Combined Synopsis/Solicitation Notice

SUBJECT* RFQ: VISN16-Wide Court Reporting and Transcription - SDVOSB Set-Aside - IDC

GENERAL INFORMATION

CONTRACTING OFFICE'S ZIP CODE*	77056-5643
SOLICITATION NUMBER*	36C25626Q1138
QUESTIONS DATE/TIME/ZONE	08-11-2026 1:00pm CENTRAL TIME, CHICAGO, USA
RESPONSE DATE/TIME/ZONE	08-20-2026 1:00pm CENTRAL TIME, CHICAGO, USA
ARCHIVE	1 DAYS AFTER THE RESPONSE DATE
RECOVERY ACT FUNDS	N
SET-ASIDE	SDVOSBC
PRODUCT SERVICE CODE*	R606
NAICS CODE*	561492
CONTRACTING OFFICE ADDRESS	Department of Veterans Affairs Network Contracting Office 16 Galleria Financial Center 5075 Westheimer Road, Suite 750 Houston TX 77056-5643
POINT OF CONTACT*	Contracting Officer Shasta Britt shasta.britt@va.gov

PLACE OF PERFORMANCE

ADDRESS	Department of Veterans Affairs Michael E. DeBakey VA Medical Center MEDVAMC 2002 Holcombe Blvd. Houston TX
POSTAL CODE	77030-4211
COUNTRY	USA

ADDITIONAL INFORMATION

AGENCY'S URL	https://www.va.gov
URL DESCRIPTION	Department of Veterans Affairs
AGENCY CONTACT'S EMAIL ADDRESS	shasta.britt@va.gov
EMAIL DESCRIPTION	36C25626Q1138_RFQ Reponse_Vendor Name

Combined Synopsis/Solicitation Notice

DESCRIPTION

This is a combined synopsis/solicitation for commercial products or commercial services prepared in accordance with part 12. This announcement constitutes the only solicitation. Offers are being requested, and a separate written solicitation will not be issued.

Solicitation number is issued as a request for quotation (RFQ) for VISN-wide Court Reporting and Transcription Services.

This acquisition is set-aside for Service Disable Veteran-Owned Small Business (SDVOSB) concerns. The solicitation documents and incorporated provisions and clauses are those in effect through Revolutionary FAR Overhaul (RFO) (eff. 03/16/2026), FAC 2026-01 (eff. 03/13/2026), FAR Deviation APR 2026 (eff. 04/23/2026), VAAR DEVIATION MAY 2026 (eff. 05/12/2026), VAAM Alert 26-01 (eff. 10/01/2025), and Acquisition Policy Flash 26-30 eff. 05/12/2026). This solicitation incorporates provisions and clauses by reference. The full text of provisions and clauses may be accessed electronically at www.acquisition.gov.

Contractors are required to be actively registered in the System for Award Management (SAM) and certified with the Small Business administrative (SBA) Dynamic Small Business Search (DSBS) as a Service-Disable Veteran-Owned Small Business (SDVOSB). Vendor quote may be considered non-compliant and rejected if the Contracting Officer is unable to verify registration and SDVOSB certification status.

Primary NAICS Code: 561492 – This NAICS code represents the principal purpose of the acquisition, which is for Court Reporting and Stenotype Services.

The Michael E. DeBakey VA Medical Center (MEDVAMC), 2002 Holcombe Blvd, Houston, Texas 77030 is seeking to purchase the requirements described above and within this announcement, RFQ attachment. The government expects this announcement to result in a Firm-Fixed Price Single-Award Indefinite Delivery Contract (IDC) not to exceed five years.

See attached RFQ for the details…

Table of Contents

SECTION B - CONTINUATION CONTRACT OPPORTUNITIES COMBINED SYNOPSIS SOLICITATION (CSS) 4

B.1 CONTRACT ADMINISTRATION DATA 4
B.2 PRICE/COST SCHEDULE 5
ITEM INFORMATION 5

SECTION C - CONTRACT CLAUSES 9

C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 9
C.2 SUPPLEMENTAL INSURANCE REQUIREMENTS 10
C.3 52.216-18 ORDERING (AUG 2020) 11
C.4 52.216-19 ORDER LIMITATIONS (OCT 1995) 11
C.5 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026) 12
C.6 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION) 13
C.7 VAAR 852.219-73 VA NOTICE OF TOTAL SET-ASIDE FOR CERTIFIED SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESSES (JAN 2023) (DEVIATION) 22
C.8 VAAR 852.219-75 VA NOTICE OF LIMITATIONS ON SUBCONTRACTING—CERTIFICATE OF COMPLIANCE FOR SERVICES AND CONSTRUCTION (JAN 2023) (DEVIATION) 25

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS 28

D.1 PERFORMANCE WORK STATEMENT (PWS) 28
D.2 IT CONTRACT SECURITY 35
D.3 WAGE AND DETERMINATION (WD) 46

SECTION E - SOLICITATION PROVISIONS 47

E.1 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES(OCT 2025) (DEVIATION) (TAILORED) 47
E.2 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998) 49
E.3 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION) 50
E.4 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION) 50
E.5 52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION) (TAILORED) 54

SECTION B - CONTINUATION CONTRACT OPPORTUNITIES COMBINED SYNOPSIS SOLICITATION (CSS)

B.1 CONTRACT ADMINISTRATION DATA

1. Contract Administration: All contract administration matters will be handled by the following individual:
    a. CONTRACTOR: Company Name:
    ATTN/POC Name:
    Address:
    Phone:
    Email:
    UEI:
    Contract# (if applicable):

    b. GOVERNMENT: Contracting Officer 36C256
    Department of Veterans Affairs
    Network Contracting Office 16
    Galleria Financial Center
    5075 Westheimer Road, Suite 750
    Houston TX 77056-5643

2. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:
    a. 52.232-33 Payment by Electronic Funds Transfer - System for Award Management through TUNGSTEN

3. INVOICES: Invoices shall be submitted in arrears:
    a. Other: Upon receipt and acceptance by the Government

4. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests. http://www.fsc.va.gov/fsc/einvoice.asp

5. **Offeror shall complete the following located in Sections B thru E of this solicitation to be deemed eligible:**
    a. Volume I:
        a. Section B- CONTRACT ADMINISTRATION DATA, CONTRACTOR contact information.
        b. Section C- 852.219-75 (SIGNED)
        c. Submission of past performance and specifications summarized in this CSS and PWS.
    b. Volume II:
        a. Section B- PRICE/COST SCHEDULE.

6. ACKNOWLEDGMENT OF AMENDMENTS: The offeror acknowledges receipt of amendments to the Solicitation numbered and dated as follows:

AMENDMENT NO	DATE

(End of Contract Administration Data)

B.2 PRICE/COST SCHEDULE

ITEM INFORMATION

ITEM #	DESCRIPTION OF SERVICES	QTY	UNIT	UNIT ANNUAL PRICE	TOTAL LINE PRICE
0001	CLIN 0001 – Standard Transcription Services (IDC) Description: The Contractor shall provide transcription services for any PWS-covered proceeding (including but not limited to AIB, MSPB, EEOC, HRMS, and depositions) for any VISN 16 ordering activity. Specific work details will be identified in individual Task Orders. Unit of Measure: Billable line (65 printable ASCII characters; headers/footers non-billable) NTE Quantity (Annual Ordering Ceiling): 2,000,000 lines Unit Price: $_____ Annual Amount: $_____ Contract Period: IDC Ordering NTE 5 Years POP Begin: 10-01-2026 POP End: 09-30-2031 PRINCIPAL NAICS CODE: 561492 - Court Reporting and Stenotype Services PRODUCT/SERVICE CODE: R606 - Support - Administrative: Court Reporting MANUFACTURER PART NUMBER (MPN): Court Reporting-PWS	5.00	YR	_____	_____
0002	CLIN 0002 – Urgent Transcription Services (IDC) Description: Same scope as CLIN 0001 except Turnaround Time is Urgent (48 hours). Unit of Measure: Billable line (65 printable ASCII characters) NTE Quantity (Annual Ordering Ceiling): 400,000 lines Unit Price: $_____ Annual Amount: $_____ Contract Period: IDC Ordering NTE 5 Years POP Begin: 10-01-2026 POP End: 09-30-2031 PRINCIPAL NAICS CODE: 561492 - Court Reporting and Stenotype Services PRODUCT/SERVICE CODE: R606 - Support - Administrative: Court Reporting MANUFACTURER PART NUMBER (MPN): Court Reporting-PWS	5.00	YR	_____	_____

0003	5.00	YR	_____	_____

CLIN 0003 – Court Reporter Attendance (On-Site or Virtual)

Description:
The Contractor shall provide qualified court reporter attendance for hearings or depositions.

Unit of Measure: Hour
NTE Quantity (Annual Ordering Ceiling): 5,000 hours
Unit Price: $_____
Annual Amount: $_____

Contract Period: IDC Ordering NTE 5 Years
POP Begin: 10-01-2026
POP End: 09-30-2031
PRINCIPAL NAICS CODE: 561492 - Court Reporting and Stenotype Services
PRODUCT/SERVICE CODE: R606 - Support - Administrative: Court Reporting
MANUFACTURER PART NUMBER (MPN): Court Reporting-PWS

0004	5.00	YR	_____	_____

CLIN 0004 – Secure Electronic Delivery & Formatting

Description:
Contractor shall format and deliver completed transcripts per VA templates.

Unit of Measure: Each transcript delivered
NTE Quantity (Annual Ordering Ceiling): 250,000 transcripts
Unit Price: $_____
Annual Amount: $_____

Contract Period: IDC Ordering NTE 5 Years
POP Begin: 10-01-2026
POP End: 09-30-2031
PRINCIPAL NAICS CODE: 561492 - Court Reporting and Stenotype Services
PRODUCT/SERVICE CODE: R606 - Support - Administrative: Court Reporting
MANUFACTURER PART NUMBER (MPN): Court Reporting-PWS

0005	5.00	YR	_____	_____

CLIN 0005 – Audio Capture & Secure Storage

Description:
Secure storage of digital audio recordings for up to 12 months.

Unit of Measure: Month
NTE Quantity (Annual Ordering Ceiling): 12 months
Unit Price: $_____

Annual Amount: $_____ Contract Period: IDC Ordering NTE 5 Years POP Begin: 10-01-2026 POP End: 09-30-2031 PRINCIPAL NAICS CODE: 561492 - Court Reporting and Stenotype Services PRODUCT/SERVICE CODE: R606 - Support - Administrative: Court Reporting MANUFACTURER PART NUMBER (MPN): Court Reporting-PWS	
	GRAND TOTAL VALUE _____

The Contractor shall not exceed the value amount awarded “ceiling” on the issued contract or its orders. The contractor shall communicate to Program POC and CO on any orders that are anticipated to be delayed or exceed contractual obligation listed in Price/Cost Schedule.

The Contractor shall provide all personnel, supervision, management, materials, equipment, and services necessary to perform the work described in this Solicitation for a single firm-fixed price. This firm-fixed price shall be all inclusive and shall include, at a minimum, all direct labor, staff hourly compensation, fringe benefits, overhead, general and administrative expenses, profit, and any other costs necessary to fully perform the required services. No separate or additional payment will be made for labor hours, overhead, or profit beyond the firm-fixed price, except as expressly authorized by a duly executed contract modification. No additional charges outside the firm-fixed price will be accepted. Any attempts to bill the agency for costs outside of the agreed-upon price will be rejected.

Price is a firm-fixed price (FFP) agreement and may not be changed, the estimated annual price listed is an estimate on historical ordering in the past of the total requirement for the services described. The Government may place orders as needed at quantities less than the estimated total price as stated in the schedule of items. There is no express or implied guarantee that services will be ordered regularly. Orders shall not exceed the obligation shown or as outlined at 52.216-19. Any remaining order obligations that result in excess funds will be de-obligated at the end of the order’s period of performance, after issued obligated purchase order has expired and final invoice is paid in full.

Price Evaluation of Options: The Government will evaluate all option clauses using prices submitted for each option year, or, if no separate pricing is submitted, using rates then in effect for the final scheduled performance period. These evaluated option amounts will be added to the total evaluated price but do not obligate the Government to exercise the options.

1. FAR 52.217 8 (Option to Extend Services). Incorporated. For evaluation purposes, the Government will add an amount equal to six (6) times the monthly rate in effect for the final scheduled performance period immediately preceding any 52.217 8 extension. No separate pricing is required; the option price is presumed “reasonably determinable” per FAR.

2. FAR 52.237 3 (Continuity of Services). Incorporated. To evaluate up to 90 days of post-expiration transition support, the Government will include a not-to-exceed amount equal to 30% of the annual rate in effect for the final scheduled performance period, added to the total evaluated price for award purposes only. The Government is not obligated to exercise any or all of such transition; actual phase-out services, if directed by the Contracting Officer, will be reimbursed per contract terms.

[End of Section B]

SECTION C - CONTRACT CLAUSES

ADDENDUM to FAR 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Clauses that are incorporated by reference (by Citation Number, Title, and Date), have the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

The following clauses are incorporated into 52.212-4 as an addendum to this contract:

C.1 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):

https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

FAR Number	Title	Date
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	JUN 2020
52.203-16	PREVENTING PERSONAL CONFLICTS OF INTEREST	JUN 2020
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-13	SYSTEM FOR AWARD MANAGEMENT—MAINTENANCE (DEVIATION)	NOV 2025
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED	JAN 2025
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.212-4	CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION)	OCT 2025
52.217-8	OPTION TO EXTEND SERVICES	NOV 1999
52.222-35	EQUAL OPPORTUNITY FOR VETERANS (DEVIATION)	NOV 2025
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (DEVIATION)	NOV 2025
52.222-37	EMPLOYMENT REPORTS ON VETERANS (DEVIATION)	NOV 2025
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT (DEVIATION)	NOV 2025
52.222-41	SERVICE CONTRACT LABOR STANDARDS (DEVIATION)	NOV 2025
52.222-42	STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES	MAY 2014
52.222-50	COMBATING TRAFFICKING IN PERSONS (DEVIATION)	NOV 2025
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION (DEVIATION)	NOV 2025
52.222-55	MINIMUM WAGES FOR CONTRACTOR WORKERS UNDER EXECUTIVE ORDER 14026 (DEVIATION)	NOV 2025

52.222-62	PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706 (DEVIATION)	NOV 2025
52.224-3	PRIVACY TRAINING ALTERNATE I (JAN 2017)	JAN 2017
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.228-5	INSURANCE—WORK ON A GOVERNMENT INSTALLATION	JAN 1997
52.229-3	FEDERAL, STATE, AND LOCAL TAXES (DEVIATION)	SEP 2025
52.229-4	FEDERAL, STATE, AND LOCAL TAXES (STATE AND LOCAL ADJUSTMENTS) (DEVIATION)	SEP 2025
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-19	AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR	APR 1984
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	PROTEST AFTER AWARD	AUG 1996
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
52.237-3	CONTINUITY OF SERVICES	JAN 1991
52.244-6	SUBCONTRACTS FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION)	APR 2026
852.201-70	CONTRACTING OFFICER'S REPRESENTATIVE	DEC 2022
852.203-70	COMMERCIAL ADVERTISING	MAY 2018
852.211-76	LIQUIDATED DAMAGES-REIMBURSEMENT FOR DATA BREACH COSTS	FEB 2023
852.216-71	ECONOMIC PRICE ADJUSTMENT OF CONTRACT PRICE(S) BASED ON A PRICE INDEX	MAR 2018
852.222-71	COMPLIANCE WITH EXECUTIVE ORDER 13899 (DEVIATION) (APR 2025)	APR 2025
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018
852.242-71	ADMINISTRATIVE CONTRACTING OFFICER	OCT 2020

(End of Clause)

C.2 SUPPLEMENTAL INSURANCE REQUIREMENTS

In accordance with FAR 28.307-2 and FAR 52.228-5, the following minimum coverage shall apply to this contract:

(a) Workers' compensation and employers liability: Contractors are required to comply with applicable Federal and State workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with a Contractor's commercial operations that it would not be practical to require this coverage. Employer's liability coverage of at least $100,000 is required, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

(b) General Liability: $500,000.00 per occurrences.

(c) Automobile liability: $200,000.00 per person; $500,000.00 per occurrence and $20,000.00 property damage.

(d) The successful bidder must present to the Contracting Officer, prior to award, evidence of general liability insurance without any exclusionary clauses for asbestos that would void the general liability coverage.

(End of Clause)

C.3 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 10/01/2026 through 09/30/2031.

(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)

C.4 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 $100.00, 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 $55,000.00;

(2) Any order for a combination of items in excess of $350,000.00; or

(3) A series of orders from the same ordering office within 10 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 5 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)

C.5 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026)

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

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of Clause)

C.6 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION)

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

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at *https://www.sam.gov* (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

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

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Covered article, as defined in 41 U.S.C. 4713(k), means:

(1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;

(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or

(4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

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

Covered telecommunications equipment or services means—

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

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

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

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

Critical technology means—

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

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

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

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

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

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

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

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

FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.

FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency

information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):

(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.

(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoD FASCSA order.

(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) 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;

(2) 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

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;

(9) The Bureau of Intelligence and Research of the Department of State;

(10) The Office of Intelligence and Analysis of the Department of the Treasury;

(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

(12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

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

Kaspersky Lab-covered article means any hardware, software, or service that—

(1) Is developed or provided by a Kaspersky Lab-covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab-covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab-covered entity.

Kaspersky Lab-covered entity means—

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is

to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

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

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.

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

Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).

Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).

(b) *Prohibitions on providing or using specific products or services in performance of contract*. Unless a waiver or exception applies, the Contractor is prohibited from providing any products or services to the Government or using in the performance of the contract any of the following:

(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor’s employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));

(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));

(3) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—

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

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

(c) Prohibition on unmanned aircraft systems manufactured or assembled by American Security Drone Act—covered foreign entities.

(1) Prohibition. The Contractor is prohibited from—

(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);

(ii) On or after December 22, 2025, operating a FASC-prohibited unmanned aircraft system in the performance of the contract (section 1824 of Pub. L. 118-31); and

(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31).

(2) *Procedures*. The Contractor shall search SAM for the FASC-maintained list of American Security Drone Act—covered foreign entities before proposing, or using in performance of the contract, any unmanned aircraft system. Also, the Contractor shall ensure any effort or expenditure associated with a FASC-prohibited unmanned aircraft system is consistent with a corresponding exemption, exception, or waiver determination expressly stated in the contract.

(3) *Exemptions, exceptions, and waivers*. The prohibitions in paragraph (c) of this clause do not apply where the agency has determined an exemption, exception, or waiver applies, and the contract indicates that such a determination has been made. See sections 1823 through 1825 and 1832 of Public Law 118-31 for statutory requirements pertaining to exemptions, exceptions, and waivers.

(d) *Prohibition on using or providing specific products or services or conducting certain transactions regardless of connection to contract*.

(1) *Certain telecommunications and video surveillance equipment, systems, or services*.

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

(ii) This prohibition applies to using covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. This does not prohibit the contractor from using—

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

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

(2) *Office of Foreign Assets Control Restrictions*.

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(ii) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas.

(A) For lists of entities and individuals subject to economic sanctions, see OFAC's List of Specially Designated Nationals and Blocked Persons at *https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists*.

(B) For more information about these restrictions, as well as updates, see OFAC's regulations at 31 CFR chapter V and at *https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information*.

(C) To conduct electronic screens of potential parties to regulated transactions, see the consolidated screening list at *https://www.trade.gov/consolidated-screening-list*, which consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury.

(3) *Sudan prohibition*. The Contractor is prohibited from conducting any restricted business operations in Sudan in accordance with Accountability and Divestment Act of 2007 (Pub. L. 110-174).

(4) *Iran prohibitions*.

(i) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, the contractor shall not engage in certain activities or transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note).

(ii) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, contractor shall not export certain sensitive technology to Iran, as determined by the President, and has an active exclusion in SAM (22 U.S.C. 8515).

(iii) The prohibition in paragraphs (d)(4)(i) and (d)(4)(ii) do not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see part 25).

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $15,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) *Governmentwide exclusion and removal orders*.

(1) Unless the Government has issued an applicable waiver, contractors shall not provide or use as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order as follows:

(i) For solicitations and contracts awarded by a Department of Defense contracting office, DoD FASCSA orders apply.

(ii) For all other solicitations and contracts, DHS FASCSA orders apply.

(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award Management (SAM) at *https://www.sam.gov* to locate applicable FASCSA orders.

(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.

(4) A FASCSA order issued after the date of solicitation applies to this contract only if added by an amendment to the solicitation or modification to the contract (see FAR 40.204-1(c)).

(f)*Reasonable inquiry*. The contractor shall conduct a reasonable inquiry to determine if there are any prohibited products or services. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(g) *Removal of prohibited products and services*. For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any other procurement instrument intended for use by multiple agencies, upon notification from the Contracting Officer, during the performance of the contract, the Contractor shall promptly make any necessary changes or modifications to remove any product or service produced or provided by a source that this clause prohibits.

(h) *General report*.

(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:

(i) Contract number and order number, if applicable;

(ii) The specific prohibition the product or service is not complying with;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the contractor would like the Government to consider a waiver, and asks for such a waiver);

(vii) Whether alternative products or services are available that would comply with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions implemented or recommended.

(2) If a report must be submitted to a contracting office, the Contractor shall submit the report as follows:

(i) If a Department of Defense contracting office, the Contractor shall report to the website at *https://dibnet.dod.mil*.

(ii) For all other contracting offices, the Contractor shall report to the Contracting Officer.

(iii) For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order.

(3) If the report provided does not contain any of the information required by paragraph (h)(1) of this clause, and the contractor later discovers new information that is required by paragraph (h)(1) of this clause, then the contractor shall submit a subsequent report within 72 hours of discovering the new information.

(4) The contractor shall also report the information in paragraph (h)(1) if the contractor wishes to ask for a waiver of the requirements of a new FASCSA order being applied through modification.

(i) *New FASCSA orders report*.

(1) During contract performance, the Contractor shall review SAM at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSA order(s), or for products or services produced by a source subject to FASCSA order(s) not currently identified under paragraph (e) of this clause.

(2) If the Contractor identifies a new FASCSA order(s) that could impact their supply chain, then the Contractor shall conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSA order(s) was provided to the Government or used during contract performance. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(3) The Contractor shall submit a report to the contracting office identified in paragraph (h)(2) of this clause if the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a source was provided to the Government or used during contract performance and is subject to a FASCSA order(s). For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order. The Contractor shall report the following information within 72 hours for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSA order:

(i) Contract number and order number, if applicable;

(ii) Name of the covered article or source subject to a FASCSA order;

(iii) The specific FASCSA order the product or service does not comply with;

(iv) The elements of (h)(1)(iii) through (ix) of this clause.

(j) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (j) but excluding subparagraphs (d)(1) and (i)(1), in all subcontracts and other contractual instruments, including subcontracts for acquiring commercial products or commercial services.

(End of Clause)

C.7 VAAR 852.219-73 VA NOTICE OF TOTAL SET-ASIDE FOR CERTIFIED SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESSES (JAN 2023) (DEVIATION)

(a) *Definition*. for the Department of Veterans Affairs, ‘‘*Service-disabled Veteran-owned small business concern or SDVOSB”*:

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled Veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled Veterans or eligible surviving spouses (see VAAR 802.201, Surviving Spouse definition);

(ii) The management and daily business operations of which are controlled by one or more service-disabled Veterans (or eligible surviving spouses) or, in the case of a service-disabled Veteran with permanent and severe disability, the spouse or permanent caregiver of such Veteran;

(iii) The business meets Federal small business size standards for the applicable North American Industry Classification System (NAICS) code identified in the solicitation document;

(iv) The business has been certified for ownership and control pursuant to 38 U.S.C. 8127, 13 CFR 128, and is listed as certified in the SBA certification database at *https://veterans.certify.sba.gov/*; and

(v) The business agrees to comply with VAAR subpart 819.70 and Small Business Administration (SBA) regulations regarding small business size, government contracting, and the Veteran Small Business Certification Program at 13 CFR parts 121, 125, and 128.

(2) The term ‘‘Service-disabled Veteran’’ means a Veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

(3) The term ‘‘small business concern’’ has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632).

(4) The term ‘‘small business concern owned and controlled by Veterans with service-connected disabilities’’ has the meaning given the term ‘‘*small business concern owned and controlled by service-disabled veterans*’’ under section 3(q)(2) of the Small Business Act (15 U.S.C. 632(q)(2)).

(5) The term *“SDVOSB participant”* or *certified SDVOSB* means a small business that has been certified in the SBA Veteran Small Business Certification Program and listed in the SBA certification database (see 13 CFR 128.102).

(b) *General*. In order for a concern to submit an offer and be eligible for the award of an SDVOSB set-aside or sole source contract, the concern must qualify as a small business concern under the size standard corresponding to the NAICS code assigned to the contract and be listed as an SDVOSB participant in the SBA certification database as set forth in 13 CFR 128.

(1) Offers received from entities that are not certified SDVOSBs and listed in the SBA certification database at the time of offer shall not be considered.

(2) Any award resulting from this solicitation shall be made to a certified SDVOSB listed in the SBA certification database who is eligible at the time of submission of offer(s) and at the time of award.

(3) The requirements in this clause apply to any contract, order or subcontract where the firm receives a benefit or preference from its designation as an SDVOSB, including set-asides, sole source awards, and evaluation preferences.

(c) *Representation*. Pursuant to 38 U.S.C. 8127(e), only certified SDVOSBs listed in the SBA certification database are considered eligible to receive award of a resulting contract. By submitting an offer, the prospective contractor represents that it is an eligible and certified SDVOSB as defined in this clause, 13 CFR 121, 125, and 128, and VAAR subpart 819.70.

(d) *Agreement/LOS certification.* When awarded a contract action, including orders under multipleaward contracts, an SDVOSB agrees that in the performance of the contract, the SDVOSB shall comply with requirements in VAAR subpart 819.70 and SBA regulations on small business size, and government contracting programs at 13 CFR part 121 and part 125, including the non-manufacturer rule and limitations on subcontracting (LOS) requirements in 13 CFR 121.406(b) and 13 CFR 125.6. For the purpose of limitations on subcontracting, only certified SDVOSBs listed in the SBA certification database (including independent contractors) shall be considered eligible and/or ‘‘similarly situated’’ (i.e., a firm that has the same small business program status as the prime contractor). An otherwise eligible firm further agrees to comply with the required LOS certification requirements in this solicitation (see 852.219–75 or 852.219–76 as applicable). These requirements are summarized as follows:

(1) *Services*. In the case of a contract for services (except construction), the SDVOSB prime contractor will not pay more than 50% of the amount paid by the government to the prime for contract performance to firms that are not certified SDVOSBs listed in the SBA certification database (excluding direct costs to the extent they are not the principal purpose of the acquisition and the SDVOSB/ VOSB does not provide the service, such as airline travel, cloud computing services, or mass media purchases). When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract.

(2) *Supplies/products*.

(i) In the case of a contract for supplies or products (other than from a non-manufacturer of such supplies), the SDVOSB prime contractor will not pay more than 50% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, to firms that are not certified SDVOSBs listed in the SBA certification database. When a contract includes both supply and services, the 50 percent limitation shall apply only to the supply portion of the contract.

(ii) In the case of a contract for supplies from a non-manufacturer, the SDVOSB prime contractor will supply the product of a domestic small business manufacturer or processor, unless a waiver as described in 13 CFR 121.406(b)(5) has been granted. Refer to 13 CFR 125.6(a)(2)(ii) for guidance pertaining to multiple item procurements.

(3) *General construction*. In the case of a contract for general construction, the SDVOSB prime contractor will not pay more than 85% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, to firms that are not certified SDVOSBs listed in the SBA certification database.

(4) *Special trade construction contractors*. In the case of a contract for special trade contractors, no more than 75% of the amount paid by the government to the prime for contract performance, excluding the cost of materials, may be paid to firms that are not certified SDVOSBs listed in the SBA certification database.

(5) *Subcontracting*. An SDVOSB subcontractor must meet the NAICS size standard assigned by the prime contractor and be certified and listed in the SBA certification database to count as similarly situated. Any work that a first tier SDVOSB subcontractor further subcontracts will count towards the percent of subcontract amount that cannot be exceeded. For supply or construction contracts, the cost of materials is excluded and not considered to be subcontracted. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the portion of the contract with the preponderance of the expenditure upon which the assigned NAICS is based. For information and more specific requirements, refer to 13 CFR 125.6.

(e) *Required limitations on subcontracting compliance measurement period*. An SDVOSB shall comply with the limitations on subcontracting as follows:

[] By the end of the base term of the contract or order, and then by the end of each subsequent option period; or

[X] By the end of the performance period for each order issued under the contract.

(f) *Joint ventures*. A joint venture may be considered eligible as an SDVOSB if the joint venture complies with the requirements in 13 CFR 128.402 and the managing joint venture partner makes the representations under paragraph (c) of this clause. A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (d) of this clause will be performed by the aggregate of the joint venture participants.

(g) *Precedence*. The VA Veterans First Contracting Program, as defined in VAAR 802.101, subpart 819.70, and this clause, takes precedence over any inconsistencies between the requirements of the SBA Veteran Small Business Certification Program and the VA Veterans First Contracting Program.

(h) *Misrepresentation*. Pursuant to 38 U.S.C. 8127(g), any business concern, including all its principals, that is determined by VA to have willfully and intentionally misrepresented a company's SDVOSB status is subject to debarment from contracting with the Department for a period of not less than five years (see VAAR 809.406–2 Causes for Debarment).

(End of Clause)

C.8 VAAR 852.219-75 VA NOTICE OF LIMITATIONS ON SUBCONTRACTING—CERTIFICATE OF COMPLIANCE FOR SERVICES AND CONSTRUCTION (JAN 2023) (DEVIATION)

(a) Pursuant to 38 U.S.C. 8127(l)(2), the offeror certifies that—

(1) If awarded a contract (see FAR 2.101 definition), it will comply with the limitations on subcontracting requirement as provided in the solicitation and the resultant contract, as follows:

(i) [X] *Services*. In the case of a contract for services (except construction), the contractor will not pay more than 50% of the amount paid by the government to it to firms that are not certified SDVOSBs listed in the SBA certification database as set forth in 852.219–73 or certified VOSBs listed in the SBA certification database as set forth in 852.219–74. Any work that a similarly situated certified SDVOSB/VOSB subcontractor further subcontracts will count towards the 50% subcontract amount that cannot be exceeded. Other direct costs may be excluded to the extent they are not the principal purpose of the acquisition and small business concerns do not provide the service as set forth in 13 CFR 125.6.

(ii) [] *General construction*. In the case of a contract for general construction, the contractor will not pay more than 85% of the amount paid by the government to it to firms that are not certified SDVOSBs listed in the SBA certification database as set forth in 852.219–73 or certified VOSBs listed in the SBA certification database as set forth in 852.219–74. Any work that a similarly situated certified SDVOSB/VOSB subcontractor further subcontracts will count towards the 85% subcontract amount that cannot be exceeded. Cost of materials are excluded and not considered to be subcontracted.

(iii) [] *Special trade construction contractors*. In the case of a contract for special trade contractors, the contractor will not pay more than 75% of the amount paid by the government to it to firms that are not certified SDVOSBs listed in the SBA certification database as set forth in 852.219–73 or certified VOSBs listed in the SBA certification database as set forth in 852.219–74. Any work that a similarly situated certified SDVOSB/VOSB subcontractor further subcontracts will count towards the 75% subcontract amount that cannot be exceeded. Cost of materials are excluded and not considered to be subcontracted.

(2) The offeror acknowledges that this certification concerns a matter within the jurisdiction of an Agency of the United States. The offeror further acknowledges that this certification is subject to Title 18, United States Code, Section 1001, and, as such, a false, fictitious, or fraudulent certification may render the offeror subject to criminal, civil, or administrative penalties, including prosecution.

(3) If VA determines that an SDVOSB/ VOSB awarded a contract pursuant to 38 U.S.C. 8127 did not act in good faith, such SDVOSB/VOSB shall be subject to any or all of the following:

(i) Referral to the VA Suspension and Debarment Committee;

(ii) A fine under section 16(g)(1) of the Small Business Act (15 U.S.C. 645(g)(1)); and

(iii) Prosecution for violating 18 U.S.C. 1001.

(b) The offeror represents and understands that by submission of its offer and award of a contract it may be required to provide copies of documents or records to VA that VA may review to determine whether the offeror complied with the limitations on subcontracting requirement specified in the contract. Contracting officers may, at their discretion, require the contractor to demonstrate its compliance with the limitations on subcontracting at any time during performance and upon completion of a contract if the information regarding such compliance is not already available to the contracting officer. Evidence of compliance includes, but is not limited to, invoices, copies of subcontracts, or a list of the value of tasks performed.

(c) The offeror further agrees to cooperate fully and make available any documents or records as may be required to enable VA to determine compliance with the limitations on subcontracting requirement. The offeror understands that failure to provide documents as requested by VA may result in remedial action as the Government deems appropriate.

(d) Offeror completed certification/fill-in required. The formal certification must be completed, signed and returned with the offeror's bid, quotation, or proposal. The Government will not consider offers for award from offerors that do not provide the certification, and all such responses will be deemed ineligible for evaluation and award.

Certification

I hereby certify that if awarded the contract, _____ will comply with the limitations on subcontracting specified in this clause and in the resultant contract. I further certify that I am authorized to execute this certification on behalf of _____.

Printed Name of Signee: _____

Printed Title of Signee: _____

Signature: _____

Date: _____

Company Name and Address: _____

_____

(End of Clause)

(End of Addendum to 52.212-4)

[End of Section C]

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

D.1 PERFORMANCE WORK STATEMENT (PWS)

Transcription/Court Reporting Services

1. Scope: The contractor shall provide all personnel, supervision, equipment, and services necessary to deliver accurate and timely court reporting and transcription services for all VA facilities within VISN 16. Performance shall meet or exceed the accuracy, timeliness, security, and quality standards defined in this PWS.
    a. Based on VA facility listings and VISN 16 coverage, the following are major VA Medical Centers in the NCO 16 network:
        i. Michael E. DeBakey VA Medical Center, Houston, Texas
        ii. Southeast Louisiana Veterans Health Care System, New Orleans, Louisiana
        iii. Alexandria Veterans Health Care System, Pineville, Louisiana
        iv. Overton Brooks VA Medical Center, Shreveport, Louisiana
        v. Central Arkansas Veterans Healthcare System, Little Rock, Arkansas
        vi. Veterans Health Care System of the Ozarks, Fayetteville, Arkansas
        vii. G.V. (Sonny) Montgomery VA Medical Center, Jackson, Mississippi
        viii. Gulf Coast Veterans Health Care System, Biloxi, Mississippi

2. Acronyms:
    a. Equal Employment Opportunity Commission (EEOC)
    b. Equal Employment Opportunity program (EEO)
    c. Contracting Officer (CO)
    d. Contracting Officer's Representative (COR)
    e. Administrative Investigation Boards (AIB)
    f. Human Resource Management Service (HRMS)
    g. Merit System Protection Board (MSPB)
    h. Department of Veteran Affairs (VA)
        i. VA may be used interchangeably to refer all VA facility listings for VISN 16 coverage listed above.

3. Dictation Subjects: The contractor shall support all VA-required hearing types including but not limited to AIBs, MSPB hearings, EEOC hearings, and depositions. The contractor shall ensure personnel and systems can support these proceedings in accordance with all performance requirements.

4. Definitions:
    a. Character: Printable ASCII characters, including a single space, <CR><LF>. A space between words is counted as one ASCII character. Carriage returns to create blank lines are excluded.
    b. Turnaround Time Standard: Standard transcripts shall be delivered within 10 business days, and urgent requests shall be delivered within 48 hours when identified by the VA.
    c. Variations: Material is dictated by many personnel, which will require the contractor and his/her equipment to adapt to variations on dialect, speech, tone, voice volume, speed, delivery, pronunciation, and enunciation.

5. Destination of transcribed documents: The transcribed documents will be delivered to the VA HRMS or EEO offices.
    a. The contractor shall deliver transcripts in the electronic formats specified by the VA at the time of task order issuance. All deliverables must meet accuracy, completeness, and confidentiality requirements but the contractor may determine internal tools, software, and workflow methods.
    b. Contractor must provide his/her own communications software.
    c. STAT reports, meaning "immediately" or "without delay" are not typically required under this contract; however, if an emergency arises, will request a STAT report from the contractor telephonic electronically, along with any special instructions to the contractor regarding a special delivery location.

6. Format of Documents: Contractor shall be able to formulate types of documents in accordance with the needs of the VA.
    a. General Format: The length of each report will vary according to the type of court report required. The reports will be created and saved as ASCII text -only printable characters, single spaces, and <CR><LF>. The text is double spaced with double space between paragraphs. No report shall include any text other than what was dictated. Documents that appear to be incomplete or the dictation was cut off should be notated as INCOMPLETE DICTATION. An effort to locate a new dictation and/or continuation of the incomplete dictation must be made by the contractor so that the report can be completed as one document. Typed comments or questions other than a statement of INCOMPLETE DICTATION should not be in the transcribed report. If there are questions, a phone call to the contact person must be made to have the question answered.
    b. Header and Footer Format: Specific formats for report types and headers for uploaded reports will be furnished at time of contract award prior to commencement of work. VA will provide formats for new report types as needed. It is the contractor's responsibility to assure all header, and footer information complies with sample header and footer information as furnished by VA technical staff.
    c. Lines: Lines are to be defined as 65-characters per line. Special formatting (underline, bold, etc.) should not be used. Vertical spaces (between lines, between paragraphs, or between text) and footers and headers are not billable. Headers and footers are not to be included in the line length.

d. Scope of Work -Human Resource Management Service HRMS reports are transcribed using dictation equipment.
e. Scope of Work -Equal Employment Opportunity Program EEO reports are transcribed using dictation equipment.
f. Turnaround Time (TAT): The contractor shall meet turnaround times as follows.
    i. Standard: 10 business days
    ii. Urgent: 48 hours from request
    iii. The VA will identify urgent requests at the time of order.
g. Completed Documents: Documents shall be in final form and in accordance with the quality standards called for under the contract.
h. Completed documents shall be transmitted with appropriate document header to facilitate receipt of document by VA computer system.

7. Applicable Laws, Regulations, and Standards.
    a. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
    b. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. Chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
    c. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

8. Quality Control: The contractor shall maintain a Quality Control (QC) plan ensuring compliance with all performance requirements. Errors identified by the Government shall be corrected at no additional cost.
    a. The Contractor shall implement and maintain a quality control (QC) system that results in correction of potential and actual problems throughout the entire scope of contract performance. The QC system shall contain a mechanism for corrective actions without dependence upon government direction. Records of all Contractor QC activities shall be maintained during the life of the contract.
    b. The contractor shall maintain a minimum transcript accuracy of 98 percent. Accuracy includes the correct capture of dictated material, correct spelling, correct speaker identification, and correct punctuation sufficient

to maintain meaning. Percentage is based on ratio of errors to lines. (Example: 1000 lines produced, 20 errors: 20/1000=0.02 or 2% errors. Accuracy is 98%.) Errors are considered to be:

i. Omitted material that is legible or intelligible
ii. Misspelled words
iii. Transposed letters
iv. Transcription that is not reflective of dictation, including material that is not dictated or entering material that is not part of the report such as dictator's directions to the transcriptionist.
v. Punctuation or spelling which changes the meaning of the sentence.
vi. Unauthorized abbreviations (VA will provide a list of approved abbreviations), blank lines or ...@@@" for dictation that is clearly intelligible.

c. Each single-page report which contains one or more errors that change the meaning of the report shall be at no cost to the VA. Multiple-page reports containing two (2) or more errors shall be at no cost to the VA.
d. No more than four (4) errors per 20 reports which do not change the meaning of the report, including, but not limited to, grammar, punctuation, spelling, or transposed letters.
e. The Contractor shall be responsible for correct spelling, including unfamiliar words, checking medical dictionaries and references when needed to distinguish between similar-sounding terms. All material shall be transcribed in the tense dictated. Only terms approved by the VA shall be used.
f. The Contractor shall be required to exercise professional judgment to recognize errors of omission, which are technical in nature (e.g., inability to transcribe due to poor dictation quality). Such errors shall be referred to by the COR for clarification or correction.
g. Reports lost or damaged by the Contractor shall be redone at no additional charge to the Government. The Contractor shall send a letter to the COR and EEO/HRMS representatives stating that the dictation was lost and give the reason.
h. Reports that do not meet the timeliness deadline due to errors or omissions on the part of the VA and which are not correctable by the contractor are not counted against the contractor's performance.
i. The contractor shall correct errors identified by the Government at no additional cost within the timeline specified in Section 8.

9. Quality Assurance: The contractor shall ensure all transcripts are complete, accurate, and free of material errors prior to delivery. The contractor shall return corrected documents within four (4) hours when notified by the VA.
    a. Proof reading: Contractor shall proofread all reports for compliance with established format for each work type and corrections made at that time. For any words or phrases that cannot be transcribed due to difficulties in hearing the dictator’s voice, the transcriptionist shall type "'@@@* for unintelligible words.
    b. Spell Check: Contractor shall use a spell checker on each document and perform corrections for spelling and grammar.

c. Corrections: Any report(s) returned to the contractor for correction for reasons stated herein, shall be corrected within four hours of receipt at no additional expense to VA.
d. The contractor shall retain recordings and final transcripts for 12 months unless otherwise directed by the VA.

10. Retention of Voice and Documents: The contractor shall have the capacity to maintain backup media of voice dictation and transcribed material for a period of 12 months. Voice dictation may be kept for a period of less than 12 months ONLY if certified by COR that documents can be disposed.

11. Records Storage and Ownership: The Contractor shall not create or maintain any records containing any non-public VA information that are not specifically tied to or authorized by the contract. At the conclusion of the first year of the contract and at least once per year thereafter, Contractor shall erase all media containing VA reports that are aged more than 12 months. At each erasure, certify to the VA that the information has been destroyed. The VA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which VA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
    a. Requirements follow for VA sensitive information:
    b. Prohibition of authorized disclosure Data breach notification
    c. Requirement to pay liquidated damages in event of data breach Requirement for annual security/privacy awareness training Required signature of VA's Rules of Behavior

12. Equipment: The Contractor shall have the capability to store digitally dictated voice recordings for a period of not less than twelve (12) months, allowing VA to review dictated reports during that period on an as-needed basis. Recordings shall be easily accessible.

13. Privacy Act: The contractor shall comply with the provisions of the Privacy Act of 1974, Health Insurance Portability and Accountability Act and all applicable VA laws and regulations. Additional information to identify the employee and type of document will be provided by the VA as needed. The Contractor shall not maintain, in any form, any sensitive or patient identified information. The Contractor shall comply with the Privacy Act and HIPAA as it pertains to general patient information, HIV, Drug and Alcohol Abuse, and Sickle Cell Anemia. The Contractor shall have plant security and ADP security necessary to safeguard court reports.

14. Security and Privacy Requirements: Contract employees performing on this contract shall be required to undergo the appropriate background screen. Contract employees shall complete a Special Agreement Check (SAC), which includes completing and submitting the Optional Form (OF) 306 and undergoing a fingerprint screen. Fingerprinting can be accomplished at the medical center badging offices. Employees determined to have an unsatisfactory SAC adjudication are prohibited from performing on this contract. The contractor will not have access to protected

Patient Health Information (PHI) and they will/nor will they have the capability of accessing patient information during the services provided to the VA and if removal of equipment from the VA is required, any memory storage devices, such as hard drives, solid state drives and non-volatile memory units will remain in VA control and will not be removed from VA custody. All research data available for Contractor analyses are de-identified. VA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of VA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to VA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

15. The contractor will not have access to VA Desktop computers, and they will not have access to online resources belonging to the government while conducting services. If removal of equipment from the VA is required, any memory storage devices, such as hard drives, solid state drives and non-volatile memory units will remain in VA control and will not be removed from VA custody

16. The Contractor shall immediately notify the appropriate COR and CO upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment are properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment are no longer required, it shall be returned to VA control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand-carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the [contract vehicle]. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

17. Contract Administration: Monthly invoices shall be submitted in arrears through the designated electronic invoice system. Contractor personnel must maintain compliance with all training and reporting requirements throughout contract performance. Invoices shall provide sufficient details to enable comparisons of billed units to the typed reports.

18. Contractor’s Training and Quality Assurance Plans: All Contractor employees assigned to this contract who create, process, manage records are required to take -provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training. The Contractor shall not retain, use,

sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

19. Workload Fluctuation: The contractor shall have a plan to address periodic fluctuations in VA workload.

20. Information Technology: The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with VA policy.

21. Contingency Services: Contractor shall maintain adequate resources necessary to ensure that transcription services for the VA are uninterrupted regardless of contingency or circumstance.

22. Contractor may set any schedule of work hours for its employees performing work at its own facility under this contract providing the VA's STAT requirements will be met. However, the contract price stated on the price/cost schedule is considered payment in full for all services rendered under this contract.

23. The CO reserves the right to reject any of the contractor's personnel and refuse them permission to perform work under the contract.

24. The Contractor is required to obtain the CO's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and VA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

25. Government Quality Assurance Surveillance: The Government will conduct performance monitoring through random sampling, timeliness reviews, and customer feedback in accordance with the Quality Assurance Surveillance Plan (QASP).

26. Performance Requirements Summary (PRS)

Requirement	Standard	AQL	Surveillance Method	Remedy
Accuracy	≥ 98% accuracy	98%	Random sampling	Correct at no cost
Timeliness	10 days / 48 hours urgent	100%	Invoice & log review	Correct at no cost
Availability	Coverage for all VISN 16 facilities	100%	COR monitoring	Corrective action

(End of PWS)

D.2 IT CONTRACT SECURITY

VA INFORMATION AND INFORMATION SYSTEM SECURITY AND PRIVACY LANGUAGE

1. GENERAL. This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

2. VA INFORMATION CUSTODIAL LANGUAGE. This entire section applies to all acquisitions requiring any Information Security and Privacy language.
    a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter "contract") unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 R*ights in Data – General.* The primary clause used to define computer software license (not data/intellectual property first produced under this contractor or order) is FAR 52.227-19, *Commercial Computer Software License.*
    b. Information made available to the contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 *Rights in Data – General*.
    c. VA information will not be co-mingled with any other data on the contractor's information systems or media storage systems. The contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.
    d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to contractor and subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.
    e. The contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.
    f. The contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are

made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contactor.
h. The contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.
i. The contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.
j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.
k. Notwithstanding the provision above, the contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality- assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the contractor is in receipt of a court order or other requests for the above- mentioned information, the contractor shall immediately refer such court order or other requests to the VA CO for response.
l. Information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.
m. Any data destruction done on behalf of VA by a contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.
n. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, *Guidelines for*

Media Sanitization prior to termination or completion of this contract. If directed by the COR/CO, the contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA.The contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS. This section applies when any person requires access to information made available to the contractor by VA for the performance or administration of this contract or information developed by the contractor in performance or administration of the contract.

   a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of contractor/subcontractor and agent of contractor/subcontractor.

   b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.

   c. All contractors and subcontractors working with VA information are subject to the same security investigative and clearance requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors shall be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the

Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

d. All contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All contractors and subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the contractor must state where all non-U.S. services are provided. The contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.
e. The contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
    i. Contractor/subcontractor personnel no longer has a need for access to VA information or VA information systems.
    ii. Contractor/subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.
    iii. Contractor believes their own personnel or subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.
    iv. Any previously undisclosed changes to contractor/subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.
    v. Contractor/subcontractor personnel have their authorization to work in the United States revoked.
    vi. Agreement by which contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for contractor personnel.
f. In such cases of contract fulfillment, termination, or other causes; the contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by contractor/subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.
g. Contractors/subcontractors who no longer require VA accesses will return VA-issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have

had access to VA information, information systems, networks and VA property in their possessions removed, contractors shall notify the appropriate VA COR/CO.

4. TRAINING. This entire section applies to all acquisitions which include section 3.
    a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:
        i. VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) 10176) and Privacy & HIPAA Training TMS# 10203, initially and annually thereafter.
        ii. Sign and acknowledge (electronically through TMS 10176/10203) understanding of and responsibilities for compliance, relating to access to VA information and information systems initially and annually thereafter; and
        iii. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].
    b. The contractor shall provide the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.
    c. Failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the required training is complete.

5. SECURITY INCIDENT INVESTIGATION. This entire section applies to all acquisitions requiring any Information Security and Privacy language.
    a. The contractor, subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the contractor, subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.
    b. To the extent known by the contractor/subcontractor, the contractor/ subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:
        i. The date and time (or approximation of) the Security Incident occurred.
        ii. The names of individuals involved (when applicable).
        iii. The physical and logical (if applicable) location of the incident.
        iv. Why the Security Incident took place (i.e., catalyst for the failure).
        v. The amount of data belonging to VA believed to have been compromised.
        vi. The remediation measures the contractor is taking to ensure no future incidents of a similar nature.

c. After the contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The contractor, subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.
d. VA IT contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.
e. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the VA Office of Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.
f. The contractor shall comply with VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.
g. With respect to unsecured Protected Health Information (PHI), the contractor is deemed to have discovered a data breach when the contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.
h. If the contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the contractor/subcontractor processes or maintains under the contract; the contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT. Intentionally Left Blank.

7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE. This entire section applies to information systems, systems, major applications, minor applications, enclaves, and platform information technologies (cloud and non- cloud) hosted, operated, maintained, or used on behalf of VA at non-VA facilities.
    a. The contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities. Security controls for collecting, processing, transmitting, and storing of VA sensitive information, must

be in place. The controls will be tested by VA or a VA sanctioned 3PAO and approved by VA prior to hosting, operation, maintenance or use of the information system or systems by or on behalf of VA. This includes conducting compliance risk assessments, security architecture analysis, routine vulnerability scanning, system patching, change management procedures and the completion of an acceptable contingency plan for each system. The contractor's security control procedures shall be the same as procedures used to secure VA-operated information systems.

b. Outsourcing (contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.
c. The contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) on non-VA leased or non-VA owned IT equipment used to store, process or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.
d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).
e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with contractor activities are also subject to such assessments. The contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.
f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

g. The contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessment using government personnel or a third-party if deemed necessary. The contractor shall correct or mitigate any weaknesses discovered during the assessment.
h. VA prohibits the installation and use of personally owned or contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved contractor OE will be subject to technical inspection at any time.
i. The contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.
j. For cases wherein the contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.
k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22- 01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING. This entire section applies whenever section 6 or 7 is included.
    a. Should VA request it, the contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the contractor's IT or systems and controls, to ascertain whether the contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the contractor.
    b. Any audits or tests of the contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the contractor uses to destroy, maintain, receive, retain, or use VA information.
    c. As part of these audits, tests and assessments, the contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.
    d. The contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the contractor has generated as part of its own security assessment. The contractor shall also notify VA of the existence of any such security reports or other related assessments, upon completion and validation.
    e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The contractor shall comply with recommendations which result from these regulatory assessments on the part of VA regulators and associated government agency partners.

9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.
    a. The contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, "Securing the Information and Communications Technology and Services (ICTS) Supply Chain", which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services,

data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the contractor to procure equipment, the contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.
c. All contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The contractor shall make spare parts available. All contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The contractor shall apply encryption technology to protect procured products throughout the delivery process.
d. If a contractor provides software or patches to VA, the contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).
e. The contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report “The Minimum Elements for a Software Bill of Materials (SBOM).”
f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.
g. Throughout the delivery process, the contractor shall demonstrate a capability for detecting unauthorized access (tampering).
h. The contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

10. VIRUSES, FIRMWARE AND MALWARE. This entire section applies when the acquisition involves any product (application, hardware, or software) or when section 6 or 7 is included.
    a. The contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.
    b. The contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The contractor shall use due diligence, if supplying third-party software or patches, to ensure the

third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The contractor shall provide or arrange for the provision of technical justification as to why any “false positive” hit has taken place to ensure their code’s supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.
d. The contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter “virus or other malware”) onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the contractor shall:
    i. Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA’s information networks, computer systems and information systems; and
    ii. Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

11. CRYPTOGRAPHIC REQUIREMENT. This entire section applies whenever the acquisition includes section 6 or 7 is included.
    a. The contractor shall document how the cryptographic system supporting the contractor’s products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.
    b. The contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.
    c. The contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.
    d. The contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.
    e. The contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

12. PATCHING GOVERNANCE. This entire section applies whenever the acquisition includes section 7 is included;
    a. The contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA’s assets. This documentation will include information regarding the follow:
        i. The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and

ii. The approach and capability to remediate newly reported zero-day vulnerabilities for contractor products.

b. The contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.

c. The contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by contractor within these time periods, the contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.

d. The contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third- party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING). Intentionally Left Blank.

14. DATA CENTER PROVISIONS. Intentionally Left Blank.

(End of IT Contract Security)

D.3 WAGE AND DETERMINATION (WD)

Wage and Determination is incorporated by reference (by Citation Number, Title, and Date), have the same force and effect as if were given in full text. Upon request, the Contracting Officer will make full text available.

Service Contract Act WD #: 2015-5233 Revision Number 33 Published Date 05/12/2026. State: Texas; Counties: Austin, Brazoria, Chambers, Fort Bend, Galveston, Harris, Liberty, Montgomery, Waller.

(End of WD)

[End of Section D]

SECTION E - SOLICITATION PROVISIONS

E.1 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES(OCT 2025) (DEVIATION) (TAILORED)

Solicitation Title: VISN 16 Court Reporting & Transcription Services
Place of Performance: VISN 16 Facilities (See PWS Scope) – Michael E. DeBakey VAMC, Houston, TX is primary ordering facility.

1. REQUIREMENT: The Department of Veterans Affairs (VA), Michael E. DeBakey VA Medical Center (MEDVAMC), Houston, Texas, intends to award a single-award, Firm-Fixed-Price Indefinite Delivery Contract (IDC) not to exceed five years for Court Reporting and Transcription Services in accordance with the attached Performance Work Statement (PWS). Contractor performance shall support all VISN 16 facilities listed in the PWS.

2. SET-ASIDE AUTHORITY: This solicitation is a TOTAL Service-Disabled Veteran-Owned Small Business (SDVOSB) set-aside under the Veterans First Contracting Program (38 U.S.C. §§ 8127–8128; VAAR Subpart 819.70). Only SDVOSBs verified in SBA's Veteran Small Business Certification database are eligible for award.

3. GENERAL INSTRUCTIONS"
    - Offer Submission: Quotes shall be submitted electronically via email to the Contracting Officer (CO) by the date/time specified in the solicitation. Late submissions will be handled in accordance with FAR 52.212-1(c).
    - Offer Format: Quotes shall be clear, concise, complete, and formatted by the instructions below. Failure to comply may result in an Unacceptable rating.
        i. Two-Volume Structure: Offerors shall submit two separate volumes:
            1. Volume I – Technical / Quality
            2. Volume II – Price
        ii. Each volume must be submitted as a separate electronic file. Minimum 11-point font; pages numbered consecutively.

4. VOLUME I – TECHNICAL / QUALITY (No Pricing Allowed):
    - Page Limit: 15 pages maximum. Price information included in this volume may render the quote Unacceptable.
    - Volume I shall demonstrate the offeror's capability to meet all requirements in the PWS, including the following:
        i. Ability to Meet All PWS Requirements - Show clear understanding and capability to meet:
            1. Accuracy standard ≥ 98%
            2. Turnaround: Standard 10 business days; urgent 48 hours
            3. VISN 16 facility coverage
            4. Records management compliance (NARA, Privacy Act, HIPAA, 36 CFR 1222.32)
            5. Security/Vetting requirements (SAC, fingerprinting, no PHI access)
            6. Retention and destruction of dictation/transcripts per PWS
            7. Quality Control (QC) plan meeting PWS requirements
        ii. OEM / System Capability Compliance

1. If proprietary dictation or transcription systems are proposed, provide verification of authorized reseller/distributor status (if applicable).

iii. Delivery Schedule Compliance
1. Demonstrate ability to meet PWS turnaround standards and contingency capability to maintain uninterrupted services.

iv. Warranty / Quality Assurance Compliance
1. Describe QC review, proofreading, spell-check, error correction within 4 hours, and handling of incomplete dictation per the PWS.

v. SDVOSB Status Verification
1. Offerors must demonstrate active SDVOSB certification in SBA VetCert at both quote submission and award.
2. For joint ventures, provide:
   a. JV agreement meeting 13 CFR § 128.402(c);
   b. Certification from each SDVOSB partner.

vi. Limitations on Subcontracting
1. Provide a signed VAAR 852.219-75 certification confirming compliance.

vii. Past Performance - While not scored, Offeror must provide:
1. Up to 3 relevant past performance references for similar services.
2. Past performance will not be scored and will be assessed only as Pass/Fail for responsibility under FAR 9.104.

5. VOLUME II – PRICE:
- Submit pricing in a separate file titled “Volume II – Price.”
- Contents:
  i. Fully completed pricing schedule for all Contract Line-Item Numbers (CLINs).
  ii. All prices must be fully burdened.
  iii. Offerors are responsible for mathematical accuracy. Clarifications or rejections may occur if inconsistencies arise.
  iv. No technical information allowed.

6. QUESTIONS:
- All questions shall be submitted via email to the Contract Specialist by the date/time specified in the solicitation, by August 11, 2026, 1:00pm (CT).
- Responses will be issued via amendment.
- Offerors are responsible for monitoring SAM.gov for updates.

7. INCURRING COSTS: Offerors are responsible for all costs associated with preparing and submitting quotes. Submission does not obligate the Government to award a contract.

8. SYSTEM FOR AWARD MANAGEMENT (SAM): Offerors must be registered and active in SAM (www.SAM.gov) at the time of award.

9. SDVOSB VERIFICATION (REQUIRED FOR AWARD)
- Offerors must be verified SDVOSBs in SBA VetCert at time of quote submission and at time of award.
- Failure to verify status in SBA database will result in ineligibility.
- JV-specific rules described under Section 4.e apply.
- The SDVOSB must be the prime contractor.

10. NOTICE OF LPTA PROCEDURES
- Evaluation will use Lowest Price Technically Acceptable (LPTA) methodology.

- Technical acceptability is determined strictly by compliance with the PWS and documents required in Volume I.
- No additional consideration will be given for exceeding requirements.

11. PRELIMINARY REVIEW OF PACKET
    - The CO will perform an initial compliance review.
    - Failure to acknowledge required elements may render the quote package incomplete and subject to rejection.

12. AMENDMENT COMPLIANCE
    - Offerors must acknowledge, sign (SF30), and return all solicitation amendments.
    - Failure to do so may result in quote rejection.

13. MULTIPLE EMAIL SUBMISSIONS: If multiple quotes are received from the same offeror, the latest-date submission will be evaluated.

(End of Instructions)

ADDENDUM to FAR 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Provisions that are incorporated by reference (by Citation Number, Title, and Date), have the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

The following provisions are incorporated into 52.212-1 as an addendum to this solicitation:

E.2 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions 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. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.va.gov/oal/library/vaar/

FAR Number	Title	Date
52.203-11	CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	SEP 2024
52.203-18	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS—REPRESENTATION	JAN 2017
52.204-7	SYSTEM FOR AWARD MANAGEMENT—REGISTRATION (DEVIATION)	NOV 2025

52.212-1	INSTRUCTIONS TO OFFERORS — COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025
52.217-3	EVALUATION EXCLUSIVE OF OPTIONS	APR 1984
52.219-1	SMALL BUSINESS PROGRAM REPRESENTATIONS (DEVIATION)	NOV 2025
52.229-11	TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION	JUN 2020
852.215-72	NOTICE OF INTENT TO RE-SOLICIT	OCT 2019
852.223-70	INSTRUCTIONS TO OFFERORS—SUSTAINABLE ACQUISITION PLAN	SEP 2019
852.233-70	PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION	OCT 2018
852.233-71	ALTERNATE PROTEST PROCEDURE	OCT 2018
852.239-75	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE	FEB 2023

(End of Provision)

E.3 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION)

The Government contemplates award of a Firm-Fixed-Price, Requirements contract resulting from this solicitation.

(End of Provision)

E.4 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION)

(a) *Definitions.* As used in this provision—

Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.

Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

Marginalized populations of Sudan means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and

(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) *Procedures*.

(1) *Covered telecommunications and video surveillance*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at *https://www.sam.gov* for entities excluded from receiving federal awards for “covered telecommunications equipment or services.”

(2) *FASCSA Orders*.

(i) The Offeror shall search in SAM for the phrase “FASCSA order” for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.

(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).

(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.

(c) *Covered telecommunications equipment or services representations*. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror's possession but does not need to include an internal or third-party audit)—

(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and

(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).

(d) *FASCSA Representation*. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror's possession but does not need to include an internal or third-party audit.

(e) *Sudan certification*. By submission of its offer, the offeror certifies, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.

(f) *Iran Representation and Certifications*.

(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), by submission of its offer—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard

Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at *https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx*)

(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—

(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.

(iii) The offeror shall email questions concerning sensitive technology to the Department of State at *CISADA106@state.gov*.

(g) *Disclosure*.

(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:

(i) Contract number and order number, if applicable;

(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);

(vii) Whether alternative products or services are available that would be compliant with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions undertaken or recommended.

(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:

(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at *https://dibnet.dod.mil*.

(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.

(3) If the disclosure provided does not contain any of the information required by paragraph (1), and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.

(h) *Executive agency review of disclosures*. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.

(End of Provision)

(End of Addendum to 52.212-1)

E.5 52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (OCT 2025) (DEVIATION) (TAILORED)

1. BASIS FOR AWARD: Award will be made to the responsible SDVOSB offeror whose quotation is Lowest-Priced among those determined Technically Acceptable and otherwise eligible for award under the Veterans First program. This procurement uses Lowest Price Technically Acceptable (LPTA) procedures.

2. EVALUATION FACTORS: The Government will evaluate quotations solely on the following factors:
    a. Factor 1 – Technical Acceptability: The Technical volume will be evaluated on a Pass/Fail basis. To be rated “Acceptable,” the quotation must clearly demonstrate compliance with all mandatory requirements of the solicitation and PWS, including:
        - Compliance with PWS Requirements: The offeror must demonstrate capability to meet all PWS technical requirements, including:
            1. Transcript accuracy standard of ≥ 98%
            2. Standard and urgent turnaround times: 10 business days and 48 hours respectively
            3. Ability to support all VISN 16 facilities listed in the PWS

4. Quality Control (QC) system, proofreading, spell-check, 4-hour correction requirements
5. Records management and retention requirements (36 CFR 1222.32, NARA, Federal Records Act; 12-month retention; destruction certification)
6. Security & Privacy requirements (SAC, fingerprinting, no PHI access, safeguarding VA records)
7. Ability to ensure contingency service continuity and workload fluctuation support

- Authorized Distributor/Reseller Documentation (If Applicable)
  1. If proprietary dictation/transcription systems are used, offeror must show proof of authorization (Pass/Fail).
- Delivery Schedule Compliance
  1. Offeror must provide a clear plan demonstrating its capability to meet the turnaround standards and rapid correction times specified in the PWS.
- Warranty / Quality Assurance Compliance
  1. Offeror must describe QASP/QC procedures aligned with PWS requirements, including mechanisms for error correction at no cost.
- SDVOSB Eligibility Verification
  1. Offeror must be a verified SDVOSB in SBA's VetCert at time of quotation and award.
  2. If submitting as a Joint Venture, the following must be present to be rated Acceptable:
     a. JV agreement compliant with 13 CFR § 128.402(c);
     b. Certification from each SDVOSB JV member.
- Limitations on Subcontracting
  1. A signed VAAR 852.219-75 certification must be submitted.
- Technical Rating Definitions
  1. Acceptable – Quote meets all technical requirements with no deficiencies.
  2. Unacceptable – Quote fails to meet one or more mandatory requirements; will not be considered for award.

a. FACTOR 2 – Past Performance (Responsibility)
   i. Past performance will be evaluated as Pass/Fail to determine responsibility under FAR 9.104.
   ii. The Government may use CPARS, PPIRS, FAPIIS, or internal VA data.
   iii. Alternate forms of past performance are acceptable and may include relevant project summaries, customer commendations, or other documentation demonstrating successful performance on similar work.

b. FACTOR 3 – PRICE: The Price volume will be evaluated for reasonableness, completeness, and mathematical accuracy.
   - Price evaluation will:
     1. Verify all CLINs are priced;
     2. Confirm all prices are fully burdened;
     3. Ensure no technical information is included in Volume II;
     4. Determine the lowest evaluated price among technically acceptable offerors.
   - Since this is LPTA, prices will not be scored, nor will additional value be assigned for exceeding minimum requirements.

c. FACTOR 4 – SDVOSB VERIFICATION (GO/NO-GO)
    - Offerors must be certified SDVOSBs in the SBA Veteran Small Business Certification database at both the time of submission and time of award.
    - If the CO cannot verify eligibility, the offer will be rated Ineligible and excluded from further consideration.

3. OVERALL EVALUATION APPROACH (LPTA)
    a. The Government will perform evaluations in the following order:
        - Confirm SDVOSB eligibility (Go/No-Go)
        - Evaluate Technical Acceptability (Pass/Fail)
        - Evaluate Price (Lowest Price Technically Acceptable)
    b. Award will be made to the lowest-priced, technically acceptable, verified SDVOSB.

4. NOTICE REGARDING AMENDMENTS: Offerors must acknowledge all amendments (SF30) to remain eligible.

5. RESPONSIBILITY DETERMINATION: Before award, the Government will ensure the selected offeror:
    a. Is registered and active in SAM;
    b. Is a responsible prospective contractor under FAR 9.104.

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

(End of Provision)

[End of Section E]