contract over the term of the contract in advance of their use. The approved devices will be clearly marked and labeled as containing federal GJ information or FGI. The devices will also be marked as containing controlled unclassified information (CUI).

b. IT Processing, Transmitting, and Storing GJ. The GJ information processed and stored on a Contractor owned or provided device, must be used solely for the purpose of processing and/or storage of GJ information. Data must be encrypted, including additional peripherals or devices such as a flash drive, thumb drive, and/or external storage. In addition to encryption, any temporary file(s) created by the operating system or user must be deleted after each use. Any and all portable devices or removable media used for GJ must be stored in the approved security container(s) when not in use. The contractor is required to establish an internal process for backing-up GJ information. The USAO can provide physical storage of backed-up GJ information for the Contractor upon request or necessity. The GJ information may not be processed or backed-up on a commercial mainframe, data server, cloud, or with a data warehousing service.

c. Modification and/or Changes to Approved IT. Any modification, repair, or replacement of any IT device used to process and/or store GJ information must be approved by the USAO. Only individuals approved by the USAO are authorized to repair or modify any previously approved device or equipment used for the processing and storage of GJ information.

d. Damaged or Defective Storage Devices. The Contractor will turn over any and all damaged or defective storage media used for processing and/or storing GJ information to the USAO throughout the term of the contract.

e. Access to IT. Access to IT used for, and any products created from or containing, GJ information must be restricted to individuals approved, by name, by the USAO or the Court. Equipment must be turned off and sufficiently secured when not in use even for short periods of time during normal business or working hours as well.

f. IT Storage Device No Longer Used and at End of Contract. When a storage device including a laptop, removable hard drive, flash drive, DVD, etc., is no longer needed during the course of the contract or upon termination of the contract, storage devices used will be given to the COR.

g. Security of Systems and Data including Personally Identifiable Information (PII) Data**.** *The term "PII," as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.*

Standard A (Storing PII on less than 25 Individuals). *This standard applies to Contractors handling electronically stored information containing PII on less than 25 individuals in connection with this contract. Refer to Standard B below if more than 25 individuals.)*

(1) Keep the computer in a safe place, such as a locked office or other location with limited access, when not in use.

(2) Mark any laptop with contact information in case of loss to facilitate its safe return.

(3) Keep the operating system, security, and application software used in connection with any computer updated on a regular basis.

(4) Use anti-viral software.

Standard B (Storing PII on more than 25 Individuals). *This standard applies to Contractors handling electronically stored information containing PII on more than 25 individuals in connection with this contract. Refer to Standard A above if less than 25 individuals.)*

(1) The work to be performed under this contract requires the handling of data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel. For all systems handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including, but not limited to, all Executive Branch system security requirements (*e.g.*, requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 2640.2F.

(2) The Contractor shall provide DOJ access to and information regarding the Contractor's systems when requested by the Department, in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, Federal Information Security Management Act (FISMA) data reviews, and access by the DOJ Office of the Inspector General for its reviews. The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the CO certifying the following requirements:

(a) Laptops must employ hard drive encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 validated product; (FIPS 140-2 is available on line at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. Instructions for obtaining a paper copy of FIPS 140-2 are outlined in the document as well.)

(b) The Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

(c) Laptop will utilize anti-viral software;

(d) The Contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is sensitive information unless designated as non-sensitive by the Department. Contractor-owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, shall not be removed from DOJ facilities unless encrypted using a NIST FIPS 140-2 validated product;

(e) When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;
(f) Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;

(g) Rules of behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and PII; and

(h) All DOJ data will be removed from Contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractor's project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work.

<u>h. Data Security Breach Reporting</u>. By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified above, in the event of any actual or suspected breach of such data (*i.e.*, loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately (and in no event later than within one hour of discovery) report the breach to the CO and COR.) If the data breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, the contractor shall call the EOUSA Security Operations Center at (803) 705-5533 within one hour of discovery of the breach. The Contractor shall also notify the CO as soon as possible during regular business hours.
<u>i. Personally Identifiable Information Security Breach Notification</u>. The Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual who's PII has, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department, and shall not proceed until the Department 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 the Contractor shall be coordinated with and be subject to the approval of the Department. The Contractor assumes full responsibility for taking

corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.

j. Pass-through of IT Security Requirements to Subcontractors. The requirements set forth above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the Contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the Contractor.

5. Destruction Requirements.

The Contractor must destroy by cross-cut shredding that meets or exceeds National Security Agency/Central Security Service (NSA/CSS) Level 4 requirement or by burning all waste documents associated with any GJ proceeding. Or as an alternative, the Contractor may elect to transport GJ waste (i.e., drafts, notes, working papers, CDs, DVDs, typewriter ribbons, copies of GJ information, and other material which is no longer needed) to the USAO for destruction. When GJ information and related working papers are no longer needed during the course of the contract or upon termination of the contract, the original documents and tapes shall be returned to the USAO. This includes storage devices such as hard drives (internal or external), flash drives, CDs or DVDs, memory cards, and other storage media used to store GJ information.

a. Destruction methods and equipment must be approved by the COR in writing.

b. The Contractor is not authorized to destroy any GJ material or replace any electronic storage devices without prior approval from the COR or USAO representative in writing.

c. When an electronic storage device is no longer needed during the course of the contract and/or upon termination of the contract, the storage devices used will be given to the COR for destruction by the Government.

6. Duplication of GJ Information.

The GJ information may not be copied without the approval of the COR or USAO. If duplication of GJ information is required, the Contractor will only produce the number of copies needed or requested. Copiers used to duplicate GJ information must have security features approved by the COR which may include an on-demand or automatic overwrite feature. Running the on-demand overwrite function of the copier immediately after copying the GJ material is encouraged.

7. Delivery, Shipping, and Packaging GJ Information to USAO.

The GJ information must be protected from unauthorized and/or inadvertent disclosure at all times. This includes during shipment and electronic transfer or delivery to the USAO. The Contractor must either (1) hand carry, (2) use government approved messengers/messenger service, (3) use the U.S. Postal Service from an official post office or picked-up by a U.S. Postal employee, (4) use an overnight mail service with the online capability to track packages shipped and delivered, or (5) use a secure government provided file exchange system. The USAO must approve the method(s) before the Contractor can use a given method of delivery. The Contractor must maintain a delivery or shipping log, double-wrap GJ information (envelope within an envelope or box within a box, etc., with the inner packaged marked GJ Information), and must notify the USAO in advance when GJ information is shipped or is electronically transmitted by the Government's file exchange system to the USAO. The use of curbside collection is strictly prohibited when mailing packages containing GJ information.

a. Packing Materials. Grand Jury Information and Transcripts must be double wrapped in two opaque layers; both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, and must clearly display the following warning notice:

GRAND JURY MATERIAL ENCLOSED
TO BE OPENED BY AUTHORIZED PERSONNEL ONLY
UNAUTHORIZED VIEWING OF THIS MATERIAL IS A VIOLATION OF THE LAW

The outer enclosure shall also clearly identify the address of both the sender and the intended recipient except that no markings to indicate that the contents contain grand jury information shall be visible.

b. Using the U.S. Postal Service. When documents cannot be personally transported between authorized recipients, or by official couriers or messengers, the transmittal of GJ information and related working papers shall be transferred by the U.S. Postal Service Certified Mail with a return receipt. Facsimile is not permitted.

c. Using a Commercial Overnight Service. When an urgent requirement exists for overnight delivery of GJ information, the USAO may authorize the use of an overnight delivery service. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the package, and ensure package integrity during transit. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The release signature block on the receipt label must not be waived under any circumstances. The use of external (street side) collection boxes is prohibited. The package

must be physically handed to a uniformed employee of the delivery service and immediately registered into the automated tracking system.

d. Messenger/Courier Services. For the purpose of this contract, any messenger or courier service used by the Contractor is considered a sub-contractor or the contractor's employee and all security requirements apply.

e. File Exchange System. The use of the Government's file exchange system is an efficient and secure means of exchanging materials with the USAO. The CO will provide the file exchange system details, requirements, and procedures to the Contractor upon request.

8. Transportation of and/or Transmitting GJ Information to USAO.

The GJ information is vulnerable to loss, tampering, and even theft during transportation. Equipment used for recording and processing GJ information is also vulnerable to criminal activity. The Contractor must provide and ensure safe transport of GJ material from point of origin directly to facility previously approved by the USAO for the processing and/or storage of GJ information. Local delivery and courier services contracted by the Contractor to deliver GJ information to the USAO must be known to and approved by the USAO.

9. Site Security Reviews and Governmental Oversight.

The COR or a designated USAO representative may conduct an initial and/or recurring security review(s) of the Contractor's location(s) where GJ information is or is to be processed and/or stored.

a. Preliminary Security Review. Prior to the award of a GJ Court Reporter contract, the COR may assess the ability and feasibility of the Contactor to provide and sustain the security requirements contained in the Statement of Work. An inability to provide and sustain the security requirement, in whole or in part, could be cause for disqualification or warrant special arrangements with the USAO to process and store the materials within USAO space and control vice in a commercial facility and/or residence.

b. Initial and Periodic Security Review. At the time of award and periodically thereafter as determined by the COR and/or at the request of the Contractor, the COR or other designated USAO representative may complete an on-site security reviews of the Contractor's facility. The areas subject to inspection include all primary and secondary GJ processing locations and storage locations including proofreading sites. The purpose for the review is to ensure that all of the security requirements and expectations outlined in the Contract are in place and sufficient to ensure the proper protection of the GJ information. The Government's *Federal Grand Jury Court Reporter Contract Security Review Checklist* is included in this Contract and will be used by the Government to complete the site security reviews. The results of the security review could result in termination for cause, issuance of a cure notice, or other remedial action as determined appropriate by the Government.

c. Essential Security Information. The Contractor is required to provide the Government (prior to the start of work and update as needed) the following specific essential security information:

1) The business name and owner.
2) The contactor's physical and mailing address(es) and telephone number(s).
3) A list of any other United States Attorney Offices (USAOs) supported by the contractor.
4) The list of government approved court reporter(s) to perform work under the contract along with the form and date of their latest completed background investigation or the date of temporary waiver if provided by the government; if a national security clearance is also required, list the level and date of clearance.
5) The business name(s), address(es) and telephone number(s) of any sub-contractor(s) including proofreaders.
6) The name(s) of the government approved sub-contractor personnel to perform work under the contractor along with the form and date of their completed background investigation or temporary waiver if provided by the government; if national security clearances are required by the contract, the level and date of clearance.
7) Processing and storage location information:
8) The physical address(es) where grand jury materials will be processed, reviewed and stored by the contractor.
9) Indicate the type of facility (commercial leased space, private residence, etc.).
10) The names of individuals having access (possess alarm code, key, etc.) to the location (room or area) approved by the government for processing and/or storing grand jury information. If it is a private home or a multi-use business location, also describe how the material will be safeguarded against unauthorized, inadvertent, or illegal access by other residents, employees, and guests.
11) The alarm service company name, address, and telephone number.
12) The list of government approved IT processing and storage device(s) consisting of make, model, serial number, and the names of approved users; also indicate who has "administrative privileges and/or rights" over the devices.
13) The location, brand, and model of safe(s) used to store grand jury materials and the date the combination was last changed.

14) The names of individuals having physical access to the government approved contractor maintained safe(s) and also those knowing each safe's combination.

15) The method of delivering or transporting grand jury materials to the USAO.

10. Reporting Requirements.

a. It is the Contractor's obligation to report any incident or situation that places the GJ information at risk of loss, unauthorized disclosure, unapproved review, theft, or tampering. It is essential that this be recorded, the COR informed, and measures taken to immediately minimize or mitigate risk(s). If a theft or break-in, or attempt thereof occurs, the local police are to be contacted. A copy of the police report is to be provided to the COR as soon as available.

b. The Government may request and require the execution of an inadvertent and/or unauthorized disclosure agreement as needed and appropriate. The COR will advise when and how this will be accomplished and will provide an agreement form when appropriate. In essence, the agreement provides notice that access was not approved and/or allowed and any further unauthorized disclosure could subject the individual to certain civil and criminal penalties, including being held in contempt of court.

(end of clause)

OBD-01 Electronic Signatures (MAY 2019)

(a) The Department of Justice is committed to doing business in the most efficient and effective way possible, and to facilitate paperless processes. In furtherance of this goal, the Contracting Officer may apply their digital signature to procurement documents in the Portable Document Format (PDF) through the use of their government issued Personal Identity Verification (PIV) Card with a valid public key certificate. A digital signature made with these certificates is evidence that a specific individual signed the electronic record and that it was not altered. The recipient of a signed document can rely on the digital signature as evidence for a third party that the signature was generated by the claimed signer.

(b) For procurement documents that require a signature from a representative of the Contractor, the Contractor may utilize manual or electronic signature. Should the Contractor utilize an electronic signature, by returning the document with an electronic symbol affixed to the appropriate signature block, the Contractor representative signing on behalf of the Contractor certifies that:

(1) Electronic Form of Signature: The Contractor representative has knowingly adopted, applied or affixed an electronic symbol to the document;

(2) Intent to Sign: The Contractor representative has applied an electronic symbol with the intent to legally bind the Contractor;

(3) Association of Signature to Record: the Contractor representative's signature is attached to the electronic record being signed;

(4) Identification and Authentication of Signer: The Contractor has a means to identify and authenticate a particular person as the signer; and

(5) Integrity of Signed Record: The Contractor can attest to the integrity of the signed record between the time of signature and the returned record to the government.

This clause applies to this document and any subsequent documents (e.g., modifications, task/delivery orders) associated with this action.

Section 9 – Attachments

1. Authorized Individuals & Sample Documents

2. Pricing Schedule

3. Wage Determination

4. Security Checklists