656-S
Diagnostic Letter Mailers
Date of Award to September 30, 2026

DESCRIPTION	Basis of Award	Advantage Mailing LLC - Anaheim Anaheim, CA UNIT RATE	Advantage Mailing LLC - Anaheim Anaheim, CA COST	Direct Technologies Inc. Suwanee, GA UNIT RATE	Direct Technologies Inc. Suwanee, GA COST	NPC Inc. Claysburg, PA UNIT RATE	NPC Inc. Claysburg, PA COST	One2One Communications LLC dba OneSource Buffalo Grove, IL UNIT RATE	One2One Communications LLC dba OneSource Buffalo Grove, IL COST	Pitney Bowes Stamford, CT UNIT RATE	Pitney Bowes Stamford, CT COST
PROOFS AND PRIOR TO PRODUCTION											
CONSTRUCTION SAMPLES:											
Letters: Digital one-off proof.....per page....	25	$25.00	$625.00	N/C	$0.00	N/C	$0.00	N/C	$0.00	N/C	$0.00
Envelope: Prior to production construction samples.....per order.....	1	$2,500.00	$2,500.00	N/C	$0.00	N/C	$0.00	$25.00	$25.00	N/C	$0.00
PRINTING AND BINDING:											
Makeready/setup charge.....per print order...	48	$2,500.00	$120,000.00	$50.00	$2,400.00	$250.00	$12,000.00	N/C	$0.00		----------
Letters: Printing face and back in black ink, including binding.....per 1,000 printed pages	7,500	$88.88	$666,600.00	$29.00	$217,500.00	$13.00	$97,500.00	$37.50	$281,250.00		----------
ADDITIONAL OPERATIONS:											
6 x 9 1/2" Envelopes (including paper)..... per 1,000 envelopes.....	1,500	$44.44	$66,660.00	$43.20	$64,800.00	$28.31	$42,465.00	$39.10	----------	N/C	$0.00
At contractor's option (per Amendment# 2): #10 Envelopes (including paper)..... per 1,000 envelopes.....	1,500							$22.70	$34,050.00		
GATHERING, INSERTING, AND MAILING:											
Mailers....per 1,000 complete mailers....	1,500	$22.22	$33,330.00	$29.00	$43,500.00	$32.79	$49,185.00	$39.00	$58,500.00	N/C	$0.00
CONTRACTOR SUBTOTAL			----------		$328,200.00		$201,150.00		$373,825.00		----------
DISCOUNT		0.25%	----------	0.00%	$0.00	0.25%	$502.88	0.00%	$0.00		----------
DISCOUNTED TOTALS			----------		$328,200.00		$200,647.13		$373,825.00		----------
							Awarded				

DESCRIPTION	Basis of Award	Wolverine Mailing, Packaging, Warehouse, Inc. Detroit, MI UNIT RATE	Wolverine Mailing, Packaging, Warehouse, Inc. Detroit, MI COST
PROOFS AND PRIOR TO PRODUCTION			
CONSTRUCTION SAMPLES:			
Letters: Digital one-off proof.....per page....	25	N/C	$0.00
Envelope: Prior to production construction samples.....per order.....	1	N/C	$0.00
PRINTING AND BINDING:			
Makeready/setup charge.....per print order...	48	$475.00	$22,800.00
Letters: Printing face and back in black ink, including binding.....per 1,000 printed pages	7,500	$28.00	$210,000.00
ADDITIONAL OPERATIONS:			
Envelopes (including paper)..... per 1,000 envelopes.....	1,500	$42.00	$63,000.00
GATHERING, INSERTING, AND MAILING:			
Mailers....per 1,000 complete mailers....	1,500	$38.00	$57,000.00
CONTRACTOR SUBTOTAL			$352,800.00
DISCOUNT		(1% - 10 days)	$0.00
DISCOUNTED TOTALS			$352,800.00

Reviewed by JY

GPO Jennifer Yarbrough
Contracting Officer

since 1861

September 17, 2025

This is Amendment No. 1. The specifications in our invitation for bids on Program 656-S, scheduled for opening at 11:00 am October 1, 2025 are amended as follows:

1. Change the bid opening date to September 30, 2025.

All other specifications remain the same.

If amendment is not acknowledged on bid, direct acknowledgement to: bids@gpo.gov

Amended bid or acknowledgement must be submitted using the method(s) specified in the solicitation for bid submission.

BIDDER MUST ACKNOWLEDGE RECEIPT OF THIS AMENDMENT PRIOR TO BID OPENING. Failure to acknowledge receipt of amendment, by amendment number, prior to bid-opening time, may be reason for bid being declared nonresponsive.

Sincerely,

J Yarbrough
Digitally signed by Jennifer Yarbrough
Date: 2025.09.17 12:12:33 -07'00'

JENNIFER YARBROUGH
Contracting Officer

GPO **Jennifer Yarbrough**
Contracting Officer

since 1861

September 25, 2025

This is Amendment No. 2. The specifications in our invitation for bids on Program 656-S, scheduled for opening at 11:00 am September 30, 2025 are amended as follows:

1. The bid opening date remains the same.

For clarifications purposes:

2. In order to meet VA directive 6517, the VA requires that the contractor offer a secure cloud module at time of bid submission, or within 30 days of bid submission.

3. At contractor's option, envelope alternatives will be considered as long as the alternative meets the ability to securely display the mailing address and is approved by the ordering agency.

4. At contractor's option, an inserting barcode may be placed on the face of each sheet for automation processing.

5. At contractor's option, the required reporting (see pg. 25) may be provided to ordering agency via a hosted dashboard within a highly secure environment.

All other specifications remain the same.

If amendment is not acknowledged on bid, direct acknowledgement to: bids@gpo.gov.

Amended bid or acknowledgement must be submitted using the method(s) specified in the solicitation for bid submission.

BIDDER MUST ACKNOWLEDGE RECEIPT OF THIS AMENDMENT PRIOR TO BID OPENING. Failure to acknowledge receipt of amendment, by amendment number, prior to bid-opening time, may be reason for bid being declared nonresponsive.

Sincerely,

JENNIFER YARBROUGH
Contracting Officer

U.S. GOVERNMENT PUBLISHING OFFICE
Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Diagnostic Letter Mailers

as requisitioned from the U.S. Government Publishing Office (GPO) by the

U.S. Department of Veterans Affairs (VA)

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning Date of Award (for October 2025) and ending September 30, 2026, plus up to four (4) optional 12-month extension periods that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

BID OPENING: Bids shall be opened virtually at 11:00 a.m., Eastern Time (ET), on October 1, 2025, at the U.S. Government Publishing Office. All parties interested in attending the bid opening shall email bids@gpo.gov one (1) hour prior to the bid opening date and time to request a Microsoft Teams live stream link. This must be a separate email from the bid submission. The link will be emailed prior to the bid opening.

BID SUBMISSION: Bidders must email bids to bids@gpo.gov for this solicitation. No other method of bid submission will be accepted at this time. The program number and bid opening date must be specified in the subject line of the emailed bid submission. ***Bids received after the bid opening date and time specified above will not be considered for award.***

THIS IS A NEW PROGRAM. THERE IS NO ABSTRACT AVAILABLE.

For information of a technical nature, contact Stacy Bindernagel at sbindernagel@gpo.gov or (202) 512-2103.

SECTION 1. - GENERAL TERMS AND CONDITIONS

GPO CONTRACT TERMS: Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)) and GPO Contract Terms, Quality Assurance through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (Rev. 09-19)).

GPO Contract Terms (GPO Publication 310.2) –
https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/contractterms2018.pdf.

GPO QATAP (GPO Publication 310.1) –
https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/qatap-rev-09-19.pdf.

SUBCONTRACTING: Subcontracting is allowed for the manufacturing (including security tint) of the envelope only. The contractor is responsible for enforcing all contract requirements outsourced to a subcontractor.

QUALITY ASSURANCE LEVELS AND STANDARDS: The following levels and standards shall apply to these specifications:

Product Quality Levels:

(a) Printing (page related) Attributes – Level III
(b) Finishing (item related) Attributes – Level III

Inspection Levels (from ANSI/ASQC Z1.4):

(a) Non-destructive Tests – General Inspection Level I.
(b) Destructive Tests – Special Inspection Level S-2.

Specified Standards: The specified standards for the attributes requiring them shall be:

Attribute	Specified Standard
P-7. Type Quality and Uniformity	Average type dimension

OPTION TO EXTEND THE TERM OF THE CONTRACT: The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed five (5) years as a result of, and including, any extension(s) added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustment(s).

EXTENSION OF CONTRACT TERM: At the request of the Government, the term of any contract resulting from this solicitation may be extended for such period of time as may be mutually agreeable to the GPO and the contractor.

ECONOMIC PRICE ADJUSTMENT: The pricing under this contract shall be adjusted in accordance with this clause, provided that in no event will any pricing adjustment be made that would exceed the maximum permissible under any law in effect at the time of the adjustment. There will be no adjustment for orders placed during the first period specified below. Pricing will thereafter be eligible for adjustment during the second and any succeeding performance period(s). For each performance period after the first, a percentage figure will be calculated as described below and that figure will be the economic price adjustment for that entire next period. Pricing adjustments under this clause are not applicable to reimbursable postage or transportation costs, or to paper, if paper prices are subject to adjustment by separate clause elsewhere in this contract.

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from Date of Award to September 30, 2026, and the second and any succeeding period(s) will extend for 12 months from the end of the last preceding period, except that the length of the final period may vary. The first day of the second and any succeeding period(s) will be the effective date of the economic price adjustment for that period.

Pricing adjustments in accordance with this clause will be based on changes in the seasonally adjusted "Consumer Price Index For All Urban Consumers - Commodities Less Food" (Index) published monthly in the CPI Detailed Report by the U.S. Department of Labor, Bureau of Labor Statistics.

The economic price adjustment will be the percentage difference between Index averages as specified in this paragraph. An index called the variable index will be calculated by averaging the monthly Indexes from the 12-month interval ending three (3) months prior to the beginning of the period being considered for adjustment. This average is then compared to the average of the monthly Indexes for the 12-month interval ending June 30, 2025, called the base index. The percentage change (plus or minus) of the variable index from the base index will be the economic price adjustment for the period being considered for adjustment.

The Government will notify the contractor by contract modification specifying the percentage increase or decrease to be applied to invoices for orders placed during the period indicated. The contractor shall apply the percentage increase or decrease against the total price of the invoice less reimbursable postage or transportation costs and separately adjusted paper prices. Payment discounts shall be applied after the invoice price is adjusted.

WARNING: Proper control and handling must be maintained at all times to prevent any information or materials required to produce the products ordered under these specifications from falling into unauthorized hands. The contractor shall not retain or distribute, in any form, any part of the materials furnished by the Government which are not consumed in the preparation of the work, or which are generated as a result of this contract.

Unless otherwise indicated herein, all extra copies, materials, waste, etc., must be destroyed. (See "*Security Control Plans"* and "*Disposal of Waste Materials Plan*" under the "PREAWARD PRODUCTION PLANS" for additional information.)

SECURITY REQUIREMENTS: VA Handbook 6500.6, Appendix C – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION IN CONTRACTS, AS APPROPRIATE.

NOTE: All references to "contractors" (plural) are to be disregarded. This program is a single award and will be awarded to one contractor. All references to "subcontractor," "subcontracts," and "subcontracting" in the security requirements are to be disregarded (see "SUBCONTRACTING" specified herein for more information). The terms "business day" and "workday" are used interchangeably throughout these specifications.

1. GENERAL.

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.

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 *Rights 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.

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 Rules of Behavior (ROB) (see Attachment 1, following the Exhibits) 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:

(1) Contractor/subcontractor personnel no longer has a need for access to VA information or VA information systems.

(2) Contractor/subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

(3) 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.

(4) 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.

(5) Contractor/subcontractor personnel have their authorization to work in the United States revoked.

(6) 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.

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:

(1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter. (NOTE: VA will provide access to the training after award.)

(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access.

b. The contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five business 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.

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:

(1) The date and time (or approximation of) the Security Incident occurred.

(2) The names of individuals involved (when applicable).

(3) The physical and logical (if applicable) location of the incident.

(4) Why the Security Incident took place (i.e., catalyst for the failure).

(5) The amount of data belonging to VA believed to have been compromised.

(6) 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. *(NOTE: The cost of the liquidated damages for paragraph (c) and for paragraph (d) in the attached link is $37.50 per affected individual.)*

6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT.

a. Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).

b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the security and privacy requirements for cloud environments.

c. VA IT contractors, subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, *Risk Management Framework for Cloud Computing Services* and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

d. The contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M- 22-18 (September 14, 2022). The term "software" includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

e. The contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the contractor did not develop, all software configurations and all customizations.

f. The contractor shall ensure all contractor delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.

g. The contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository.

h. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default "program files" directory with silently install and uninstall. The contractor shall perform testing of all updates and patching prior to implementation on VA systems.

i. Applications designed for normal end users will run in the standard user context without elevated system administration privileges.

j. The contractor-delivered solutions shall reside on VA approved operating systems. Exceptions to this will only be granted with the written approval of the COR/CO.

k. The contractor shall design, develop, and implement security and privacy controls in accordance with the provisions of VA security system development life cycle outlined in NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, VA Directive and Handbook 6500, and VA Handbook 6517.

l. The contractor shall comply with the Privacy Act of 1974 (the Act), FAR 52.224- 2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.

m. The contractor shall ensure the security of all procured or developed information systems, systems, major applications, minor applications, enclaves and platform information technologies, including their subcomponents (hereinafter referred to as "Information Systems") throughout the life of this contract and any extension, warranty, or maintenance periods. This includes security configurations, workarounds, patches, hotfixes, upgrades, replacements and any physical components which may be necessary to remediate all security vulnerabilities published or known to the contractor anywhere in the information systems (including systems, operating systems, products, hardware, software, applications and firmware). The contractor shall ensure security fixes do not negatively impact the Information Systems.

n. When the contractor is responsible for operations or maintenance of the systems, the contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE.

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. (See "PREAWARD PRODUCTION PLANS, *Disposal of Waste Materials Plan*" specified herein for more information.)

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.

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.

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.

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:

(1) 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

(2) 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.

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.

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 following:

(1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and

(2) 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 calendar 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).

a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing Devices shall comply with all applicable Federal law, regulations, and VA policies. New developments require creation, testing, evaluation, and authorization in compliance with processes specified on the Specialized Device Cybersecurity Department Enterprise Risk Management (SDCD-ERM) Portal, VA Directive 6550, *Pre-Procurement Assessment and Implementation of Medical Devices/Systems*, VA Handbook 6500, and the VA Information Security Knowledge Service. Deviations from Federal law, regulations, and VA Policy are identified and documented as part of VA Directive 6550 and/or the VA Enterprise Risk Analysis (ERA) processes for Specialized Devices/Systems processes.

b. All contractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500 and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the contractor shall work though the COR/CO for governance or resolution.

c. The contractor shall certify to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA needs to be created, the contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.

d. The contractor shall comply with all practices documented by the Food and Drug Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Post-market Management of Cybersecurity in Medical Devices.

e. The contractor shall design devices capable of accepting all applicable security patches with or without the support of the contractor personnel. If patching can only be completed by the contractor, the contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.

f. The contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the contractor cannot install an anti-virus / anti- malware application.

g. The contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to, or installation at, a VA location.

h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive information will be returned to the contractor with media removed. When the contract requires return of equipment, the options available to the contractor are the following:

(1) The contractor shall accept the system without the drive, firmware, and solid state.

(2) VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn-in; or

(3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then:

(a) The equipment contractor shall have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact.

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

14. DATA CENTER PROVISIONS.

a. The contractor shall ensure the VA network is accessed in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

b. The contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

c. The contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards, or encrypted tunnels).

d. The contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.

e. The contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

f. The contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.

PREAWARD SURVEY: In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract. As part of the financial determination, the contractor in line for award may be required to provide one or more of the following financial documents:

1) Most recent profit and loss statement
2) Most recent balance sheet
3) Statement of cash flows
4) Current official bank statement
5) Current lines of credit (with amounts available)
6) Letter of commitment from paper supplier(s)
7) Letter of commitment from any subcontractor

The documents will be reviewed to validate that adequate financial resources are available to perform the contract requirements. Documents submitted will be kept confidential and used only for the determination of responsibility by the Government. Failure to provide the requested information in the time specified by the Government may result in the Contracting Officer not having adequate information to reach an affirmative determination of responsibility.

Additionally, the preaward survey will include a review of all subcontractors (as applicable) involved, along with their specific functions, and the contractor's security control and disposal of waste material plans as required by this specification.

PREAWARD PRODUCTION PLANS: As part of the preaward survey, the contractor shall present, in writing, to the Contracting Officer within five (5) workdays of being notified to do so by the Contracting Officer or his/her representative, detailed plans for each of the below activities. If the Government requests additional information after review of the production plans, the contractor must submit updated plans within two (2) workdays of request.

The Preaward Production Plans must be formatted so that each plan, as specified below, is its own section, and all information required for that plan is specified in that section. The plans must be furnished as one document with each plan separately identified.

Option Years: For each option year that may be exercised, the contractor will be required to review their plans and re-submit in writing the above plans detailing any changes and/or revisions that may have occurred. The revised plans are subject to Government approval and must be submitted to the Contracting Officer or his/her representative within five (5) workdays of notification of the option year being exercised.

NOTE: If there are no changes/revisions, the contractor will be required to submit to the Contracting Officer or his/her representative a statement confirming that the current plans are still in effect.

These proposed plans are subject to review and approval by the Government, and award will not be made prior to approval of same. The Government reserves the right to waive some or all of these plans.

Security Control Plan: The contractor shall maintain, in operation, an effective security system where items by these specifications are produced and/or stored (awaiting distribution or disposal) to assure against theft and/or the product falling into unauthorized hands.

The Government retains the right to conduct security reviews at any time during the term of the contract.

The security control plans must address in detail, at a minimum, the following –

- How all accountable materials will be handled throughout all phases of production.
- How the disposal of waste materials will be handled. (See "*Disposal of Waste Materials Plan*.")
- If applicable, list of subcontractor(s) and their specific function.
- How all applicable Government-mandated security/privacy/rules and regulations, as cited in this contract, shall be adhered to by the contractor and/or subcontractor(s), as applicable.

Disposal of Waste Materials Plan: The contractor is required to demonstrate how all waste materials used in the production of sensitive VA records will be definitively destroyed (e.g., burning, pulping, shredding, macerating, or other suitable similar means). Electronic records must be definitively destroyed in a manner that prevents reconstruction. *Definitively* destroying the records means the material cannot be reassembled and used in an inappropriate manner in violation of law and regulations. *Sensitive* records are records that are national security classified or exempted from disclosure by statute, including the Privacy Act or regulation.

The contractor, at a minimum, must crosscut shred all documents into squares not to exceed 1/4". All documents to be destroyed cannot leave the security of the building and must be destroyed at contractor's printing site. The contractor must specify the method planned to dispose of the material.

Subcontracting is not allowed.

POSTAWARD CONFERENCE: Unless waived by the Contracting Officer, the total requirements of the job as indicated in these specifications will be reviewed by Government representatives with the contractor's representatives at the U.S. Government Publishing Office, Washington, DC, immediately after award. The postaward conference will be held via teleconference.

Person(s) that the contractor deems necessary for the successful implementation of the contract must be in attendance.

ASSIGNMENT OF JACKETS, PURCHASE, TASK, AND PRINT ORDERS: A GPO jacket number will be assigned and a purchase order issued to the contractor to cover work performed. The purchase order will be supplemented by an individual electronic task order for each job placed with the contractor. A print order will be issued weekly and will indicate the quantity to be produced and any other information pertinent to the particular order.

ORDERING: Items to be furnished under the contract shall be ordered by the issuance of weekly print orders (supplemented by task orders) by the Government. Orders may be issued under the contract from Date of Award through September 30, 2026, plus for such additional period(s) as the contract is extended. All task orders and print orders issued hereunder are subject to the terms and conditions of the contract. The contract shall control in the event of conflict with any task order or print order.

Task orders will be "issued" for purposes of the contract and will detail the volume of letters required. A print order (GPO Form 2511) will be used for billing purposes; will be issued weekly; and will cover all task orders issued the previous week.

A task order or print order shall be "issued" upon notification by the Government for purposes of the contract when it is electronically transmitted or otherwise physically furnished to the contractor in conformance with the schedule.

REQUIREMENTS: This is a requirements contract for the items and for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "ORDERING." The quantities of items specified herein are estimates only and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated," it shall not constitute the basis for an equitable price adjustment under this contract.

Except as otherwise provided in this contract, the Government shall order from the contractor all the items set forth which are required to be purchased by the Government activity identified on page 1.

The Government shall not be required to purchase from the contractor, requirements in excess of the limit on total orders under this contract, if any.

Orders issued during the effective period of this contract and not completed within that time shall be completed by the contractor within the time specified in the order, and the rights and obligations of the contractor and the Government respecting those orders shall be governed by the terms of this contract to the same extent as if completed during the effective period of this contract.

If shipment/delivery of any quantity of an item covered by the contract is required by reason of urgency prior to the earliest date that shipment/delivery may be specified under this contract, and if the contractor will not accept an order providing for the accelerated shipment/delivery, the Government may procure this requirement from another source.

The Government may issue orders which provide for shipment/delivery to or performance at multiple destinations.

Subject to any limitations elsewhere in this contract, the contractor shall furnish to the Government all items set forth herein which are called for by print orders issued in accordance with the "ORDERING" clause of this contract.

PRIVACY ACT NOTIFICATION: This procurement action requires the contractor to do one or more of the following: design, develop, or operate a system of records on individuals to accomplish an agency function in accordance with the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties as stated in 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES. It is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a, specifically, 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES and m(1) GOVERNMENT CONTRACTORS.

PRIVACY ACT

(a) The contractor agrees:

(1) to comply with the Privacy Act of 1974 and the rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals in order to accomplish an agency function when the contract specifically identifies (i) the system or systems of records and (ii) the work to be performed by the contractor in terms of any one or combination of the following: (A) design, (B) development, or (C) operation;

(2) to include the solicitation notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation when the statement of work in the proposed subcontract requires the design, development, or operation of a system of records on individuals to accomplish an agency function; and

(2) to include this clause, including this paragraph (3), in all subcontracts awarded pursuant to this contract which require the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved where the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency where the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act when the contract is for the operation of a system of records on individuals to accomplish an agency function, the contractor and any employee of the contractor is considered to be an employee of the agency.

(c) The terms used in this clause have the following meanings:

(1) "Operation of a system of records" means performance of any of the activities associated with maintaining the system of records including the collection, use, and dissemination of records.

(2) "Record" means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(3) "System of records" on individuals means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

ADDITIONAL EMAILED BID SUBMISSION PROVISIONS: The Government will not be responsible for any failure attributable to the transmission or receipt of the emailed bid including, but not limited to, the following:

1. Illegibility of bid.
2. Emails over 75 MB may not be received by GPO due to size limitations for receiving emails.
3. The bidder's email provider may have different size limitations for sending email; however, bidders are advised not to exceed GPO's stated limit.
4. When the email bid is received by GPO, it will remain unopened until the specified bid opening time. Government personnel will not validate receipt of the emailed bid prior to bid opening. GPO will use the prevailing time (specified as the local time zone) and the exact time that the email is received by GPO's email server as the official time stamp for bid receipt at the specified location.

PAYMENT: Submitting invoices for payment via the GPO fax gateway (if no samples are required) utilizing the GPO barcode coversheet program application is the most efficient method of receiving payment. Instruction for using this method can be found at the following web address: http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

Invoices may also be mailed to: U.S. Government Publishing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401.

For more information about the billing process, refer to the General Information of the Office of Finance web page located at: https://www.gpo.gov/how-to-work-with-us/vendors/how-to-get-paid.

Contractor's billing invoice must be itemized in accordance with the items in the "SCHEDULE OF PRICES."

SECTION 2. - SPECIFICATIONS

SCOPE: These specifications cover the production of mailers consisting of a letter and mail-out envelope requiring such operations as electronic prepress, printing, binding, construction, gathering and inserting, and distribution.

TITLE: Diagnostic Letter Mailers.

FREQUENCY OF ORDERS:

An electronic task order (for example, an email) will be issued throughout the week, Monday through Friday, for production and distribution of the letters. One to five task orders may be issued each week but no more than one task order per workday.

A print order (GPO Form 2511) will be issued the following Monday and will indicate the total number of electronic task orders placed and the total number of letters ordered the previous week.

QUANTITY: The estimated requirement for all letters is 100,000 to 200,000 per month. Each weekly print order will be for approximately 25,000 to 50,000 letters.

The Government reserves the right to increase or decrease by 25% the total number of letters ordered annually.

NUMBER OF PAGES:

Letters: Approximately 1 to 11 printed pages (6 leaves) per letter.
Envelopes: Face only (after manufacturing).

TRIM SIZES:

Letters: 8-1/2 x 11".
Envelopes: 6 x 9-1/2", plus flap, with double windows.

GOVERNMENT TO FURNISH:

Letters: One (1) Adobe Acrobat (current or near current version) PDF file will be furnished for each individual letter that will consist of both the static and variable information for the recipient. Files will be furnished via contractor-hosted SFTP. PDF files will have all printer and screen fonts embedded. (The contractor is cautioned that furnished fonts are the property of the Government and/or its originator. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract.)

NOTE: At some point during the term of the contract, the ordering agency may require that all files be furnished via Government-hosted SFTP.

Identification markings such as register marks, commercial identification marks of any kind, etc., except GPO imprint, form number, and revision date, carried in the electronic files, must not print on finished product.

EXHIBITS: The facsimiles of sample pages shown as Exhibits A and B are representative of the requirements which will be ordered under this contract. However, it cannot be guaranteed that future orders will correspond exactly to these exhibits.

CONTRACTOR TO FURNISH: All materials and operations, other than those listed under "GOVERNMENT TO FURNISH," necessary to produce the products in accordance with these specifications.

The contractor must be able to accept files electronically via their secure contractor-hosted SFTP server. Appropriate log-on instructions and protocol shall be provided by the contractor at time of award. The contractor shall provide security, which at a minimum, shall require a unique user ID and password for access.

If required, the contractor must be able to download files electronically from a Government-hosted SFTP server. Appropriate log-on instructions and protocol will be provided by the Government at time of award.

ELECTRONIC PREPRESS: Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure correct output of the required production image. Any errors, media damage, or data corruption that might interfere with proper file image processing must be reported to the ordering agency contact as specified on the print order.

The contractor shall create or alter any necessary trapping, set proper screen angles and screen frequency, and define file output selection for the imaging device being utilized. Furnished files must be imaged as necessary to meet the assigned quality level.

PROOFS (LETTERS): Proofs will be required on the first order only.

One (1) set of digital color one-off proofs created using the same output device that will be used to produce the final printed product on the actual production stock. Proofs shall be collated with all elements in proper position (not pasted up), imaged face and back, trimmed, and folded to the finished size/format of the product, as applicable.

Contractor to furnish a proof (of all pages) for the first five (5) files received. Proofs are to include all the live variable data included in the furnished files.

If any contractor's errors are serious enough in the opinion of the GPO to require revised proofs, the revised proofs are to be provided at no expense to the Government. No extra time can be allowed for this reproofing; such operations must be accomplished within the original production schedule allotted in the specifications.

The contractor must not print prior to receipt of an "O.K. to Print."

PRIOR TO PRODUCTION CONSTRUCTION SAMPLES (ENVELOPES): On the first order, the sample requirement for this contract is not less than five (5) construction samples (no printing required with the exception of the security tint).

Each sample shall be constructed as specified and must be of the size, kind, and quality that the contractor will furnish. Samples must be constructed of the paper as specified under "STOCK/PAPER."

Samples will be inspected and tested and must comply with the specifications as to construction, kind, and quality of materials.

The samples must be submitted to the ordering agency with the proofs (see "PROOFS" and "SCHEDULE").

The Government will approve, conditionally approve, or disapprove the samples within three (3) workdays of the receipt thereof. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons therefore.

If the samples are disapproved by the Government, the Government, at its option, may require the contractor to submit additional samples for inspection and test, in the time and under the terms and conditions specified in the notice of rejection. Such additional samples shall be furnished, and necessary changes made, at no additional cost to the Government and with no extension in the shipping schedule. The Government will require the time specified above to inspect and test any additional samples required.

In the event the additional samples are disapproved by the Government, the contractor shall be deemed to have failed to make delivery within the meaning of the default clause in which event this contract shall be subject to termination for default, provided however, that the failure of the Government to terminate the contract for default in such event shall not relieve the contractor of the responsibility to deliver the contract quantities in accordance with the shipping schedule.

In the event the Government fails to approve, conditionally approve, or disapprove the samples within the time specified, the Contracting Officer shall automatically extend the shipping schedule in accordance with Contract Clause 12, "Notice of Compliance With Schedules," of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)).

Manufacture of the final product prior to approval of the samples submitted is at the contractor's risk. Samples will not be returned to the contractor. All costs, including the costs of all samples, shall be charged in accordance with the applicable line item in the "SCHEDULE OF PRICES."

STOCK/PAPER: The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No. 13" dated September 2019.

Government Paper Specification Standards No. 13 - https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/vol_13.pdf.

All text paper used in each copy must be of a uniform shade.

Letters: White Uncoated Text, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

Envelopes: White Writing Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20.

PRINTING:

Letters: Print leaves face only or face and back, head-to-head, in black. Printing consists of text and line matter and agency seal/logo. Variable image in black. Variable imaging consists of text and line matter to include, but not limited to, name and address and medical test/lab results. (See Exhibits A and B.) NOTE: Files will be formatted so that the return and mailing addresses are in the standard locations on a letter.

Envelopes: There is no printing required on the outside (after manufacturing) of the envelopes; however, envelopes require a security tint printed on the inside (back before manufacturing) in black ink. The contractor may use their own design but must guarantee that the product will ensure complete opacity and prevent show through of any material contained therein.

MARGINS: Margins will be as indicated on the task order or furnished electronic media.

BINDING (Letters): Trim each leaf four sides.

CONSTRUCTION (Envelopes): The Government reserves the right to make changes to the envelope at any time during the term of the contract. Notification of a proposed change will be given with sufficient time for the contractor to allow for the change and submit samples to the Government. The contractor is not to maintain more than a 60-calendar day inventory of the envelope required on this contract. The Government will not be required to purchase from the contractor the inventory of any stocked envelopes remaining on hand in excess of what was authorized when an envelope format change is implemented. However, if a revision occurs which requires destruction of outdated envelope stock, all costs incurred are to be in accordance with the "SCHEDULE OF PRICES," as applicable. No additional charge may be incurred.

Envelope must be open side, with gummed, fold-over flap for sealing and contain high-cut diagonal or side seams, at contractor's option. Flap is at the contractor's option but must meet all USPS requirements. Flap must be coated with suitable glue that will securely seal the envelope without adhering to contents, permit easy opening by the recipient, and not permit resealing of the envelope.

Envelope to contain two (2) windows – one for the return address and one for the mailing address, both with slightly rounded corners. Size and location of windows are at the discretion of the contractor; however, the contractor must ensure that only the return address and the mailing address are visible through the applicable windows. No other text on the letter can be visible through either window.

Both windows are to be covered with a suitable transparent, low-gloss, poly-type material that must be clear of smudges, lines, and distortions. Poly-type material must be securely affixed to the inside of the envelope so as not to interfere with insertion of contents. Window material must meet the current USPS readability standards/requirements.

GATHERING AND INSERTING: Gather leaves of each letter in proper sequence. Leaves are to be nested together with all faces forward. Fold from 8-1/2 x 11" down to 8-1/2 x 5-1/2" with return and mailing addresses facing out for visibility through applicable windows.

It is the contractor's responsibility to ensure that only the return and mailing addresses on the letter will be visible through the applicable windows and that only one letter is inserted into each envelope.

Seal envelopes.

DISTRIBUTION: Mail f.o.b. contractor's city to domestic (nationwide, including Alaska, Hawaii, APO/FPO, and American Territories) destinations. (The contractor is responsible for all costs incurred in transporting the mailers to the U.S. Postal Service facility.)

All mailing shall be made at the First-Class rate - *reimbursable*.

The contractor will be required to apply the appropriate postage to each mailer. Contractor will be reimbursed for all mailing costs upon submission of complete mailing receipts with billing invoice for payment.

Contractor is responsible for sorting/processing the mailers in order to receive the maximum postal discounts allowable in accordance with the USPS mailing regulations in effect at time of mailing.

All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for "Domestic Mail."

For Each Print Order - On the same day as submitting the invoice to GPO for payment (see "PAYMENT" specified herein), contractor must email a copy of their billing invoice and all postal receipts to the ordering agency contact as specified on the print order.

All expenses incidental to receiving furnished materials (as applicable) and submitting proofs and construction samples must be borne by the contractor.

SCHEDULE: Adherence to this schedule must be maintained. Contractor must not start production of any job prior to receipt of the individual task order or print order (GPO Form 2511), as applicable.

Print order and furnished materials will be furnished via contractor-hosted SFTP site.

When required, hard copy proofs must be delivered to: Midsouth Healthcare Network, Attn: CHIO, 3401 Mallory Lane, Franklin, TN 37067.

No definite schedule for placement of orders can be predetermined; however, contractor must be prepared to accept orders immediately after award.

The following schedules begin the workday after notification of the availability of task order and furnished material; the workday after notification will be the first workday of the schedule.

First Order With Proofs and Prior to Production Construction Samples:

- Contractor must complete production and distribution within nine (9) workdays of receipt of notification of availability of task order and furnished material.
- No specific date is set for submission of proofs. Proofs must be submitted as soon as possible to allow for revised proofs if contractor's errors are judged serious enough to require them.
- Prior to production construction samples must be submitted with the proofs.
- Proofs will be withheld no more than three (3) workdays from their receipt at the ordering agency until corrections/changes/"O.K. to Print" are provided via email. (The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.) (NOTE: Hard copy proofs will not be returned to the contractor.)
- The Government will approve, conditionally approve, or disapprove the construction samples within three (3) workdays of the receipt thereof.
- All proof/construction sample and transit times are included in the 9-workday schedule.

Balance of Orders:

- Contractor must complete production and distribution within five (5) workdays of receipt of notification of availability of task order and furnished material.

The ship/deliver date indicated on the task order/print order is the date products ordered for mailing f.o.b. contractor's city must be delivered to the post office.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with the order or shortly thereafter. In the event such information is not received in due time, the contractor will not be relieved of any responsibility in meeting the shipping schedule because of failure to request such information.

For compliance reporting purposes, the contractor must notify the U.S. Government Publishing Office of the date of shipment or delivery. Upon completion of each order, contractor must contact the Shared Support Services Compliance Section via email at compliance@gpo.gov or via telephone at (202) 512- 0520. Personnel receiving the email or call will be unable to respond to questions of a technical nature or transfer any inquiries.

REPORTING: On same day as mailing for each task order, the contractor shall provide a production report. At a minimum, the report is to include, but is not limited to, the following:

- Print order number
- Date of report
- Number of PDF files received
- Number of letters mailed
- Date letters were mailed
- List of letters not mailed.
- Reason for not mailing

Contractor must provide these reports as a Microsoft Excel file. Reports are to be provided via email to the ordering agency personnel as specified after award.

SECTION 3. - DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices offered in the "SCHEDULE OF PRICES" to the following units of production which are the estimated requirements to produce one (1) year's production under this contract. These units do not constitute, nor are they to be construed as, a guarantee of the volume of work which may be ordered for a like period of time.

The following item designations correspond to those listed in the "SCHEDULE OF PRICES."

I.	(a)	25
	(b)	1
II.	(a)	48
	(b)	7,500
III.		1,500
IV.		1,500

SECTION 4. - SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city.

Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications.

Bidder must make an entry in each of the spaces provided. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids may be declared non-responsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government.

Bids submitted with NB (No Bid), NA (Not Applicable), or blank spaces for an item may be declared non-responsive.

The Contracting Officer reserves the right to reject any offer that contains prices for individual items of production (whether or not such items are included in the DETERMINATION OF AWARD) that are inconsistent or unrealistic in regard to other prices in the same offer or to GPO prices for the same operation if such action would be in the best interest of the Government.

All invoices submitted to the GPO shall be based on the most economical method of production.

Fractional parts of 1,000 will be prorated at the per-1,000 rate.

Contractor's billing invoices must be itemized in accordance with the line items in the "SCHEDULE OF PRICES."

I. PROOFS AND PRIOR TO PRODUCTION CONSTRUCTION SAMPLES:

(a) Letters: Digital one-off proof ..... per page .....$_____

(b) Envelopes: Prior to production construction samples .....per order .....$_____

II. PRINTING AND BINDING: Prices offered shall include the cost of all required materials and operations (including reports and paper for the letters) for the printing and binding of the products listed in accordance with these specifications.

(a) *Makeready/setup charge ..... per print order .....$_____

*Contractor will be allowed only one (1) makeready/setup charge per print order. This combined charge shall include all materials and operations necessary to makeready and/or setup the contractor's equipment for all files transmitted for each order. Invoices submitted with more than one (1) makeready/setup charge per print order will be disallowed.

(b) Letters:
Printing in black ink, including binding .....per 1,000 printed pages .....$_____

_____
(Initials)

III. ADDITIONAL OPERATIONS:

Envelopes (including paper) ..... per 1,000 envelopes .....$_____

IV. GATHERING, INSERTING, AND MAILING: Prices offered must include the cost of all required materials and operations necessary for the mailing of the letters including cost of gathering leaves in proper sequence; folding to required size in accordance with these specifications; insertion into envelope; and, mailing in accordance with these specifications.

Mailers .....per 1,000 complete mailers .....$_____

_____
(Initials)

SHIPMENT(S): Shipments will be made from: City _____, State _____

The city(ies) indicated above will be used for evaluation of transportation charges when shipment f.o.b. contractor's city is specified. If no shipping point is indicated above, it will be deemed that the bidder has selected the city and state shown below in the address block, and the bid will be evaluated and the contract awarded on that basis. If shipment is not made from evaluation point, the contractor will be responsible for any additional shipping costs incurred.

DISCOUNTS: Discounts are offered for payment as follows: _____ Percent, _____calendar days. See Article 12 "Discounts" of Solicitation Provisions in GPO Contract Terms (Publication 310.2).

AMENDMENT(S): Bidder hereby acknowledges amendment(s) number(ed) _____

BID ACCEPTANCE PERIOD: In compliance with the above, the undersigned agree, if this bid is accepted within_____ calendar days (90 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated points(s), in exact accordance with specifications. *Failure to provide a 90-day bid acceptance period may result in expiration of the bid prior to award.*

BIDDER'S NAME AND SIGNATURE: Unless specific written exception is taken, the bidder, by signing and submitting a bid, agrees with and accepts responsibility for all certifications and representations as required by the solicitation and GPO Contract Terms – Publication 310.2. When responding by email, fill out and return one copy of all pages in "SECTION 4. – SCHEDULE OF PRICES," including initialing/signing where indicated. Valid electronic signatures will be accepted in accordance with the Uniform Electronic Transactions Act, §2. Electronic signatures must be verifiable of the person authorized by the company to sign bids. *Failure to sign the signature block below may result in the bid being declared non-responsive.*

Bidder _____
(Contractor Name) (GPO Contractor's Code)

_____
(Street Address)

_____
(City – State – Zip Code)

By _____
(Printed Name, Signature, and Title of Person Authorized to Sign this Bid) (Date)

_____
(Person to be Contacted) (Telephone Number)

_____
(Email) (Fax Number)

THIS SECTION FOR GPO USE ONLY

Certified by: _____ Date: _____ Contracting Officer: _____ Date: _____
(Initials) (Initials)

DEPARTMENT OF VETERANS AFFAIRS
Bristol Outpatient Clinic
2426 Lee Highway, Suite 200
Bristol, VA 24202

BLINKIN A ZZTEST
100 MANIKAN LN
ELIZABETHTON, TENNESSEE 37643

AUG 22, 2025

Dear BLINKIN A ZZTEST,

I would like to update you on your test results:

PROSTATE SPECIFIC ANTIGEN
The PSA test measures the level of prostate specific antigen in your blood. PSA is an enzyme that is produced by the prostate gland. In general, 0-4 is considered the normal range for PSA.

Test Name	Reference Range	Your Result
PSA	0.0 to 4.0	____

LIPID PROFILE
High cholesterol and triglycerides (lipids) are risk factors for heart disease. Your cholesterol should fall between 140 and 200, and your triglyceride level should fall between 25 and 149. HDL is the "good" cholesterol and should ideally be greater than 40. LDL is the "bad" cholesterol and optimal levels should be less than 100 (near optimal is between 100 and 129).

Test Name	Reference Range	Your Result
CHOLESTEROL	140 - 200	
TRIGLYCERIDE	25 - 149	
Direct HDL	low: < 40	____
Direct LDL	0 - 99	____

FERRITIN
These tests measure the amount of iron in your blood and measure your body's ability to use iron. They can be used to show if you are anemic.

Test Name	Reference Range	Your Result
IRON	65.0 - 175.0	
TIBC	250.0 - 450.0	
FERRITIN-male	21.8 - 274.7	____

HEMOGLOBIN and HEMATOCRIT
These tests show if you have any blood disorders: Hemoglobin and Hematocrit are measures of the red blood cells in the blood that carry oxygen. WBC (white blood count) is a measure of the number of white cells in the blood that fight infection. Platelets are clear cell fragments in the blood that control bleeding and clotting.

Test Name	Reference Range	Your Result
HEMOGLOBIN-male	13.6 - 17.3	15.5 (12/13/24 13:24)
-female	11.8 - 15.5	
HEMATOCRIT-male	39.5 - 51.7	46.2 (12/13/24 13:24)
-female	35.3 - 45.5	
WBC	4.8 - 10.5	12.8 (12/13/24 13:24)
PLATELETS	166 - 383	320 (12/13/24 13:24)

VITAMIN B12: No data available

FOLATE: No data available

PLAN
I have reviewed your lab results and they are normal. I look forward to seeing you at your next visit.

Future Appointments -

No future appointments

Sincerely,

KELLY L LOGUE

Sample Lab Results Letter

Tennessee Valley Healthcare System
1310 24th Avenue South
Nashville, TN 37212

ELBERT C JR ZZTEST
2203 MCKINLEYRD
JOHNSON CITY, TENNESSEE 37604

Dear Veteran: ELBERT C JR ZZTEST
Thank you for choosing the Tennessee Valley Healthcare System as your health care provider. Below are your Jun 04 2025 test results. For any questions, please contact your health care team by calling the VA Call Center at 1-800--876-7093 or send a secure message.

TEST NAME	RESULT	UNITS	REF. RANGE
POTASSIUM*	3.8	mmol/L	3.6 - 5.2
DIGOXIN*	<0.15 L	ng/mL	.9 - 2.0
APTT*	41.5 H	seconds	22.1 - 35.8

Sincerely

BRYCE J PROSPER, MSW
LEAD PROGRAM ANALYST

Appendix A: Department of Veteran Affairs Information Security Rules of Behavior for Organizational Users

1. COVERAGE

a. Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) provides the specific responsibilities and expected behavior for organizational users and non-organizational users of VA systems and VA information as required by 0MB Circular A-130, Appendix III, paragraph 3a(2)(a) and VA Handbook 6500, *Managing Information Security Risk: VA Information Security Program.*

b. Organizational users are identified as VA employees, contractors, researchers, students, volunteers, and representatives of Federal, state, local or tribal agencies not representing a Veteran or claimant

c. Non-organizational users are identified as all information system users other than VA users explicitly categorized as organizational users. These include individuals with a Veteran /claimant power of attorney. Change Management Agents at the local facility are responsible for on-boarding power of attorney/private attorneys

d. VA Information Security ROB does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA's information or information systems. The VA Information Security ROB provides the minimal rules with which individual users must comply. Authorized users are required to go beyond stated rules using "due diligence" and the highest ethical standards

2. COMPLIANCE

a. Non-compliance with VA ROB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include restricting access, suspension of access privileges, reprimand, demotion and suspension from work. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may result in criminal sanctions.

b. Unauthorized accessing, uploading, downloading, changing, circumventing, or deleting of information on VA systems; unauthorized modifying VA systems, denying or granting access to VA systems; using VA resources for unauthorized use on VA systems; or otherwise misusing VA systems or resources is strictly prohibited.

c. VA Information Security Rules of Behavior (ROB) does not create any other right or benefit, substantive or procedural, enforceable by law, by a party in litigation with the U.S.Government.

3. ACKNOLEDGEMENT

a. VA Information Security ROB must be signed before access is provided to VA information systems or VA information. The VA ROB must be signed annually by all users of VA information systems or VA information. This signature indicates agreement to adhere to the VA ROB. Refusal to sign VA Information Security ROB will result in denied access to VA information systems or VA information. Any refusal to sign the VA Information Security ROB may have an adverse impact on employment with VA.

_____
Initials

b. The ROB may be signed in hard copy or electronically. If signed using the hard copy method, the user should initial and date each page and provide the information requested under Acknowledgement and Acceptance For Other Federal Government Agency users, documentation of a signed ROB will be provided to the VA requesting official.

4. INFORMATION SECURITY RULES OF BEHAVIOR

Access and Use of VA Information Systems

I Will:

- Comply with all federal VA information security, privacy, and records management policies. SOURCE: PM-1
- Have NO expectation of privacy in any records that I create or in my activities while accessing or using VA information systems. SOURCE: AC-8
- Use only VA-approved devices, systems, software, services, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. SOURCE: AC-6
- Follow established procedures for requesting access to any VA computer system and for notifying my VA supervisor or designee when the access is no longer needed. SOURCE: AC- 2
- Only use my access to VA computer systems and/or records for officially authorized and assigned duties. SOURCE: AC-6
- Log out of all information systems at the end of each workday. SOURCE: AC-11
- Log off or lock any VA computer or console before walking away. SOURCE: AC-11
- Only use other Federal government information systems as expressly authorized by the terms of those systems; personal use is prohibited. SOURCE: AC-20
- Only use VA-approved solutions for connecting non-VA-owned systems to VA's network. SOURCE: AC-20

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data. SOURCE: AC-6
- Engage in any activity that is prohibited by VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. SOURCE: AC-8
- Have a VA network connection and a non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any device at the same time unless the dual connection is explicitly authorized. SOURCE: AC-17 (k)
- Host, set up, administer, or operate any type of Internet server or wireless access point on any VA network unless explicitly authorized by my Information System Owner (ISO) SOURCE: AC-18

Protection of Computing Resources

I Will:

- Secure mobile devices and portable storage devices (e.g., laptops, Universal Serial Bus (USB) flash drives, smartphones, tablets, personal digital assistants (PDA)). SOURCE: AC-19

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee. SOURCE: MP-4
- Attempt to override, circumvent, alter or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff. SOURCE: CM-3

Electronic Data Protection

I Will:

- Only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA. SOURCE: SI-3
- Safeguard VA mobile devices and portable storage devices containing VA information, at work and remotely, using FIPS 140-2 validated encryption (or its successor) unless it is not technically possible. This includes laptops, flash drives, and other removable storage devices and storage media (e.g., Compact Discs (CD), Digital Video Discs (DVD)). SOURCE: SC-13
- Only use devices encrypted with FIPS 140-2 (or its successor) validated encryption. VA owned and approved storage devices/media must use VA's approved configuration and security control requirements. SOURCE: SC-28
- Use VA e-mail in the performance of my duties when issued a VA email account. SOURCE: SC-8
- Obtain approval prior to public dissemination of VA information via e- mail as appropriate. SOURCE: SC-8

I Will Not:

- Transmit VA sensitive information via wireless technologies unless the connection uses FIPS 140- 2 (or its successor) validated encryption. SOURCE: AC- 18
- Auto-forward e-mail messages to addresses outside the VA network. SOURCE: SC-8
- Download software from the Internet, or other public available sources, offered as free trials, shareware; or other unlicensed software to a VA- owned system. SOURCE: CM-11
- Disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store or use VA information. SOURCE: CM- 10

_____
Initials

Teleworking and Remote Access

I Will:

- Keep government furnished equipment (GFE) and VA information safe, secure, and separated from my personal property and information, regardless of work location. I will protect GFE from theft, loss, destruction, misuse, and emerging threats. SOURCE: AC-17
- Obtain approval prior to using remote access capabilities to connect non-GFE equipment to VA's network while within the VA facility. SOURCE: AC-17
- Notify my VA supervisor or designee prior to any international travel with a GFE mobile device (e.g. laptop, PDA) and upon return, including potentially issuing a specifically configured device for international travel and/or inspecting the device or reimaging the hard drive upon return. SOURCE: AC-17
- Safeguard VA sensitive information, in any format, device, system and/or software in remote locations (e.g., at home and during travel). SOURCE: AC-17
- Provide authorized OIT personnel access to inspect the remote location pursuant to an approved telework agreement that includes access to VA sensitive information. SOURCE: AC-17
- Protect information about remote access mechanisms from unauthorized use and disclosure. SOURCE: AC-17
- Exercise a higher level of awareness in protecting GFE mobile devices when traveling internationally as laws and individual rights vary by country and threats against Federal employee devices may be heightened. SOURCE: AC-19

I Will Not:

- Access non-public VA information technology resources from publicly- available IT computers, such as remotely connecting to the internal VA network from computers in a public library. SOURCE: AC-17
- Access VA's internal network from any foreign country designated as such unless approved by my VA supervisor, ISO, local CIO, and Information System Owner. SOURCE: AC-17

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames, and complete any additional role-based security training required based on my role and responsibilities. SOURCE: AT-3
- Understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. SOURCE: AU-1
- Have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon demand. SOURCE: MA-2
- Permit only those authorized by OIT to perform maintenance on IT components, including installation or removal of hardware or software. SOURCE: MA-5
- Sign specific or unique ROBs as required for access or use of specific VA systems. I may be required to comply with a non-VA entity's ROB to conduct VA business. While using their system, I must comply with their ROB. SOURCE: PL-4

_____
Initials

Sensitive Information

I Will:

- Ensure that all printed material containing VA sensitive information is physically secured when not in use (e.g., locked cabinet, locked door). SOURCE: MP-4
- Only provide access to sensitive information to those who have a need- to-know for their professional duties, including only posting sensitive information to web-based collaboration tools restricted to those who have a need-to-know and when proper safeguards are in place for sensitive information. SOURCE: UL-2
- Recognize that access to certain databases has the potential to cause great risk to VA, its customers and employees due to the number and/or sensitivity of the records being accessed. I will act accordingly to ensure the confidentiality and security of these data commensurate with this increased potential risk. SOURCE: UL-2
- Obtain approval from my supervisor to use, process, transport, transmit, download, print or store electronic VA sensitive information remotely (outside of VA owned or managed facilities (e.g. medical centers, community based outpatient clinics (CBOC), or regional offices)). SOURCE: UL-2
- Protect VA sensitive information from unauthorized disclosure, use, modification, or destruction, and will use encryption products approved and provided by VA to protect sensitive data. SOURCE: SC-13
- Transmit individually identifiable information via fax only when no other reasonable means exist, and when someone is at the machine to receive the transmission or the receiving machine is in a secure location. SOURCE: SC-8
- Encrypt email, including attachments, which contain VA sensitive information. I will not encrypt email that does not include VA sensitive information or any email excluded from the encryption requirement SOURCE: SC-8
- Protect Sensitive Personal Information (SPI) aggregated in lists, databases, or logbooks, and will include only the minimum necessary SPI to perform a legitimate business function. SOURCE: SC-28
- Ensure fax transmissions are sent to the appropriate destination. This includes double checking the fax number, confirming delivery, using a fax cover sheet with the required notification message included. SOURCE: SC-8

I Will Not:

- Disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia without appropriate legal authority. I understand unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals. SOURCE IP-1
- Allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and authorized in advance by my VA supervisor, ISO, and Information System Owner, local CIO, or designee. SOURCE: AC-20
- Make any unauthorized disclosure of any VA sensitive information through any means of communication including, but not limited to, e-mail, instant messaging, online chat, and web bulletin boards or logs. SOURCE: SC-8

_____
Initials

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. SOURCE: IA-5 (1)
- Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure. SOURCE: IA-5 (h)

I Will Not:

- Store my passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption, and I am the only person who can decrypt the file. I will not hardcode credentials into scripts or programs. SOURCE: IA-5 (1) (c).

Incident Reporting

I Will:

- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) to my VA supervisor or designee immediately upon suspicion. SOURCE: IR-6

5. ACKNOWLEDGEMENT AND ACCEPTANCE

a. I acknowledge that I have received a copy of these Rules of Behavior VA information Security Rules of Behavior
b. I understand, accept and agree to comply with all terms and conditions of VA Information Security rules of Behavior

_____	_____
Print or type your full name	Signature Date
_____	_____
Office Phone	Position Title