U.S. GOVERNMENT PUBLISHING OFFICE
Government Publishing & Print Procurement

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Veterans "High Risk Flag" (HRF) Mailings

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

Department of Veterans Affairs

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning May 1, 2026 and ending April 30, 2027, 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 April 07, 2026 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.***

BIDDERS, PLEASE NOTE: These specifications have been ***extensively*** revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding.

Abstracts of contract prices are available at: https://www.gpo.gov/how-to-work-with-us/vendors/contract-pricing.

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. For information of a technical nature, contact Thomas Ferguson at (312) 353-5783 or email tferguson@gpo.gov

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. 1-18) and GPO Contract Terms, Quality Assurance Through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (revised September 2019).

Contract Terms, Forms and Standards information for contractors can be found on the GPO website at http://www.gpo.gov/how-to-work-with-us/vendors/programs-for-vendors. The Contract Terms publication noted above can be downloaded at http://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/qatap.pdf.

DOING BUSINESS WITH GPO: Contractors wishing to do business with the GPO are referred to the GPO web site http://www.gpo.gov/how-to-work-with-us/vendors/programs-for-vendors, where one can register as a GPO contractor using the '**GPO Publish information'** link in accordance with the furnished instructions on this page.

PREDOMINANT PRODUCTION FUNCTION: The predominant production function is printing and mailing. Bidders who must subcontract this operation will be determined to be non-responsible for award. Subcontracting is allowed for manufacturing of the envelopes only.

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

Product Quality Levels:
(a) Printing Attributes – Level III.
(b) Finishing 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	Approved Priors/ Average type dimension per publication
P-10. Process Color Match	Approved Priors/ Approved Proofs

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.

ADDITIONAL PREAWARD SURVEY REQUIREMENTS: Any contractor being considered for award of this program must submit the following detailed plans during the preaward survey (due diligence) process, prior to award of this contract. These proposed plans are subject to review and approval by the Government, and award will not be made prior to approval of same.

The contractor MUST NOT provide this information with their submitted bid, but must instead provide this information only upon request from the GPO contract administrator.

All requested materials and documentation must be provided within 2 workdays of request.

Production Plan: The contractor will be required to provide documentation to demonstrate how orders placed against this program will be produced. Information required must include, but is not limited to, an equipment list, breakdown of production steps and required labor, cost breakdowns, subcontractor information, sample invoice, shippers to be utilized, etc.
a. A listing of all production equipment and equipment capacities to be utilized on this contract.
b. The production capacity currently being utilized on this equipment.
c. The capacity that is available for managing and producing the volume of work products identified within this contract.
d. If new equipment is to be utilized, the documentation of the purchase order, source, delivery schedule and installation dates are required.

Security Control Plan: The contractor will be required to provide documentation to demonstrate compliance with the "Security and Privacy" section of these specifications. The contractor shall provide a security plan that addresses all aspects of physical and logical data file handling, processing and transfer, including publication and all associated mail handling as required. The security plan will address employee requirements for security training, background investigations, and credit checks. The security plan will address inventory controls, network security, visitor controls and applicable miscellaneous aspects of production. The security plan shall meet or exceed the mandated VA security requirements and be approved by a designated VA Information Security Officer and the Privacy Officer.

The contractor shall review the security plan at least quarterly and update it as soon as changes are indicated. The security plan will be maintained throughout the life of the contract. After acceptance of the security plan, the contractor shall inform the VA representative in writing, within seven (7) calendar days of changes made to the document.

See Attachment B: In addition to the above, the contractor is also required to complete the Contractor Security Control Assessment (Attachment B) annually and keep a copy with the Security Control Plan.

BAA: The contractor shall enter into a Business Associate Agreement (BAA), see below.
The proposed Security Control Plan must address the following:

Materials – The way that all accountable materials will be handled throughout all phases of production. This plan shall also include the method of disposal of all production waste materials in accordance with VA directive 6371 and the NIST publication 800-88.

Disposal of Waste Materials – The contractor is required to demonstrate how all waste materials used in the production of sensitive VA records will be definitively destroyed (ex. 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 appropriate 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.

If the contractor selects shredding as a means of disposal, it is preferred that a cross cut shredder be used. If a strip shredder is used, the strips must not exceed one-quarter inch. The contractor must provide the location and method planned to dispose of the material. The plan must include the names of all contract officials responsible for the plan and describe their duties in relationship to the waste material plan.

Production Area – The contractor must provide a secure area(s) for the processing and storage of data for the mailer items, either a separate facility dedicated to this product, or a walled-in limited access area within the contractor's existing facility. Access to the area(s) shall be limited to security-trained employees involved in the production of the postcards and mailers.

Part of the Security Control Plan shall include a floor plan detailing the area(s) to be used, showing existing walls, equipment to be used, and the printing and finishing locations.

Quality Control Plan: The contractor shall provide and maintain, within his own organization, an independent quality assurance organization of sufficient size and expertise to monitor the operations performed, and inspect the products of each operation to a degree and extent that will ensure the Government's quality assurance, inspection, and acceptance provisions are met. The contractor shall perform, or have performed, the process controls, inspections and tests required to substantiate that the products provided under this contract conform to the specifications and contract requirements. The contractor shall describe in detail their quality control/quality assurance plan describing how, when, and by whom the plans will be performed.

The plan must provide for periodic samplings to be taken during the production run, a control system that will detect defective, missing, or mutilated pieces, and the actions to be taken by the contractor when defective/missing/mutilated pieces are discovered. These actions must be consistent with the requirements found in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987, (Rev. 1-18)) and any updates thereafter. A recovery system is required to replace all defective, missing, or mutilated pieces. This control system may use a unique sequential number to aid in the recovery program which has to be maintained in order to recover any missing or damaged pieces. These pieces must be reprinted and 100% accountability must be maintained throughout the run. The contractor must ensure that there are no missing or duplicated pieces.

The plan must include examples and a detailed description of all quality control samples and their corresponding inspection reports or logs the contractor will keep to document the quality control inspections performed on each run. The plan must provide for a complete audit trail (i.e., it must be possible to locate any piece of mail at any time from the point it leaves the press, up to and including the point at which the mail is delivered to a USPS facility). An explanation of the contractor's sequential numbering system is required to understand the audit trail required for each and every piece.

Note: The Government will not, as a routine matter, request that the contractor produce individual pieces in transit within the plant, however, the contractor must demonstrate that they have an audit trail established that has the ability to comply with this type of request if and when the need arises.
The quality control plan must also include examples of the documentation and a detailed description of the random samples that document all of the contractor's activities. Furthermore, the plan must include the names of all quality assurance officials and describe their duties in relationship to the quality control plan. The plan must include a detailed description of the number and types of inspections that will be performed as well as the records maintained documenting these activities.

The quality control plan must account for the number of pieces mailed for each order, including days when no pieces are mailed.

The Government will periodically verify that the contractor is complying with the approved quality control plan through on-site examinations and/or requiring copies of the contractor's quality assurance records and quality assurance random copies.

See Attachment A: Contractor Rules of Behavior. The contractor will be bound by these requirements upon award.

Quality Control Sample Plan: The plan must provide a description of how the contractor will create quality control samples for periodic samplings to be taken during the production run and provide for backup and rerunning in the event of an unsatisfactory sample. The plan shall contain control systems that will detect defective, missing, or mutilated pieces.

The plan should include the sampling interval the contractor intends to utilize. The contractor will be required to create a quality control sample from each file, to be drawn from the production stream. Mailers samples should be in unsealed envelopes with contents inserted. Mailer number and file date must be indicated on each sample. The contractor must maintain samples as indicated in the contract specifications.

The plan shall detail the actions to be taken by the contractor when defective/missing/mutilated items are discovered. These actions must be consistent with the requirements found in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987, (Rev. 1-18)) or any updates thereafter.

Verification of Production and Mailing Plan: Contractor will be responsible for validating the integrity of every item produced in all phases of printing, packaging, and mailing and to ensure all mailpieces were correctly entered into the United States Postal System.

Mailpiece Integrity shall be defined as follows: Each mailpiece shall include all components (and only those components) intended for the designated recipient as contained in the print files received from VA.

The contractor is responsible for providing the automated print integrity control systems and processes required to prevent the commingling of mailer items intended for different recipients into a completed package. The contractor's printing process must have automated systems that include coding & scanning technology capable of –

1. Validating the count of items in a set.
2. Validating the sequence of items in a set.
3. Validating the sequence of sets in a production batch.
4. Interrupting production if variances are detected.

Mailing integrity shall be defined as follows: All records received from the VA that are designated for printing were printed, inserted (if applicable) and entered correctly into the U.S. Postal System.
The contractor is responsible for providing the automated inserted mailpiece tracking/reporting systems and processes required to validate that 100% of all records received from VA which are designated for printing were printed, inserted (if applicable), and mailed correctly. The contractor's inserting equipment must have automated systems that include coding and scanning technology capable of –

1. Reconciling letter counts and quantity counts from VA provided files to print order control totals provided by VA; reporting variances.
2. Uniquely identifying each Product Types within a print order.
3. Unique identifier to be scanned after insertion to ensure all products are present and accounted for.
4. Tracking and reporting all products produced and mailed within a print order at the Product Type level.
5. Identifying and reporting all missing products that were lost or spoiled during production within a print order.

6. Generating a new production file for all missing products.
7. Tracking and reporting all products that were reproduced and mailed within a print order at the Product Type level.
8. Reconciling the total of all products produced and mailed within a print order to the control totals provided by VA; reporting all variances.
9. Reconciling the total of all products mailed to mailing totals contained on Postal Entry Forms within a print order; reporting all variances.
10. Generating a final automated summary report which provides information that all mail pieces have been scanned, after insertion, verifying that all pieces for each mail package and file date are accounted for after contents are inserted, and event information on any spoiled or missing pieces verifying that they were scanned and accounted for. A copy of the summary report must be submitted with the matching GPO 712 form(s).

The contractor must generate an automated audit report when necessary showing the tracking of all products throughout all phases of production for each mailpiece. This audit report will contain all information identified above for each phase of printing, packaging, and mailing.

All product tracking/reporting data must be retained in electronic form for 120 calendar days after mailing, and must be made available to VA for auditing of contractor performance upon request. The contractor must maintain quality control samples, inspection reports, and records for a period of no less than 120 calendar days subsequent to the date of the check tendered for final payment by the GPO. The Government will periodically verify that the contractor is complying with the approved quality control plan through on-site examinations and/or requesting copies of the contractor's quality assurance records and quality assurance random copies.

Unique Identification Number Plan: Unique identifying numbers will be used to track each individual product, thereby providing 100% accountability. This enables the contractor to track each product through completion of the project. The contractor may create their own sequence number and run date to facilitate their presorting and inserting process but must maintain the original Unique ID (UID) for Management Information (MI) reporting.

Recovery System: A recovery system will be required to ensure all defective, missing, or mutilated pieces detected are identified, reprinted, and replaced. The contractor's recovery system must use unique sequential alpha/numeric identifiers assigned to each piece (including quality control samples) to aid in the recovery and replacement of any defective/missing/mutilated pieces, and must be capable of tracking and/or locating any individual piece of mail from the time it leaves the press, up to and including when it is off-loaded to the USPS facility. An explanation of the contractor's sequential numbering system is required to understand the audit trail required for each and every piece.

Note: The Government will not, as a routine matter, request that the contractor produce individual pieces in transit within the plant, however, the contractor must demonstrate they will have an audit trail established that has the ability to comply with this type of request if and when the need arises.

Material Handling and Inventory Control: This plan should explain in detail how the following materials will be handled: incoming raw materials; work-in-progress materials; quality control inspection materials; USPS inspection materials; and all outgoing materials cleared for USPS pickup/delivery.

Personnel Plan: This plan should include a description of the training programs employees will be given to familiarize them with the requirements of this program. If employees have current and adequate security clearances, please notate.
Postage Plan: Contractor must provide a postage cost breakout during the certification. The VA will pay the postage and furnish the permit information to the contractor. The mail class will be First Class Mail rate.

VA Business Associate Agreement: During the Preaward Survey, the contractor being considered for award will receive a PDF file of the VA Business Associate Agreement and must sign and return.

Contractors who are unable to provide the above documentation within 2 workdays may be declared non-responsible.

POST-AWARD REQUIREMENTS:

After award, the contractor may be required to have a post-award phone conference call with Government personnel from the VA and/or GPO, and additionally will be required to produce various proofs and samples for approval prior to beginning production of the first GPO Form 2511 Print Order.

Actual print production begins upon completion of these certifications.

Required post-award implementation and certification of VA security requirements (shown below) must be completed within 10 workdays after Date of Award, or completed by another documented VA-approved date.

- All applicable contractor employees must successfully complete VA Cyber Security Awareness training and annual refresher training as required.
- Contractor shall provide to the VA points of contact and the GPO contract administrator a copy of the training certificates produced at the completion of each training session, for each applicable employee within ten (10) workdays of notification of contract award and annually thereafter, as required.
- All applicable contractor employees must successfully complete any additional cyber security or privacy training, as required.

GOVERNMENT IN PLANT INSPECTIONS: The Government reserves the right to have Government representative(s) inspect any operation, including the security controls and privacy practices implemented by the contractor under this contract at the start of production, and/or at any time during production. The Government may conduct an inspection with 10 workdays notice, or on short notice, or unannounced, in the event of a security incident or at any other time. The contractor's full cooperation is required.

SECURITY AND PRIVACY REQUIREMENTS:

Confidentiality of Information: Information regarding any individual is of a confidential nature and may be used only for the purposes of producing the requirements of this contract. All materials containing confidential information, including but not exclusive to Government furnished data, imaged forms, and scrap, must be handled so that information does not have any unauthorized use. All scrap generated with any information regarding any individual person must be shredded, incinerated, otherwise destroyed beyond recognition. Any media (files, disks, etc.) produced by the VA and sent to the contractor MUST be returned to the VA upon completion of the specific order. Contractor must return this material via an overnight delivery service to prevent theft or accidental use.

All contractors and contractor personnel shall be subject to the Federal laws, regulations, standards and VA Directives and Handbooks, regarding information system security as delineated in this contract. Contractors must follow policies and procedures outlined in VA Directive 6500, Information Security Program and its handbooks to ensure appropriate security controls are in place.

Protection of Confidential Information:

(a) The contractor shall restrict access to all confidential information obtained from the Department of Veterans Affairs in the performance of this contract to those employees and officials who need it to perform the contract. Employees and officials who need access to confidential information for performance of the contract will be determined at the Post-Award Conference between the Contracting Officer and the responsible contractor representative.
(b) The contractor shall process all confidential information obtained from VA in the performance of this contract under the immediate supervision and control of authorized personnel, and in a manner that will protect the confidentiality of the records in such a way that unauthorized persons cannot retrieve any such records.
(c) The contractor shall inform all personnel with access to the confidential information obtained from VA in the performance of this contract of the confidential nature of the information and the safeguards required to protect this information from improper disclosure.
(d) For knowingly disclosing information in violation of the Privacy Act, the contractor and the contractor employees may be subject to the criminal penalties as set forth in 5 U.S.C Section 552a (i)(1), which is made applicable to contractors by 5 U.S.C. 552a (m)(1) to the same extent as employees of the VA. For knowingly disclosing confidential information as described in section 1106 of the Social Security Act (42 U.S.C. 1306), the contractor and contractor's employees may also be subject to the criminal penalties as set forth in that provision.
(e) The contractor shall assure that each contractor employee with access to confidential information knows the prescribed rules of conduct, and that each contractor employee is aware that he/she may be subject to criminal penalties for violations of the Privacy Act.
(f) All confidential information obtained from VA for use in the performance of this contract shall, at all times, be stored in an area that is physically safe from unauthorized access.
(g) The Government reserves the right to conduct on-site visits to review the contractor's documentation and in-house procedures for protection of confidential information.

VA Information Custodial Requirements:

1. Information made available to the contractor by VA for the performance and/or administration of this contract or information developed by the contractor in performance and/or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the Contracting Officer. This clause expressly limits the contractor's rights to use data as described in Rights in Data - General, Federal Acquisition Regulation (FAR) 52.227-14(d) (1).
2. Information generated by a contractor as a part of the contractor's normal business operations, such as medical records created in the course of providing treatment, is subject to a review by the Office of General Counsel (OGC) to determine if the information is the property of VA and subject to VA policy. If the information is determined by OGC to not be the property of VA, the restrictions required for VA information will not apply.
3. VA information will NOT be commingled with any other data on the contractor's information systems/media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. VA also reserves the right to conduct IT resource inspections to ensure data separation and on-site inspection of information destruction/media sanitization procedures to ensure they are in compliance with VA policy requirements.
4. Prior to termination or completion of this contract, the contractor will not destroy information received from VA or gathered or created by the contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a contractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, and applicable VA Records Control Schedules. These Directives are available at: http://www1.va.gov/vapubs/.

5. The contractor will receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. Applicable Federal information security regulations include all Federal Information Processing Standards (FIPS) and Special Publications (SP) issued by the National Institute of Standards and Technology (NIST). If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies, including FIPS or SP, in this contract.
6. Contractors collecting, storing, or disseminating personal identifiable information (PII) or protected health information (PHI) data must conform to all pertinent regulations, laws, and VA directives related to privacy. Contractors must provide access for VA privacy reviews and assessments and provide appropriate documentation as directed.
Note: Personally identifiable information is defined as any information which can be used to distinguish or trace and individual's identity, such as their name, social security number, Veterans identification number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
7. The contractor shall not make copies of VA information except as necessary to perform the terms of the agreement or to preserve electronic information stored on contractor electronic storage media for restoration in case any electronic equipment or data used by the contractor needs to be restored to an operating state.
8. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for the Government to terminate the contract for default or terminate for cause under the GPO Printing Procurement Regulations (GPO Publication 305.3).
9. If a Veterans Health Administration (VHA) contract is terminated for cause, the associated business associate agreement (BAA) will also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01 Business Associates.
10. Contractor will store, transport or transmit VA sensitive information in an encrypted form, using a VA-approved encryption application that meets the requirements of NIST's FIPS 140-2 standard.
11. The contractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA directives are available on the VA directives Web site at http://www1.va.gov/vapubs/.
12. 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 other situations: (1) in response to a qualifying order of a court of competent jurisdiction; or, (2) with VA's prior written approval. The contractor will refer all requests for, demands for production of, or inquiries about, VA information and information systems to VA for response.
13. Notwithstanding the provision above, the contractor shall NOT release medical quality assurance records protected by 38 U.S.C. 5705 or records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus protected under 38 U.S.C. 7332 under any circumstances, including in response to a court order, and shall immediately refer such court orders or other inquiries to VA for response.
14. The contractor will not use technologies banned in VA in meeting the requirements of the contract (e.g., Bluetooth enabled devices).

Security Incident Investigation:

1. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss of, or damage to VA assets or sensitive information, or an action that breaches VA security procedures. The contractor shall immediately notify the GPO and VA representative and simultaneously, the designated ISO/Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor has access.

2. To the extent known by the contractor, the contractor's notice to GPO and VA will identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information/assets were placed at risk or compromised), and any other information that the contractor considers relevant.
3. The contractor will simultaneously report the incident to the appropriate law enforcement entity(ies) of jurisdiction, including the GPO and VA Offices of the Inspector General and Security and Law Enforcement, in instances of theft or break-in or other criminal activity. The contractor and its employees will 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 will 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.
4. To the extent practicable, the contractor shall mitigate any harmful effects on individuals whose VA Information was accessed or disclosed in a security incident. In the event of a data breach with respect to any VA sensitive information processed or maintained by the contractor under the contract, the contractor is responsible for liquidated damages to be paid to VA.
5. If a security incident (as described above) occurs at the contractor's facility, the actual damage to the Government for the incident will be difficult or impossible to determine. Therefore, pursuant to the "Liquidated Damages" clause (GPO Contract Terms, Publication 310.2), in lieu of actual damages, the contractor shall pay to the Government as fixed, agreed, and liquidated damages for each record, or part thereof, involved in the incident, the amount set forth below. Liquidated damages will be assessed against that record, or part thereof, which has been compromised. Liquidated damages will not be assessed against that record or part thereof that has not been compromised. The amount of damages will be computed at $37.50 per record, or part thereof, compromised; provided that the minimum amount of liquidated damages shall not be less than $5.00 for the entire order and not more than 50% of the total value of the entire order. The total damages assessed against a contractor shall in no case exceed 50% of the total value of the entire order. Payment of an order will be withheld until evidence of steps taken to prevent the recurrence of a security incident has been taken.

Security Training:

1. All contractor employees requiring access to VA sensitive information shall complete the following before being granted access to VA sensitive information:
- Sign and acknowledge understanding of, and responsibilities for, compliance with the Contractor Rules of Behavior (Attachment A) relating to access to VA information and information systems;
- Successfully complete VA Cyber Security Awareness training and annual refresher training as required including return of completion certificates for the Government record;
- Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

2. The contractor shall provide to the GPO contract and VA points of contact a copy of the training certificates for each applicable employee (for the required training as stated above) within ten (10) workdays of notification of contract award and annually thereafter, as required. These online courses are located at the following web site: https://www.tms.va.gov.
3. Failure to complete this mandatory training within the timeframe required will be grounds for suspension or termination of all physical and/or electronic access privileges and removal from work on the contract until such time as the training is completed.

SAFEGUARD MEASURES FOR PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA: VA policies require documentation that PII data sent to contractor remains secure while projects are in progress and is eventually destroyed in such a way that it cannot be retrieved or restored after being deleted from the contractor's hard drives/systems.

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. For "PRIVACY ACT" purposes, "agency" refers to the VA.

(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

(3) 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.

CRIMINAL SANCTIONS: 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) which is made applicable to contractors by 5 U.S.C. 552a (m)(1), provides that any officer or employee of an agency, who by virtue of his/her employment of official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established there under, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $10,000.00.

PROTECTED HEALTH INFORMATION: "Protected Health Information" or "PHI" shall have the same meaning as described at 45 C.F.R. § 160.103. "Protected Health Information" and "PHI" as used in this Agreement include "Electronic Protected Health Information" and "EPHI." For the purposes of this Agreement and unless otherwise provided, the term shall also refer to PHI that the Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity or receives from Covered Entity or another Business Associate.

QUALITY CONTROL (QC): Production items should be produced in accordance with all established quality control checks and procedures to ensure that the imaged forms and letters are accurate. Any quality control checks and requirements established such as the use of review sheets, unique mark, tray checks, insertion checks and envelope sealing must be adhered to at all times.

Copies of Imaging, Mailing Receipts and Status Reports: Contractor is required to provide copies of all pages of all mailing receipts (GPO Form 712, PS Form 3600-R or equivalents) to the VA. These reports should also include the actual date mailed, quantity deemed unqualified for mailing with a separate description of problems making them un-mailable, and quantities of statements requiring reprinting. Additionally, any other pertinent information should be provided or as requested by the Government.

Contractor is responsible for reviewing all factors which could affect mail acceptance including ensuring that:

- The Post Office location for the mailings is familiar with Government permit imprint mail.
- Specific requirements for mail using a Government permit imprint are met, including requirements which may affect the wording of the permit imprint and/or requirements that require additional paperwork and account set up prior to the mailing being accepted by the Postal Service.
- Problems are resolved sufficiently before the start of mailing such that delays in mailing do not occur.

QUALITY CONTROL SAMPLE PULLS: The contractor will be required to pull one (1) test sample for every 1,000 mailers. For orders placed with a quantity of less than 1,000 copies, contractor must pull 1 random test sample. These samples are a duplicate of an addressee, and the contractor is responsible for ensuring that the actual mailing for that addressee mails.

For Quality Control Sample Pulls, the mailers must be complete – all required items printed/imaged, bound/constructed, and inserted in accordance with these specifications.

Quality Control Sample Pulls for an order must be signed and dated by the contractor operator and placed in the contractor's secure archive for one (1) year from the order delivery date. These samples do not deliver to the VA unless requested.

Upon request from the Government, Quality Control Sample Pulls must be shipped within one (1) workday via overnight shipping at the contractor's expense, to the requesting Government point of contact.

The Quality Control Sample Pulls are in addition to the total quantity ordered. No additional charges will be allowed.

OPTION TO EXTEND THE CONTRACT TERM: 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 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 periodic pricing revision.

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 **May 1, 2026 and ending April 30, 2027**, 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 January 31, 2026 for a May 1, 2026 contract, 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.

If the Government exercises an option, the extended contract shall be considered to include this economic price adjustment clause.

ASSIGNMENT OF JACKETS, PURCHASE 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 "print order" for each job placed with the contractor. The print order, when issued, 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 print orders by the Government. Orders may be issued under the contract from **May 1, 2026 and ending April 30, 2027**, plus for such additional period(s) as the contract is extended. All 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 print order. A print order shall be "issued" for purposes of the contract, when it is either deposited in the U.S. Postal Service mail or otherwise 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. 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 are to be completed by the contractor within the time specified in the order. 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.

When production covered by this contract is required before the dates specified under this contract, and the contractor will not accept the accelerated schedule, the Government may procure this requirement from another source for that accelerated schedule.

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.

OPTIONS: Whenever an option is indicated in the specifications, it is the Government's option, not the contractor's, unless it is specifically stated otherwise.

PAYMENT: Submit invoices for payment within 10 workdays of complete mailing for each order via the GPO fax gateway (if no samples are required) utilizing the GPO barcode coversheet program application is the most efficient method of invoicing. 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.

NOTE: Use of the Secure Server Workspace (SFTP): Print orders, artwork, distribution lists and all furnished materials will be provided via the Secure Server Workspace. When required, PDF soft proofs must be sent via the Secure Server Workspace. All reports, postal receipts, etc. must be archived on the Secure Server Workspace. Use of this workspace must be supplemented by timely email notifications from the contractor to the VA points of contact below, or other contacts as designated by the VA through email, notation on the GPO Form 2511 Print Order, or other means, in order to document the upload or download of all critical documents.

U.S. Department of Veterans Affairs
Brian Mano, Production Manager
Email: brian.mano@va.gov

U.S. Department of Veterans Affairs
Project Manager
Email: MaryGrace.Lauver@va.gov

Courtesy Copy of Invoice: Contractor is required to upload a copy of each print order invoice voucher (including postal statements) to the VA secure online workspace within two workdays of fax submission to GPO FMCE.

RECEIPTS FOR DELIVERY: Contractor must furnish their own receipts for delivery, and postal statements for mailing, as suitable. These receipts must include the GPO jacket, program and print order numbers, total quantity shipped and/or delivered, number of cartons and quantity per carton; date delivery made; and signature of the Government agent accepting delivery. Original copy of these receipts or other acceptable proof must accompany the contractor's voucher for payment.

NOTE: Number of pieces listed on the postal receipts MUST match the number of recipients in the supplied distribution lists, with an accounting for undeliverables, etc.

CONTRACTOR'S INVOICE FOR PAYMENT MUST BE ITEMIZED IN ACCORDANCE WITH THE SCHEDULE OF PRICES AND ISSUED TO GPO WITHIN 10 WORKDAYS AFTER COMPLETION OF EACH INDIVIDUAL PRINT ORDER. FAILURE TO ITEMIZE IN ACCORDANCE WITH THE SCHEDULE OF PRICES OR ISSUED TO GPO WITHIN 10 WORKDAYS AFTER ORDER COMPLETION MAY RESULT IN DELAYED PAYMENT.

SECTION 2. - SPECIFICATIONS

SCOPE: These specifications cover the secure (PII/PHI) production of envelopes and notecards, requiring such operations as pickup of furnished materials, electronic prepress, proofs, address list processing, printing in black and two additional colors (dark red and dark blue), variable data personalization, trimming, envelope construction, collating, inserting, addressing, mailing and sample delivery.

TITLE: Veterans "High Risk Flag" (HRF) Mailings.

Although this is an option year contract, all estimates, averages, etc. are based on one year's production.

FREQUENCY OF ORDERS: It is anticipated that approximately 56 orders will be placed per year, 1 per week.

QUANTITY: Approximately 300 to 6,000 mailed sets per order. In a base year, it is anticipated that the average order will be for 2,700 mailers. The first few months will be for the lower end quantity as the program starts up.

Each set will include:

- An average of 8 different versions of Personalized Notecards per order. There is a total of 8 possible personalized notecard artwork template versions. In the furnished mail list for each order, each addressee will have a template version indicated. Additionally, each personalized notecard will have 1 variable data field for the addressee name.
- One (1) Outer Light Green Envelope, static printing, totaling an average of 2,700 copies per order.

All quantities mailed are +/- NONE after list processing. It is the contractor's responsibility to produce any additional quantities required for samples and spoilage at no additional charge to the Government.

TRIM SIZE AND NUMBER OF PAGES:

Personalized Notecard: 7 x 5" – prints face only.
Outer Light Green Envelope: A7 – 7-1/4 x 5-1/4" – Construction at contractor's option, prints face only.

GOVERNMENT TO FURNISH:

VA reserves the right to send data files via encrypted email.

Artwork: High resolution artwork files will be sent by the VA agency by Azure RMS encrypted email. Electronic media will be generated using Adobe Creative Suite and Microsoft Office applications. At the Government's option, files may be provided via other electronic method such as via email, downloadable link, etc. Artwork files for static text matter/artwork will be furnished immediately after contract award and are to be held for re-use throughout the term of the contract. In the event that any of the static text matter/artwork changes, new files will be furnished to the contractor.

The static text matter and artwork for all items will be furnished as Adobe Acrobat print ready PDF files. In some instances MS Word files may be supplied. All fonts will be embedded. The contractor is cautioned that the furnished fonts are the property of the Government and/or its contractors. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract.

A black and white VA logo will be provided for use on the envelopes in the upper left corner.

Distribution Lists: One to four times per month, ASCII or MS Excel file(s) will be supplied for distribution lists and will include the variable data and template information for each addressee. These files will be sent to the contractor by Azure RMS encrypted email. At the Government's option, lists may be provided via other electronic method such as via downloadable link, etc.

Print Order (GPO Form 2511): Print orders will generally be sent via email. At the Government's option, print orders may be furnished as a hard copy, a faxed copy, or by SFTP. Contractor must be able to accept via email.

DATA RIGHTS: All data and materials furnished and/or produced in the performance of this contract shall be the sole property of the Government. The contractor agrees not to assert rights or to establish any claim to such data/materials in whole or in part in any manner or form, or to authorize others to do so, without prior written consent of the Contracting Officer.

FONTS: Any fonts provided are the property of the ordering VA and are provided for use on this contract only. Using the furnished fonts on any job other than the one for which the fonts were submitted violates copyright law. All fonts should be eliminated from contractor's archive immediately after completion of the production run.

CONTRACTOR TO FURNISH: All materials and operations, other than those listed under "Government to Furnish," necessary to produce the product(s) in accordance with these specifications.

EXAMINATION OF FURNISHED MATERIAL: Contractor must immediately upon receipt perform a basic check (preflight) of the furnished media and publishing files to assure accurate output of the required reproduction image. Additional charges or extensions in schedule will not be allowed due to contractor's failure to thoroughly examine material.

ELECTRONIC PREPRESS: Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure accurate output of the required reproduction image. Any errors, media damage or data corruption that might interfere with proper file imaging must be reported to the VA and Thomas Ferguson at 312-353-5783 in sufficient time to comply with the shipping schedule. 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. Contractor must maintain the latest version of all programs and operating systems used in this contract as well as maintain backwards-compatibility.

Contractor may occasionally be required to perform minor prepress adjustments such as adjusting pages in furnished electronic files as needed to ensure adequate margins, converting colors, adding bleeds, and/or perform other similar prepress adjustments. In order to make these adjustments, contractor may be required to revise either supplied PDFs or native files. Prior to making revisions, the contractor shall copy the furnished files and make all changes to the copy.

These required electronic prepress operations must be provided at no additional charge to the Government.

TYPESETTING: It is anticipated that the VA will provide all artwork, including any adjustments for author alterations. Occasionally, orders may require the contractor to perform type or content corrections to furnished artwork, such as correcting misspellings. The contractor must match specified or existing typefaces and sizes as ordered. Acceptance of any similar alternate typeface is at the discretion of the VA.

Separate charges will be allowed for these operations in the "SCHEDULE OF PRICES."

DIGITAL DELIVERABLES: The VA must always have returned to them the most up-to-date versions of all files related to this program, in the same format as furnished, with additional formats provided as suitable or as requested. If changes are made to the artwork and/or the list files that are furnished (during the proofing stage, at upon request, or per the specifications), the contractor must upload to the secure online workspace, or at the

Government's option, create a CD with all changes incorporated therein for return to the VA after completion of the order.

PROOFS AND ADDRESSING SAMPLES:

AT THE START OF THE CONTRACT

Hard copy proofs, addressing samples and Prior to Production samples are required at the start of the contract, to the address in "Distribution". Proofs, etc. must allow the VA to confirm how the variable data will look (display the name merge, etc.)

Include a paper stock sample of each item at the start of the contract. VA approved paper stocks must be maintained throughout the contract, or must be re-approved if contractor desires revisions.

Include up to 24 addressing samples at the start of the contract. Any contractor-applied codes or barcodes must be included for VA review and approval. Approved addressing format/style must be maintained throughout the contract, or must be re-approved if contractor desires revisions.

A copy of the GPO Print Order Form 2511 and a return air bill must be furnished with all deliveries of hard copy proofs, addressing samples and/or Prior to Production samples. Email tracking information after shipping any of these items to brian.mano@va.gov Contractor must confirm receipt of these items by calling: Brian Mano at the VA at Office: 202-461-5002 or Mobile: 202-430-0011.

Up to 5 sets of hard copy proofs will be ordered. One set will be retained by the VA and the other set will be returned to the contractor for use as the standard throughout the contract. The addressing samples and Prior to Production samples will be retained by the VA for their record, they will not be returned.

Returned proofs will be withheld not more than 5 workdays. Contractor must not proceed without receipt of an "OK to Print/Mail". See "Schedule" for additional information.

For all artwork versions (8 Personalized Notecard versions and Outer Green Envelope):

Hard Copy Proofs (at start of contract): (at the customer option):

Up to 5 sets of digital color content proofs. Direct to plate must be used to produce the final product with a minimum resolution of 2400 x 2400 dpi. Proofs must be created using the same Raster Image Processor (RIP) that will be used to produce the product. Proofs shall be collated with all elements in proper position (not pasted up), imaged face and back, trimmed and folded to the finished size of the product, as applicable.

Up to 5 sets of inkjet proofs that are G7 profiled and use pigment-based inks. A proofing RIP that provides an option for high quality color matching (such as Device Links Technology and/or ICC Profiles Technology), and meets or exceeds industry tolerance to ISO 12647-7 Standard for Graphic Technology (as of 3/19/09, and future amendments) must be utilized plus GRACoL 2006 Coated #1 specifications (CGATS TR006) must be achieved. Output must be a minimum of 720 x 720 dpi on a GRACoL or SWOP certified proofing media. Proofs must contain the following color control strip to be evaluated for accuracy: IDEAlliance ISO 12647-7 Control Strip 2009 or 2013(i1).

Proofs must contain color control bars (such as Brunner, GATF, GRETAG, or RIT) for each color of ink on the sheet. Control bars must be placed parallel to the press's ink rollers and must show areas consisting of minimum 1/8 x 1/8" solid color patches; tint patches of 25, 50 and 75%; dot gain scale; and gray balance patches for process color (if applicable). These areas must be repeated consecutively across the sheet.

The make and model number of the proofing system utilized shall be furnished with the proofs. These proofs must contain all elements, be in press configuration, and indicate margins. Proofs will be used for color match on press. Direct to plate must be used to produce the final product with a minimum of 2400 x 2400 dpi.

Addressing Samples (at start of contract):

To ensure that address formatting is correct, including font size, style, etc., number of address lines, etc, the contractor will be required to furnish not less than 24 addressing samples from the first furnished distribution list, or a sample distribution list. At the contractor's option, addressing samples and Prior to Production samples may be combined.

Prior to Production Samples (at start of contract): (at the customers option):

Prior to the commencement of production of the contract production quantity, the contractor must submit not less than ten (10) printed construction samples of each item per set as ordered, utilizing a wide range of personalized notecard templates. Each sample must be constructed as specified using the form, materials, equipment, and methods of production, which will be used in producing the final product.

All samples shall be manufactured at the facilities in which the contract production quantities are to be manufactured. Samples will be inspected and tested and must comply with the specifications in all respects (construction, kind and quality of materials).

The container and accompanying documentation shall be marked "PRIOR TO PRODUCTION SAMPLES" and shall include the GPO jacket number, purchase order number, program number, and print order number.

Samples will be inspected and tested and must comply with the specifications as to kind and quality of materials. The samples must be submitted in sufficient time to allow Government testing of the samples and production and shipment in accordance with the shipping schedule.

The Government will approve, conditionally approve, or disapprove the samples within 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 therefor.

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 the procedures as indicated in 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 sample 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 included in the contract price for the production quantity.

The contractor must not proceed prior to written receipt of an "OK to Print/Mail."

AT THE START OF PRODUCTION

After proof approval at the start of the contract, usually NO hard proofs will be required for each mailing. The contractor will be responsible for performing all necessary proofreading to insure that the final product is in conformity with the copy/data submitted. The contractor will be responsible for reporting immediately to the VA and GPO if there are any discrepancies or concerns with furnished materials.

For all print orders, PDF proofs will be ordered, usually as indicated on the GPO Form 2511 print order.

PDF proofs should be sent by Azure RMS encrypted email. The contractor must email all VA and GPO points of contact a notification of the upload. Contractor must confirm receipt of PDF proofs by calling: Brian Mano at the VA – Office: 202-461-5002 or Mobile: 202-430-0011 or by encrypted email.

PDF proofs, if ordered, will be withheld not more than 2 workdays. PDF proof approval will be made by the VA.

Contractor must not print prior to receipt of an "OK to Print/Mail".

Contractor to submit "Press Quality" PDF "soft" proofs (for content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proofs will be evaluated for text flow, image position, and color breaks. PDF proofs will not be used for color match.

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.

AUTHOR'S ALTERATIONS: Author's alterations (AA's) may occur occasionally during the proofing stage. At the Government's option, changes may be supplied by the VA or requested from the contractor. It is anticipated that most AA's will be supplied by the VA.

Author's alterations (AA's) proofs shall usually be digital color content PDF proofs. At the VA's option, hard copy proofs, addressing samples and/or Prior to Production samples may instead or additionally be ordered.

Author's alterations performed by the contractor will be charged at the regular contract rates for System Timework per the "SCHEDULE OF PRICES". Charges for making AA's will not be honored unless the invoice voucher that is submitted to GPO is supported by documentation and written approval by the VA of all changes. The contracting officer has the final determination related to any requested charges.

Contractor must not print prior to receipt of an "OK to Print/Mail".

STOCK: 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, and any amendments thereto.

Color of paper furnished shall be of a uniform shade. The GPO Contracting Officer reserves the right to reject any order printed on paper the color of which materially differs from JCP standards.

Personalized Notecard: JCP L23: White Offset Cover, Basis Weight 20 x 26", 100 lb.
Outer Light Green Envelope: JCP V20: LIGHT GREEN Writing Envelope, Basis Weight 17 x 22", 24-28 lb.

PRINTING, INKS AND MARGINS:

At contractor's option, the static-only products (products that will not require variable imaging at any time) may be produced via conventional offset or digital printing provided that Quality Level III standards are maintained. Final output must be a minimum of 150-line screen and at a minimum resolution of 2400 x 2400 x 1 dpi or 600 x 600 x 8 bit depth technology. Digital device must have a RIP that provides an option for high quality color matching such as Device Links Technology and/or ICC Profiles.

Personalized Notecard:

For products that contain variable data, contractor must print, merge templates and variable data image in a single pass.

Template Merge: There will be 8 base artwork versions of the personalized notecards. Each addressee, for each mailing, will have one of the 8 different templates indicated for that addressee in the furnished Excel file. When printing, the contractor must ensure that the correct base template is used, and additionally ensure that the variable data field below is correctly inserted for each addressee, see below.

Static Printing: The static information on the Personalized Notecards prints face only in black and two additional colors, dark red and dark blue

Variable Data Personalization: Each notecard has one (1) variable data field. Data files for the variable data personalized information will be furnished in an Excel file. The variable data field will be: "Recipient First Name".

Accuracy of Imaged Forms: A form must be produced for each data file. 100% of the records must be properly imaged and mailed. No improper forms may be distributed. No duplicate forms may be distributed. No damaged forms may be distributed. Contractor must guarantee 100% accuracy. Contractor must have a method for verifying that all records are correctly imaged and a plan for regenerating any that are un-imaged, incorrectly imaged, damaged, or destroyed. This must include methods for determining what records have been imaged to insure the imaging of all forms, tracking all forms, determining missing or damaged forms, insuring that damaged forms and test forms are not mailed, regenerating forms that are missing or damaged, and insuring that duplicate forms are not generated or mailed. Additionally, contractor must have a specific plan for guaranteeing that incorrectly imaged statements or duplicate statements, produced for whatever reason (tests, makeready, spoilage, etc.) are not mailed and are destroyed by a process that renders them unreadable, such as by shredding or incineration.

Damaged Forms: Contractor must maintain a record of all damaged imaged forms and a record of when these forms were regenerated. These records will be required to be provided to the VA upon request.

Secure Destroy: Contractor to use the USPS "Secure Destroy" feature to handle any mail pieces that are ultimately undeliverable even after all necessary presorts.

Outer Green Envelope: Prints face only before construction in black ink – VA seal (no return address) and permit block – type and line matter, must meet USPS requirements, and VA requirements for font, layout etc. VA seal artwork, will be furnished by the VA or contractor to pick up from their files. Permit number to be provided by the contractor. The envelope shall accept printing without feathering or penetrating to the reverse side.

Envelopes require a security tint printed on the inside (back - before construction) in black ink. 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.

INVENTORY: It is recommended that the contractor request a forecast from the VA on possible changes to artwork before printing large quantities of any item for inventory storage/future use.

Personalized Notecards: Because the personalized notecards are uniquely printed with each mailing and must be printed in a single pass, no inventory will accrue. If artwork is changed during the term of the contract, the contractor must comply with the new requirement, and produce new proofs for VA approval.

Envelopes: If copy is changed during the term of the contract, the contractor must comply with the new requirement, and cannot exhaust previous stock. The contractor must produce a new supply of envelopes using the current valid copy of the envelopes.

IDENTIFICATION MARKINGS: Identification markings such as register marks, ring folios, rubber stamped jacket numbers, commercial identification marks of any kind, etc., except GPO imprint, form number, and revision date, carried on copy or film, must not print on finished product.

BINDING OPERATIONS:

Personalized Notecard: Trim 4 sides.

Outer Green Envelope: Envelope construction is open side. Style of flap is at contractor's option. Side or diagonal seams construction is at contractor's option. Once the style and construction of the envelopes is approved by the VA, the furnished envelopes must stay the same throughout the contract. Flap must be fully gummed.

Personalized Notecard should be inserted into each addressed outer green envelope. Securely seal each envelope.

It is the contractor's responsibility to assure that the correct items are inserted into each envelope. Contractor must have quality control measures in place that ensure that the correct Personalized Notecard is inserted in the correct addressed Outer light green Envelope. After inserting, seal envelope securely. Any loosening of the seals prior to opening by the recipient may result in order rejection.

LIST PROCESSING, SORTING, ADDRESSING, ETC. IN ACCORDANCE WITH UNITED STATES POSTAL SERVICE (USPS) REGULATIONS:

Mail Rate: All mailed pieces must meet all USPS requirements and must mail at the Presorted First Class rate.

Addressing: All recipient addressing will be located on the face of the Outer Green Envelope. Address each Outer Green Envelope in black ink. Addressing must follow all postal regulations including those for typography/fonts, print quality, reflectance, barcode location, clear zones, etc. Inkjet or labels at contractor's option. All imaged addresses must be complete and include the recipient's name and complete mailing address. Addresses in the United States or as otherwise applicable, must have the zip + 4 barcode.

Furnished Distribution Lists: The vendor will be supplied Data files, which will require list processing and VA approval of cleaned list prior to printing.

List Processing: Contractor will be required to do all sorting and CASS Certification to obtain the maximum postage discount allowed by the USPS in accordance with appropriate USPS rules and regulations, including the USPS Domestic Mail Manual and Postal Bulletins in effect at the time of the mailing. Contractor will be required to run the furnished distribution lists for each order through the National Change of Address (NCOA) service database to verify addresses are NCOA certified. All related costs to perform these operations must be included in submitted bid pricing. No additional reimbursement will be authorized.

An output file containing the rejected names and addresses must be provided to the VA along with the reject code or some explanation for reason of rejection. The output containing the names and addresses of those records retained after NCOA cleaning (i.e. cleared for mailing) must be provided to VA. The contents of the processed address file must be approved/verified by VA before proceeding to printing. If international addresses are identified as bad addresses, they must be verification to ensure they are not excluded. To do this the output file must be uploaded to the VA secure server workspace along with an email notification, so that the VA can verify that the vendor has received the full contents of the address file.

Bad Addresses, Mailed Quantity and Secure Destroy: The contractor must provide to the VA a list of any addresses that NCOA and USPS deem undeliverable so that the VA can make a determination of further handling. Any mail that is deemed deliverable by USPS and mail software but is still refused or ultimately undelivered, the VA would like those pieces to be destroyed using the USPS “Secure Destroy” service. The VA will then require a listing of all mailpieces that were destroyed via “Secure Destroy.” Once the final adjusted quantity is known, contractor must forward the final quantity to the VA point of contact brian.mano@gpo.gov and cc to the GPO contract administrator at tferguson@gpo.gov The GPO Print Order Form 2511 must reflect the final mailed count, and the contractor’s submitted invoice must reflect the final mailed count as would match the submitted postal statements.

Non-USPS Postage (Invalids): It is anticipated that a small quantity of mailings may contain mailing addresses deemed invalid (unqualified) by the U.S. Postal Service (may not qualify for the imprint). Contractor must notify the VA of any such non-qualifying pieces. At the Government’s option, the contractor may be required to overnight these pieces to the VA at the contractor’s expense. Orders which result in mailings of less than 200 pieces or less than 50 pounds may require the contractor to apply the appropriate postage to each mailing. Contractor will be reimbursed for postage by submitting a properly completed Postal Service Certificate of Mailing with the invoice for billing.

Quality Control Codes: Contractor will be allowed to insert a matching code in the address block if desired. The matching code must not interfere with any other information or affect the piece being accepted by the Postal Service. The size of the matching code must be inconspicuous and in a smaller typeface than the other information. Matching codes, if used, must appear on proofs and addressing samples. Contractor must provide the information as to the type of code to be used and what it indicates.

Mailing Permit and Postage Account: The U.S. Department of Veterans Affairs will supply a USPS CRID and EPS account for the vendor to establish an appropriate mail permit. Contractor will mail using departmental mailing permit imprint through VA’s Centralized Account Processing System (CAPS). Contractor is responsible for establishing the CAPS account.

Postal Service Forms and Other Requirements: Contractor must generate all bag tags, tray labels, etc. and is required to do all bagging, traying, sorting, etc. for this class of mail and level of sortation. Contractor must generate and accurately complete all required Postal Service forms.

The contractor is cautioned that mailing permit imprint may be used only for the purpose of mailing material produced under this contract.

The contractor is responsible for all costs incurred in transporting the mailers to the U.S. Postal Service facility.

Certificate of Conformance: When using Permit Imprint Mail the contractor must complete the current version of GPO Form 712 - Certificate of Conformance, and the appropriate mailing statement or statements supplied by USPS. A fillable GPO Form 712 Certificate of Conformance can be found at https://www.gpo.gov/how-to-work-with-us/vendors/forms-and-standards.

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

Special carrier mailings maybe needed for International Mailing addresses. If identified as a location in which USPS mail is unreliable (not timely), a special carrier may be used by the local facility for their mail delivery if USPS is determined to not be timely on delivery. Agency may use their FedEx/UPS account in these situations or via require reimbursable contractor's delivery.

PACKING, LABELING AND MARKING: Proofs and samples must be packed suitably to ensure protection from contamination and damage resulting from handling, storage or shipping. Pack to protect corners. No loose items in cartons are permitted.

Inner Packaging: Include sufficient inner packaging in submitted price. Ensure sufficient inner packaging to ensure no damage occurs during shipping.

Any items damaged during production or shipping may be required to be re-fulfilled in an expedited manner, including expedited handling, expedited production, and expedited shipping.

Refer to Labeling and Marking Specifications (GPO Form 905). See GPO Contract Terms Booklet, Publication 310.2., and any updates thereto, for more information.

All expenses incidental to packing and labeling must be borne by the contractor.

GPO SAMPLES: Every GPO Form 2511 Print Order will require Compliance Samples to be sent to the GPO contract administrator for quality review. Mark package with Program number and Print Order number. GPO samples are to be shipped at the same time as the scheduled mailing and cannot be deducted from the total quantity ordered. It is not required that GPO samples be addressed. Un-addressed/un-sealed items are acceptable. Deliver sample copies by the most economical method. No additional charge will be allowed for these samples.

GPO "VERIFICATION OF DELIVERY": Contractor MUST email mailing/delivery verification information to compliance@gpo.gov WITHIN 24 HOURS OF DELIVERY. Enter Program and Print Order numbers in the subject line, and in the body of the message indicate the method of mailing/shipment and the delivery date. If a contract specifies a shipping method of f.o.b. contractor's city (at government's expense), enter the date of mailing/shipment. If a contract specifies f.o.b. destination (at contractor's expense), enter the date of delivery. If a contract specifies a combination of both methods, include all shipping and delivery dates. Failure to provide this information for each print order may result in delayed payment of invoices.

DISTRIBUTION:

Mailing of any order must NOT commence until "OK to Print/Mail" approval is given by the VA.

See "LIST PROCESSING, SORTING, ADDRESSING, ETC. IN ACCORDANCE WITH UNITED STATES POSTAL SERVICE (USPS) REGULATIONS" for additional information.

Mail f.o.b. contractor's city: Mailing using the agency's mailing permit (at Government's expense).

Approximate Mailing Address Breakdown:
Domestic destinations: 98%

HI/AK destinations: 1%
International destinations (country 1, country 2, country 3): 1%

Due to PII/PHI security requirements, a sample of a mailing list for this program will NOT be available for review during the Invitation for Bid process.

All expenses incidental to overnight delivery services, picking up and returning materials must be borne by the contractor.

NOTICE OF USPS CONTACT INFORMATION: Within 2 weeks prior to the first scheduled mailing date, the contractor must provide the VA with the name, address, phone number, fax number, and a contact person at the post office(s) where the mailing will be accepted. Email brian.mano@va.gov

DROP SHIPPING: If using drop shipping, Post Office locations must be identified during the preaward survey. Any changes after award must be approved by the VA and GPO.

USPS INFORMED DELIVERY SERVICES AND TRACKING: The agency intends to utilize USPS Informed Delivery services that are offered in connection with the agency's USPS CAPS/EPS account. Contractor may be required to provide serial number ranges to the agency and/or to the USPS in relation to this advanced delivery tracking and/or will be required to provide all other additional related types of account administration in support of the use of these services.

NOTIFICATION OF COMPLETION OF MAILING: Upon completion of each order, the contractor must complete the following two steps:

Within 1 workday: Upload the postage receipts, tracking numbers, and other finalized paperwork for each GPO Form 2511 Print Order to the SFTP server workspace for agency access. The print order number must be clearly indicated.

Within 1 workday: Email a notification to the VA agency point of contact brian.mano@va.gov (with cc to GPO contract administrator). The subject line of the email shall be "Distribution Notice for Program 2529-S, P.O. GXXXX, Jacket XXX-XXX, Print Order XXXXX." The notice must provide all applicable shipment tracking numbers and mailing information.

Deliver f.o.b. destination (at contractor's expense) via traceable means:

Deliver proofs, priors and other samples to up to 2 locations:

U.S. Department of Veterans Affairs
Office of Procurement, Acquisition and Logistics/Publication Services Division
Brian Mano, Production Manager
810 Vermont Ave NW
Room 744-A
Washington DC 20420
Office: 202-461-5002
Mobile: 202-430-0011
Email: brian.mano@va.gov

2 unsealed samples for each GPO Print Order Form 2511 to:
U.S. Government Publishing Office
Compliance Thomas Ferguson
9302 W 79th PL.
Schererville, IN 46375

RETURN OF GOVERNMENT FURNISHED MATERIALS: Upon completion of each order, any furnished materials must be packed separately and returned to the same address indicated for delivery of proofs in "DISTRIBUTION" unless otherwise indicated on the GPO Print Order Form 2511 or by the VA, and shall be marked with program number, print order number, jacket number and requisition number.

All expenses incidental to returning furnished materials 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 print order (GPO Form 2511).

NOTE: Use of the Azure RMS encrypted email: Print orders, artwork, distribution lists and all furnished materials will be provided via Azure RMS encrypted email. When required, PDF soft proofs must be sent via the Azure RMS encrypted email. All reports, postal receipts, etc. must be archived on Azure RMS encrypted email. Use of this workspace must be supplemented by timely email notifications from the contractor to all VA and GPO points of contact, in order to document the upload or download of all critical documents.

When required, hard copy proofs, addressing samples and/or Prior to Production samples must be delivered to and picked up from the address listed is "Distribution".

No definite schedule for notification of availability of furnished materials can be predetermined.

It is anticipated that the contractor will be required to send all proofs, samples etc. via an overnight delivery service. All such pickups or deliveries must be made at no additional charge to the Government.

The following schedule begins the workday after notification of the availability of print order and furnished material. The workday after notification will be the first workday of the schedule.

AT THE START OF THE CONTRACT:

Hard copy proofs, addressing samples and Prior to Production samples: Contractor to produce at the start of the contract, and additionally when ordered and/or upon changes to any item.

Upon receipt of artwork, hard copy proofs, addressing samples and Prior to Production samples will be required to be delivered to the VA **within 3 work days.**

VA will approve **within 2 work days.**

REGULAR ORDER PROCESSING:

List Processing: Upon receipt of each distribution list, the cleaned list and error reports will be required to be sent by encrypted email **within 2 work days.**

Upon receipt of approval of cleaned list, the VA will give the approval to Print/Mail **within 2 workdays.** No other proofs will usually be ordered.

If PDF or other proofs are ordered for any individual print order, the contractor will add 2 workdays to the schedule for production, and add the number of days of agency hold, which is anticipated to be 2 workdays.

Upon receipt of the "OK to Print/Mail", the contractor is required to complete all production, shipping and mailing **within 5 workdays.**

The specified date on the print order is the date that the order must be printed/mailed.

When author's alterations are made, the schedule will be extended by 1 additional workday.

No extension will be made when new proofs are required due to printer's errors.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with each 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.

VA BUSINESS ASSOCIATE AGREEMENT (BAA):
During the Preaward Survey, the contractor being considered for award will receive an updated PDF file of this Business Associate Agreement and must sign and return it to GPO within 2 workdays of receipt.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, VETERANS CRISIS LINE, AND [COMPANY TBD].

Purpose. The purpose of this Business Associate Agreement (Agreement) is to establish requirements for the Department of Veterans Affairs (VA), Veterans Health Administration (VHA), **<Insert Facility Name>** and **<Company/Organization>** in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI) under the terms and conditions specified below.

Scope. Under this Agreement and other applicable contracts or agreements, **<Company/Organization>** will provide **<BRIEFLY DESCRIBE SERVICES (i.e., medical device, transcription, publishing)>** services to, for, or on behalf of **<Insert Facility Name>**.

In order for **<Company/Organization>** to provide such services, **<Insert Facility Name>** will disclose PHI to **<Company/Organization>**, and **<Company/Organization>** will use or disclose PHI in accordance with this Agreement.

Definitions. Unless otherwise provided, the following terms used in this Agreement have the same meaning as defined by the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

"Business Associate" shall have the same meaning as described at 45 C.F.R. § 160.103. For the purposes of this Agreement, Business Associate shall refer to **<Company/Organization>**, including its employees, officers, or any other agents that create, receive, maintain, or transmit PHI as described below.

"Covered Entity" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Covered Entity shall refer to **<Insert Facility Name>**.

"Protected Health Information" or "PHI" shall have the same meaning as described at 45 C.F.R. § 160.103. "Protected Health Information" and "PHI" as used in this Agreement include "Electronic Protected Health Information" and "EPHI." For the purposes of this Agreement and unless otherwise provided, the term shall also refer to PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity or receives from Covered Entity or another Business Associate.

"Subcontractor" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Subcontractor shall refer to a contractor of any person or entity, other than Covered Entity, that creates, receives, maintains, or transmits PHI under the terms of this Agreement.

Terms and Conditions. Covered Entity and Business Associate agree as follows:

1. Ownership of PHI. PHI is and remains the property of Covered Entity as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate agreement is in place.

2. Use and Disclosure of PHI by Business Associate. Unless otherwise provided, Business Associate:

   A. May not use or disclose PHI other than as permitted or required by this Agreement, or in a manner that would violate the HIPAA Privacy Rule if done by Covered Entity, except that it may use or disclose PHI:

      (1) As required by law or to carry out its legal responsibilities;
      (2) For the proper management and administration of Business Associate; or
      (3) To provide Data Aggregation services relating to the health care operations of Covered Entity.

   B. Must use or disclose PHI in a manner that complies with Covered Entity's minimum necessary policies and procedures.

   C. May de-identify PHI created or received by Business Associate under this Agreement at the request of the Covered Entity, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

3. Obligations of Business Associate. In connection with any Use or Disclosure of PHI, Business Associate must:

   A. Consult with Covered Entity before using or disclosing PHI whenever Business Associate is uncertain whether the Use or Disclosure is authorized under this Agreement.

   B. Implement appropriate administrative, physical, and technical safeguards and controls to protect PHI and document applicable policies and procedures to prevent any Use or Disclosure of PHI other than as provided by this Agreement.

   C. Provide satisfactory assurances that PHI created or received by Business Associate under this Agreement is protected to the greatest extent feasible.

   D. Notify Covered Entity within twenty-four (24) hours of Business Associate's discovery of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Breach of PHI.

      (1) Any incident as described above will be treated as discovered as of the first day on which such event is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate.

      (2) Notification shall be sent to the **<Insert local VHA Privacy Officer's name(s) and email address(es)>** and to the VHA Health Information Access Office, Business Associate Program Manager by email at VHABAAIssues@va.gov**.**

      (3) Business Associate shall not notify individuals or the Department of Health and Human Services directly unless Business Associate is not acting as an agent of Covered Entity but in its capacity as a Covered Entity itself.

   E. Provide a written report to Covered Entity of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Breach of PHI, within ten (10) business days of the initial notification.

(1) The written report of an incident as described above will document the following:

(a) The identity of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, disclosed, modified, or destroyed;

(b) A description of what occurred, including the date of the incident and the date of the discovery of the incident (if known);

(c) A description of the types of secured or unsecured PHI that was involved;

(d) A description of what is being done to investigate the incident, to mitigate further harm to Individuals, and to protect against future incidents; and

(e) Any other information as required by 45 C.F.R. §§ 164.404(c) and 164.410.

(2) The written report shall be addressed to:

<Insert local VHA Privacy Officer's name(s) and facility address> and submitted by email to **<Insert local VHA Privacy Officer's email address(es)>** and to the VHA Health Information Access Office, Business Associate Program Manager at VHABAAIssues@va.gov**.**

F. To the greatest extent feasible, mitigate any harm due to a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate.

G. Use only contractors and Subcontractors that are physically located within a jurisdiction subject to the laws of the United States, and ensure that no contractor or Subcontractor maintains, processes, uses, or discloses PHI in any way that will remove the information from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing.

H. Enter into Business Associate Agreements with contractors and Subcontractors as appropriate under the HIPAA Rules and this Agreement. Business Associate:

(1) Must ensure that the terms of any Agreement between Business Associate and a contractor or Subcontractor are at least as restrictive as Business Associate Agreement between Business Associate and Covered Entity.

(2) Must ensure that contractors and Subcontractors agree to the same restrictions and conditions that apply to Business Associate and obtain satisfactory written assurances from them that they agree to those restrictions and conditions.

(3) May not amend any terms of such Agreement without Covered Entity's prior written approval.

I. Within five (5) business days of a written request from Covered Entity:

(1) Make available information for Covered Entity to respond to an Individual's request for access to PHI about him/her.

(2) Make available information for Covered Entity to respond to an Individual's request for amendment of PHI about him/her and, as determined by and under the direction of Covered Entity, incorporate any amendment to the PHI.

(3) Make available PHI for Covered Entity to respond to an Individual's request for an accounting of Disclosures of PHI about him/her.

J. Business Associate may not take any action concerning an individual's request for access, amendment, or accounting other than as instructed by Covered Entity.

K. To the extent Business Associate is required to carry out Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the provisions that apply to Covered Entity in the performance of such obligations.

L. Provide to the Secretary of Health and Human Services and to Covered Entity records related to Use or Disclosure of PHI, including its policies, procedures, and practices, for the purpose of determining Covered Entity's, Business Associate's, or a Subcontractor's compliance with the HIPAA Rules.

M. Upon completion or termination of the applicable contract(s) or agreement(s), return or destroy, as determined by and under the direction of Covered Entity, all PHI and other VA data created or received by Business Associate during the performance of the contract(s) or agreement(s). No such information will be retained by Business Associate unless retention is required by law or specifically permitted by Covered Entity. If return or destruction is not feasible, Business Associate shall continue to protect the PHI in accordance with the Agreement and use or disclose the information only for the purpose of making the return or destruction feasible, or as required by law or specifically permitted by Covered Entity. Business Associate shall provide written assurance that either all PHI has been returned or destroyed, or any information retained will be safeguarded and used and disclosed only as permitted under this paragraph.

N. Be liable to Covered Entity for civil or criminal penalties imposed on Covered Entity, in accordance with 45 C.F.R. §§ 164.402 and 164.410, and with the HITECH Act, 42 U.S.C. §§ 17931(b), 17934(c), for any violation of the HIPAA Rules or this Agreement by Business Associate.

4. Obligations of Covered Entity. Covered Entity agrees that it:

A. Will not request Business Associate to make any Use or Disclosure of PHI in a manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if made by Covered Entity, except as permitted under Section 2 of this Agreement.

B. Will promptly notify Business Associate in writing of any restrictions on Covered Entity's authority to use or disclose PHI that may limit Business Associate's Use or Disclosure of PHI or otherwise affect its ability to fulfill its obligations under this Agreement.

C. Has obtained or will obtain from Individuals any authorization necessary for Business Associate to fulfill its obligations under this Agreement.

D. Will promptly notify Business Associate in writing of any change in Covered Entity's Notice of Privacy Practices, or any modification or revocation of an Individual's authorization to use or disclose PHI, if such change or revocation may limit Business Associate's Use and Disclosure of PHI or otherwise affect its ability to perform its obligations under this Agreement.

5. Amendment. Business Associate and Covered Entity will take such action as is necessary to amend this Agreement for Covered Entity to comply with the requirements of the HIPAA Rules or other applicable law.

6. Termination.

A. Automatic Termination. This Agreement will automatically terminate upon completion of Business Associate's duties under all underlying Agreements or by termination of such underlying Agreements.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, at its discretion, upon review as provided by Section 9 of this Agreement.

C. Termination for Cause. In the event of a material breach by Business Associate, Covered Entity:

(1) Will provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Covered Entity, and;

(2) May terminate this Agreement and underlying contract(s) if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.

D. Effect of Termination. Termination of this Agreement will result in cessation of activities by Business Associate involving PHI under this Agreement.

E. Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate Agreement is in place.

7. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement confers any rights, remedies, obligations, or liabilities whatsoever upon any person or entity other than Covered Entity and Business Associate, including their respective successors or assigns.

8. Other Applicable Law. This Agreement does not abrogate any responsibilities of the parties under any other applicable law.

9. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date to determine the applicability and accuracy of the Agreement based on the circumstances that exist at the time of review.

10. Effective Date. This Agreement shall be effective on the last signature date below.

Department of Veterans Affairs **Veterans Health Administration** **<Insert Facility Name>**	**COMPANY/ORGANIZATION**
By: _____	**By:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

SECTION 3. - DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices 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.

The following item designations correspond to those listed in the “Schedule of Prices”.

		(1)	(2)	(3)
I.	(A)	56	1512	1512
	(B)	56	1512	1512
II.	(A)	2		
	(B)	2		
	(C)	56		
	(D)	2		
	(E)	2		

SECTION 4. - SCHEDULE OF PRICES

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

Bidder must make an entry in each of the spaces provided, Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications. Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids, may be declared nonresponsive.

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) or blank spaces for an item within the category that a bidder is bidding on may be declared nonresponsive.

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.

The contractor is cautioned not to perform any operation(s) or produce any product(s) for which a price has not been offered under the contract. Further, the contractor is not to accept print orders which are outside the scope of the contract. Any changes made to the print order MUST be confirmed in writing by the Contracting Officer, GPO. If such orders are placed, and no Modification is received from the GPO, the contractor is to notify GPO immediately. Failure to do so may result in nonpayment.

CONTRACTOR MUST INVOICE IN ACCORDANCE WITH SCHEDULE OF PRICES. FAILURE TO ITEMIZE IN ACCORDANCE WITH THE SCHEDULE OF PRICES MAY RESULT IN DELAYED PAYMENT.

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

Fractional parts of 100 will be prorated at the Per 100 rate.

I. COMPLETE PRODUCT (except for Item II. "PROOFS AND AUTHOR'S ALTERATIONS"): Prices shall include the cost of all required materials and operations, including but not limited to: printing, paper, trimming, envelope construction, and all packing/mailing material and operations, as necessary for the complete production, mailing and delivery of the items listed, in accordance with these specifications.

Regardless of the number of copies run, contractor will be allowed only one (1) "Makeready and/or Setup" charge for each template of 8 postcard versions and envelope item per order.

NOTE: VA will pay postage via a Government furnished permit.

I. COMPLETE PRODUCT: (Continued)

(A) Personalized Notecard:

(1) Makeready and/or Setup…… per template of 8 versions……...$_____

(2) Running …… per 100 copies of 8 versions.……..$_____

(3) Paper …… per 100 sheets of 8 versions…….$_____

(B) Outer Light Green Envelope:

(1) Makeready and/or Setup…… per item……$_____

(2) Running …… per 100 copies …….$_____

(3) Paper …… per 100 sheets ……..$_____

II. PROOFS AND AUTHOR'S ALTERATIONS: Any charge made under "System timework" must be supported by a statement outlining in detail the operation for which payment is claimed. In case of dispute, the Contracting Officer reserves the right to be the final judge as to the operations and/or number of hours chargeable.

(A) Digital color content proofs…….per each set …….$_____

(B) G7 profiled inkjet proofs……..….per each set ……..…….$_____

(C) PDF proofs……...per each set ……$_____

(D) System timework (AA's)……..per hour…….…….... $_____

(E) Prior to Production samples (10 copies per set) ..... per set .....$_____

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID) _____ (Initials)

LOCATION OF POST OFFICE: All mailing will be made from the _____,

Post Office located at Street Address_____.

City_____, State_____, Zip Code_____.

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 (60 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.

NOTE: Failure to provide a 60-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 State & 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)

****

THIS SECTION FOR GPO USE ONLY

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

****

COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID

MARCH 12, 2010 VA HANDBOOK 6500.6 APPENDIX D

CONTRACTOR RULES OF BEHAVIOR

This User Agreement contains rights and authorizations regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the Department of Veterans Affairs (VA). This User Agreement covers my access to all VA data whether electronic or hard copy ("Data"), VA information systems and resources ("Systems"), and VA sites ("Sites"). This User Agreement incorporates Rules of Behavior for using VA, and other information systems and resources under the contract.

1. GENERAL TERMS AND CONDITIONS FOR ALL ACTIONS AND ACTIVITIES UNDER THE CONTRACT:

a. I understand and agree that I have no reasonable expectation of privacy in accessing or using any VA, or other Federal Government information systems.

b. I consent to reviews and actions by the Office of Information & Technology (OI&T) staff designated and authorized by the VA Chief Information Officer (CIO) and to the VA OIG regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA. These actions may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing to all authorized OI&T, VA, and law enforcement personnel as directed by the VA CIO without my prior consent or notification.

c. I consent to reviews and actions by authorized VA systems administrators and Information Security Officers solely for protection of the VA infrastructure, including, but not limited to monitoring, recording, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized OI&T, VA, and law enforcement personnel.

d. I understand and accept that unauthorized attempts or acts to access, upload, change, or delete information on Federal Government systems; modify Federal government systems; deny access to Federal government systems; accrue resources for unauthorized use on Federal government systems; or otherwise misuse Federal government systems or resources are prohibited.

e. I understand that such unauthorized attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. This includes penalties for violations of Federal laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications).

f. I agree that OI&T staff, in the course of obtaining access to information or systems on my behalf for performance under the contract, may provide information about me including, but not limited to, appropriate unique personal identifiers such as date of birth and social security number to other system administrators, Information Security Officers (ISOs), or other authorized staff without further notifying me or obtaining additional written or verbal permission from me.

g. I understand I must comply with VA's security and data privacy directives and handbooks. I understand that copies of those directives and handbooks can be obtained from the Contracting Officer's Technical Representative (COTR). If the contractor believes the policies and guidance provided by the COTR is a material unilateral change to the contract, the contractor must elevate such concerns to the Contracting Officer for resolution.

h. I will report suspected or identified information security/privacy incidents to the COTR and to the local ISO or Privacy Officer as appropriate.

2. GENERAL RULES OF BEHAVIOR

a. Rules of Behavior are part of a comprehensive program to provide complete information security. These rules establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users must understand that taking personal responsibility for the security of their computer and the information it contains is an essential part of their job.

b. The following rules apply to all VA contractors. I agree to:

(1) Follow established procedures for requesting, accessing, and closing user accounts and access. I will not request or obtain access beyond what is normally granted to users or by what is outlined in the contract.

(2) Use only systems, software, databases, and data which I am authorized to use, including any copyright restrictions.

(3) I will not use other equipment (OE) (non-contractor owned) for the storage, transfer, or processing of VA sensitive information without a VA CIO approved waiver, unless it has been reviewed and approved by local management and is included in the language of the contract. If authorized to use OE IT equipment, I must ensure that the system meets all applicable 6500 Handbook requirements for OE.

(4) Not use my position of trust and access rights to exploit system controls or access information for any reason other than in the performance of the contract.

(5) Not attempt to override or disable security, technical, or management controls unless expressly permitted to do so as an explicit requirement under the contract or at the direction of the COTR or ISO. If I am allowed or required to have a local administrator account on a government-owned computer, that local administrative account does not

confer me unrestricted access or use, nor the authority to bypass security or other controls except as expressly permitted by the VA CIO or CIO's designee.

(6) Contractors' use of systems, information, or sites is strictly limited to fulfill the terms of the contract. I understand no personal use is authorized. I will only use other Federal government information systems as expressly authorized by the terms of those systems. I accept that the restrictions under ethics regulations and criminal law still apply.

(7) Grant access to systems and information only to those who have an official need to know.

(8) Protect passwords from access by other individuals.

(9) Create and change passwords in accordance with VA Handbook 6500 on systems and any devices protecting VA information as well as the rules of behavior and security settings for the particular system in question.

(10) Protect information and systems from unauthorized disclosure, use, modification, or destruction. I will only use encryption that is FIPS 140-2 validated to safeguard VA sensitive information, both safeguarding VA sensitive information in storage and in transit regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA.

(11) Follow VA Handbook 6500.1, *Electronic Media Sanitization* to protect VA information. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders.

(12) Ensure that the COTR has previously approved VA information for public dissemination, including e-mail communications outside of the VA as appropriate. I will not make any unauthorized disclosure of any VA sensitive information through the use of any means of communication including but not limited to e-mail, instant messaging, online chat, and web bulletin boards or logs.

(13) Not host, set up, administer, or run an Internet server related to my access to and use of any information assets or resources associated with my performance of services under the contract terms with the VA unless explicitly authorized under the contract or in writing by the COTR.

(14) Protect government property from theft, destruction, or misuse. I will follow VA directives and handbooks on handling Federal government IT equipment, information, and systems. I will not take VA sensitive information from the workplace without authorization from the COTR.

(15) Only use anti-virus software, antispyware, and firewall/intrusion detection software authorized by VA. I will contact the COTR for policies and guidance on complying with this requirement and will follow the COTR's orders regarding my access to and use of any information assets or resources associated with my performance of services under the contract terms with VA.

(16) Not disable or degrade the standard anti-virus software, antispyware, and/or firewall/intrusion detection software on the computer I use to access and use information assets or resources associated with my performance of services under the contract terms with VA. I will report anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages to the COTR.

(17) Understand that restoration of service of any VA system is a concern of all users of the system.

(18) Complete required information security and privacy training, and complete required training for the particular systems to which I require access.

3. ADDITIONAL CONDITIONS FOR USE OF NON- VA INFORMATION TECHNOLOGY RESOURCES

a. When required to complete work under the contract, I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA approved remote access software and services.

b. Remote access to non-public VA information technology resources is prohibited from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library.

c. I will not have both a VA network line and any kind of non-VA network line including a wireless network card, modem with phone line, or other network device physically connected to my computer at the same time, unless the dual connection is explicitly authorized by the COTR.

d. I understand that I may not obviate or evade my responsibility to adhere to VA security requirements by subcontracting any work under any given contract or agreement with VA, and that any subcontractor(s) I engage shall likewise be bound by the same security requirements and penalties for violating the same.

4. STATEMENT ON LITIGATION
This User Agreement does not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

MARCH 12, 2010 VA HANDBOOK 6500.6 APPENDIX D

5. ACKNOWLEDGEMENT AND ACCEPTANCE

I acknowledge receipt of this User Agreement. I understand and accept all terms and conditions of this User Agreement, and I will comply with the terms and conditions of this agreement and any additional VA warning banners, directives, handbooks, notices, or directions regarding access to or use of information systems or information. The terms and conditions of this document do not supersede the terms and conditions of the signatory's employer and VA.

Print or type your full name	Signature
Last 4 digits of SSN	Date
Office Phone	Position Title
Contractor's Company Name	

Please complete and return the original signed document to the COTR within the timeframe stated in the terms of the contract.

Contractor Security Control Assessment (CSCA)

Self-Assessment Questionnaire for Contract Service Providers

Version 1.2

May 15, 2009

VA INFORMATION PROTECTION

Document Change Control

Version	Release Date	Summary of Changes	Name
Version 0.1	March 13, 2009	First working draft submitted to CPO.	CPO
Version 0.2	March 13, 2009	Format and minor content changes	CPO
Version 0.3	March 16, 2009	Second working draft with incorporated CPO changes	CPO
Version 0.4	March 16, 2009	Third working draft with incorporated CPO changes	CPO
Version 0.5	March 18, 2009	Final working draft with incorporated CPO suggestions	CPO
Version 0.6	April 15, 2009	Incorpoation of CPO and VA staff combined suggestions	CPO
Version 1.0	May 5, 2009	Final draft document	CPO
Version 1.1	May 5, 2009	Updates made to NIST references in Appendix A	CPO
Version 1.2	May 15, 2009	Final Review for Release	FSS, OCS

Table of Contents

Executive Summary

The Department of Veterans Affairs (VA) must comply with the Federal Information Security Management Act (FISMA) and with Office of Management and Budget (OMB) direction to ensure oversight of contractors who access, maintain, store, or transmit Veterans' sensitive information. VA established the Contractor Security Control Assessment (CSCA) to assist in defining and evaluating information security control protection mechanisms and practices used to protect Veterans' sensitive information. All contractors and contract service providers must comply with the same information security requirements as VA is recommended to do the CSCA on an annual basis.

Purpose

The purpose of this document is to provide security guidance for contractors and contract service providers in remote locations or alternative work-sites who access, maintain, store, or transmit Veterans' sensitive information. This CSCA is a checklist built around the framework of the National Institute of Standards and Technology (NIST).

Per NIST Special Publication (SP) 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*:

> "The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data information devices."

Scope

The protection of Veterans' sensitive information is a critical and intricate part of the overall security awareness and health of the VA organization. This CSCA will assist VA in:

- Extending VA security mandates and education to affiliated contractor agencies;
- Maintaining a record of contractor agency compliance with VA-necessitated security regulations and polices that can be included in the contract file; and
- Strengthening and improving the process of securing Veterans' sensitive information on approved information devices. (An "information device" is any device used access, maintain, store, or transmit Veterans' sensitive information, such as a workstation, home computer, laptop, Blackberry, etc.)

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Attestation of Compliance

Please complete this Attestation of Compliance as a declaration of your compliance with the CSCA to protect Veterans' sensitive information.

Part 1. Person Completing This Document	
Contact Name:	Chris Sherbine
Title:	Security and Compliance Lead
Telephone:	(814) 239-8787 x1328
Business Address:	13710 Dunnings Hwy Claysburg, PA 16625
Email:	Chris.Sherbine@npcweb.com

Part 2. Contractor Organization Information	
Contact Name:	Frank Swalga
Title:	Government Contract Manager
Telephone:	(814) 239-8787 x1295
Business Address:	13710 Dunnings Hwy Claysburg, PA 16625
Email:	Frank.Swalga@npcweb.com

Part 2a. Relationships

Does your company have a relationship with one or more third-party service providers (e.g., gateways, web-hosting companies)? ☐ Yes ☑ No

Part 2b. Transaction Processing

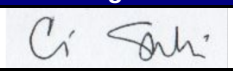
How is information exchanged with VA?: Information is exchanged with VA via SFTP.

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Part 3. CSCA Validation
☑ **Compliant**: All sections are complete and all questions are answered affirmatively, resulting in an overall **COMPLIANT** rating.
☐ **Non-Compliant**: Not all sections are complete and/or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating. **Target Date for Compliance**:

Part 3a. Confirmation of Compliant Status	
☑	CSCA was completed according to the instructions therein.
☑	All information within the above-referenced CSCA and in this Attestation fairly represent the results of my assessment.
☑	I have read the appropriate VA directives relative to information securityand understand that I must maintain full data security standards at all times.

Part 3b. Contracting Officer's Technical Representative (COTR) Acknowledgement	
	9/30/2022
Signature of Person Completing this Document	***Date***
Chip Gallaher	NPC, Inc.
Printed Name of Executive Officer	***Company***
Signature of Information Security Officer	***Date***

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Action Plan for Non-compliance

Please select the appropriate "Compliant" status for each requirement. If you answer "No" to any of the requirements, please complete the table below with the necessary steps to become compliant and the date on which you will be compliant.

VA CSCA	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (If Compliance Status is "No")
		YES	NO	
1	Install and maintain a firewall configuration.	☑	☐	
2	Host, operate, maintain, or use information devices.	☑	☐	
3	Use and regularly update antivirus software.	☑	☐	
4	Implement access controls.	☑	☐	
5	Conduct risk assessments.	☑	☐	
6	Institute information security protection.	☑	☐	
7	Privacy regulation for storage of Veterans' sensitive Information.	☑	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Self-Assessment Questionnaire

Requirement 1: Install and maintain a firewall configuration

VA requires the use of firewalls as a protection mechanism to ensure the confidentiality, integrity and availability of VA information.

Question	Response: (Select One)		Comment
	YES	NO	
1. Is a firewall used and installed on devices that will store, process, and maintain Veterans' sensitive information?	☑	☐	
2. If the firewall used is a hardware device, were the vendor supplied passwords removed? (hardware includes all wireless devices and routers) *Wireless environment defaults include, but are not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and simple network management protocol (SNMP) community strings*	Yes, all default settings are changed		
3. If the firewall used is a software product:	☐	☐	N/A
a) Is it set to download automatic updates?	☐	☐	N/A
b) Is the firewall software product installed on your PC (i.e, McAfee, Norton)?	☐	☐	N/A
c) Is there a personal firewall software installed on any mobile and/or employee-owned computers that have direct connectivity to the Internet (e.g., laptops used by employees) and are used to access the VA's network?	☑	☐	
4. Does the firewall monitor, restrict, and respond to inbound and outbound communications by sending notification alerts when a connection is attempted?	☑	☐	
5. Does the firewall provide email-scanning that monitors incoming and outgoing messages for viruses and security threats?	☑	☐	
6. Does the firewall prohibit direct public access between external networks and any information device component that stores Veterans' sensitive information (e.g., databases, logs, trace files)?	☑	☐	
7. Is there Wi-Fi protected access (WPA and WPA2) technology enabled for encryption and authentication when WPA-capable?	☑	☐	
8. Is there justification and documentation for any risky protocols allowed (e.g., file transfer protocol [FTP]), including the reason for the use of the protocol and security features implemented?	☑	☐	
9. Are you using Federal Information Processing Standard (FIPS) 140-2 validated encryption for storing and transferring VA sensitive information?	☑	☐	

Requirement 2: VA Information Hosting, Operation, Maintenance or Use

Question	Response: (Select One) YES	NO	Comment
1. Are you designing or developing a system or information device for or on behalf of VA?	☑	☐	
2. Are you hosting, operating, maintaining, or using an information device on behalf of the VA that contains Veterans' sensitive information? (If so, then Certification & Accreditation (C&A) is required for the information device; and all security controls outlined in the VA Handbook 6500, Appendix D are required.)	☐	☑	

Requirement 3: Use and regularly update antivirus software

Information devices with access to Veterans' sensitive information are required to implement malicious code protection that includes a capability for automatic updates and real-time scans.

Question	Response: (Select One) YES	NO	Comment
1. Is antivirus software installed on all information devices with access to Veterans' sensitive information?	☑	☐	
2. Is the antivirus programs capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware?	☑	☐	
3. Is the antivirus mechanism current, actively running, and capable of generating audit logs?	☑	☐	
4. Does the antivirus mechanism provide malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software)?	☑	☐	
5. Are updates to malicious code protection mechanisms made whenever new releases are available?	☑	☐	
6. Are information devices with access to Veterans' sensitive information email clients and servers configured to block attachments with file extensions associated with malicious code (e.g., .pif, .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe)?	☑	☐	
7. Do you scan your systems regularly for vulnerabilities?	☑	☐	
Please identify the scanning technology you use here: Rapid7 insightVM 8. Are malicious code protection mechanisms: a) Appropriately updated to include the latest malicious code definitions? b) Configured to perform periodic scans of the information device, as well as real-time scans of each file, as the file is downloaded, opened, or executed?	☑ ☑ ☑	☐ ☐ ☐	

Requirement 4: Implement Access Controls

VA requires the management of information device accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The frequency for reviews of information device accounts should be documented: the review of information device accounts every 90 days for moderate- and high-impact systems; the review of information device accounts every six months for low-impact systems.

At a minimum, VA requires addressing the deactivation of all computer information device accounts in a timely manner, indicative of the information device impact level, when a change in user status occurs, regardless of platform (including personal computer, network, mainframe, firewall, router, telephone, and other miscellaneous utility information devices), such as when the account user:

- Departs the agency voluntarily or involuntarily;
- Transfers to another area within the agency;
- Is suspended;
- Goes on long-term detail; or
- Otherwise no longer has a legitimate business need for information device access.

Question	Response: (Select One)		Comment
	YES	NO	
1. Are all users identified with a unique ID before allowing them to access information device components or Veterans' sensitive information?	☑	☐	
2. In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? a) Password b) Token devices (e.g., SecureID, certifications, or public key) c) Biometrics	☑	☐	
3. Are group, shared, or generic accounts and passwords forbidden?	☑	☐	
4. Are first-time passwords set to a unique value for each user?	☑	☐	
5. Must each user change their password immediately after the first use?	☑	☐	
6. Are password procedures and policies communicated to all users who have access to Veterans' sensitive information?	☑	☐	
7. Are users required to change their passwords every 90 days?	☑	☐	
8. Are user passwords required to contain both numeric and alphabetic characters?	☑	☐	
9. Are users required to submit a new password that is different from any of the last four passwords he or she has used?	☑	☐	
10. Are repeated access attempts limited by locking out the user ID after no more than six attempts?	☑	☐	
11. If a session has been idle for more than 15 minutes, must a user re-enter the password to re-activate the terminal or session?	☑	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Question	Response: (Select One)		Comment
	YES	NO	
12. Is all access to any database containing Veterans' sensitive information authenticated?	☑	☐	

Requirement 5: Conduct Risk Assessments

Risk assessments are conducted to determine the likelihood of risk to information, and whether protection mechanisms are in place to reduce risk.

Risk assessments must be conducted at VA in order to evaluate the readiness of the information device, organization, or asset that will be using Veterans' sensitive information. The risk assessments for information devices or assets with access to Veterans' sensitive information are to be updated/conducted at least every three years or whenever there is a significant change to the information device, asset or work environment that may impact the security protection of the information.

Question	Response: (Select One)		Comment
	YES	NO	
1. Has a System of Records been created per the Privacy Act of 1974?	☐	☑	***AITC mainframe is system of record for each job major app***
2. Has the information device used under this contract been categorized (High, Medium, Low) in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*?	☑	☐	
3. Has a risk assessment been conducted to estimate potential risks and vulnerabilities to the confidentiality, integrity, and availability of Veterans' sensitive information stored, processed, or transmitted?	☑	☐	
4. If a risk assessment has been conducted for the information device or asset, does the assessment adequately address:			
a) The magnitude of harm that could result from the unauthorized access, use, disclosure, modification, or destruction of the information and the information devices that support its operations and assets (including information and information devices managed/operated by external parties); and	☑	☐	
b) When the risk assessment was conducted (i.e., a risk assessment was performed for the information device in [month/year]?	☑	☐	
5. Does the risk assessment reflect and detail the folllowing conditions that may impact the security or accreditation status of the information device with access to VA sensitive information:	☑	☐	
a) Where the information is stored on the device;	☑	☐	
b) The work location of the information device;	☑	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Question	Response: (Select One) YES	NO	Comment
c) Potential access to the information device from unauthorized personnel;.and	☑	☐	
d) The latest significant changes to the information device?	☑	☐	
6. What is the risk rating of the information device, based on the risk level matrix (High, Medium, Low risk level)?	Low		
7. Are there recommended controls/alternative options to reduce risk?	☑	☐	
8. Are risk determinations annually reviewed/updated?	☑	☐	
9. What is the impact analysis and evaluation of the information device with access to Veterans' sensitive information (High, Med, Low impact)?	Med		
10. Were potential impacts considered in accordance with the US Patriot Act of 2001 and related Homeland Security Presidential Directives (HSPDs),?	☑	☐	
11. Have mitigation strategies been discussed with VA officials with significant information and information device responsibilities?	☑	☐	
12. If a risk assessment does not exist for this information device, will a risk assessment be conducted in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, as part of the C&A process?	☐	☐	N/A
13. Does a contigency plan exist for your system(s)?	☑	☐	

Requirement 6: Institute Information Security Protection

Information security is the protection of information from a wide range of threats and vulnerabilities to ensure business continuity. The framework of information security includes a minimum set of security actions needed to effectively incorporate security in the system development process.

The protection of information devices with access to Veterans' sensitive information and communications is required at the session—as opposed to packet—level by implementing session level protection where needed.

System and Communications Protection

Question	Response: (Select One)		Comment
	YES	NO	
1. Are documents or records maintained that define, either explicitly or by reference, the time period of inactivity before the information device terminates a network connection?	☑	☐	
2. Does the information device terminate a network connection at the end of a session or after the organization-defined time period of inactivity?	☑	☐	

System and Information Integrity

Question	Response: (Select One)		Comment
	YES	NO	
1. Do you use web services that utilize VA information?		☑	
2. Is the output from the information device handled in accordance with applicable laws, Executive Orders (E.O.), directives, policies, regulations, standards, and operational requirements?	☑	☐	
3. Is the output from the information device retained in accordance with applicable laws, E.O.s, directives, policies, regulations, standards, and operational requirements?	☑	☐	
4. Does the organization restrict the capability to input information to the information device to authorized personnel?	☑	☐	
5. Does the information device implement spam protection by verifying that the organization: a) Employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network? b) Employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by email, email attachments, Internet access, or other common means?	☑ ☑	☐ ☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Physical Security

Question	Response: (Select One)		Comment
	YES	NO	
1. Is the Veterans' senstive information physically controlled and securely store in controlled areas?	☑	☐	
2. Is the information device located within an area that minimizes potential damage from physical and environmental hazards?	☑	☐	
3. Is the information device positioned within an area that minimizes the opportunity for unauthorized access?	☑	☐	
4. Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where Veterans' sensitive information is accessible?	☑	☐	
5. Are appropriate facility entry controls in place to limit and monitor physical access to information devices that store, process, or transmit Veterans' sensitive information?	☑	☐	
6. Is physical access controlled to prevent unauthorized individuals from observing the display output of information system devices that display information?	☑	☐	

Requirement 7: Privacy Regulation for Storage of Veterans' Sensitive Information

VA requires that the handling and retention of output of Veterans' sensitive information be in accordance with VA policy and operational requirements. Other requirements include: (a) physical control and secure storage of the information media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media; and (b) utilizing alternative sites for the storage of backup information. Information devices with access to Veterans' sensitive information must prevent unauthorized and unintended information transfer via shared information device resources.

Access to VA Information and VA Information Systems

Question	Response: (Select One)		Comment
	YES	NO	
1. Do you maintain a current list of employees/sub-contractors that are accessing VA's information and information systems for this contract?	☑	☐	
2. Have the appropriate background investigative requirements been met for all employees and subcontractors?	☑	☐	
3. Has access (both technical and physical) to VA information and/or VA information systems been provided to employees and subcontractors, only to the extent necessary to perform the services specified in the contract?	☑	☐	
4. When employees/subcontractors leave or are reassigned, is the contracting officer 's technical representative COTR notified?	☑	☐	

Custodial Requirements

Question	Response: (Select One)		Comment
	YES	NO	
1. Were you required to sign a Business Associate Agreement prior to receiving access to Veterans' sensitive information?	☑	☐	
2. Is Veterans' senstive information, made available by the VA for the performance of this contract, used only for those purposes, unless prior written agreement from the contracitng officer?	☑	☐	
3. Is Veterans' senstive information maintained separately and not co-mingled with any other data on the contractors/subcontractors systems/media storage systems ?	☑	☐	
4. Are you ensuring that Veterans' senstive information gathered or created by the contract is not destroyed without prior written approval by the COTR?	☑	☐	
5. Are you aware that making copies of Veterans' senstive information is not permitted, except as necessary to perform efforts in support of as agreed upon by the VA?	☑	☐	
6. Is the protection of Veterans' sensitive information commensurate with the FIPS 199 security categorization?	☑	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Question	Response: (Select One) YES	NO	Comment
7. If hard drives or other removable media contain VA sensitive information, is the data sanitized (three time wipe) consistent with NIST SP 800-88, *Guidelines for Media Sanitization,* and returned to the VA at the end of the contract?	☑	☐	
8. Does the organization sanitize Veterans' sensitive information, both paper and digital, prior to disposal or release for reuse?	☑	☐	
9. Are you identified and authorized to transport Veterans' sensitive information outside of controlled areas?	☐	☑	
10. Are there policies and procedures documented for protecting Veterans' sensitive information during transport?	☑	☐	
11. Is the information device located within an area that minimizes potential damage from physical and environmental hazards?	☑	☐	
12. Is the information device positioned within an area that minimizes the opportunity for unauthorized access?	☑	☐	
13. Does the organization employ appropriate management, operational, and technical information system security controls at alternate work sites?	☑	☐	

Security Incident Investigation

Question	Response: (Select One) YES	NO	Comment
1. Does your company have a security incident reporting process?	☑	☐	
2. Do you and/or your employees know to immediately report a security/privacy incident that involves Veterans' sensitive information to their supervisor?	☑	☐	
3. Does your company know to report a security/privacy incident that involves Veterans' sensitive information to the COTR and the appropriate law enforcement entity, if applicable?	☑	☐	
4. Does the company collect the information concerning the incident (who, how, when, and where) and provide it to the COTR?	☑	☐	

Training

Question	Response: (Select One) YES	NO	Comment
1. Does the organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures?	☑	☐	

Contractor Security Control Assessment (CSCA)

Question	Response: (Select One)		Comment
	YES	NO	
2. Have all contractors/subcontractors signed the VA National Rules of Behavior?	☑	☐	
3. Have all contractors/subcontractors completed the VA approved security training?	☑	☐	
4. Have all contractors/subcontractors completed the VA approved privacy training?	☑	☐	

Appendix A. References

Department of Veterans Affairs

VA Directive 6500, *Information Security Program*.

VA Handbook 6500, Information Security Program

VA Handbook 6500.1 Electronic Media Sanitization

VA Handbook 6500.3 Certification and Accreditation

Federal Information Processing Standards

FIPS 140-2, Security Requirements for Cryptographic Modules

FIPS 190, Guideline for the Use of Advanced Authentication Technology Alternatives.

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

FIPS 201-1, Personal Identity Verification for Federal Employees and Contractors.

National Institute of Standards and Publications

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*.

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*.

NIST SP 800-73, *Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV Card Application Namespace, Data Model and Representation, 2- End-Point PIV Card Application Interface, 3- End-Point PIV Client Application Programming Interface, 4- The PIV Transitional Data Model and Interfaces*.

NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*.

NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.

NIST SP 800-88, *Guidelines for Media Sanitization*.

VA BUSINESS ASSOCIATE AGREEMENT (BAA):
During the Preaward Survey, the contractor being considered for award will receive an updated PDF file of this Business Associate Agreement and must sign and return it to GPO within 2 workdays of receipt.

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS VETERANS HEALTH ADMINISTRATION, VETERANS CRISIS LINE, AND [COMPANY TBD].

Purpose. The purpose of this Business Associate Agreement (Agreement) is to establish requirements for the Department of Veterans Affairs (VA), Veterans Health Administration (VHA), **<Veterans Crisis Line>** and **<_____>** in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI) under the terms and conditions specified below.

Scope. Under this Agreement and other applicable contracts or agreements, **<_____>** will provide **<printing and mailing>** services to, for, or on behalf of **<Veterans Crisis Line>**.

In order for **<_____>** to provide such services, **<Veterans Crisis Line>** will disclose PHI to **<_____>**, and **<_____>** will use or disclose PHI in accordance with this Agreement.

Definitions. Unless otherwise provided, the following terms used in this Agreement have the same meaning as defined by the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

"Business Associate" shall have the same meaning as described at 45 C.F.R. § 160.103. For the purposes of this Agreement, Business Associate shall refer to **<_____>**, including its employees, officers, or any other agents that create, receive, maintain, or transmit PHI as described below**.**

"Covered Entity" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Covered Entity shall refer to **<Veterans Crisis Line>**.

"Protected Health Information" or "PHI" shall have the same meaning as described at 45 C.F.R. § 160.103. "Protected Health Information" and "PHI" as used in this Agreement include "Electronic Protected Health Information" and "EPHI." For the purposes of this Agreement and unless otherwise provided, the term shall also refer to PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity or receives from Covered Entity or another Business Associate.

"Subcontractor" shall have the same meaning as the term is defined at 45 C.F.R. § 160.103. For the purposes of this Agreement, Subcontractor shall refer to a contractor of any person or entity, other than Covered Entity, that creates, receives, maintains, or transmits PHI under the terms of this Agreement.

Terms and Conditions. Covered Entity and Business Associate agree as follows:

1. Ownership of PHI. PHI is and remains the property of Covered Entity as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate agreement is in place.

2. Use and Disclosure of PHI by Business Associate. Unless otherwise provided, Business Associate:

A. May not use or disclose PHI other than as permitted or required by this Agreement, or in a manner that would violate the HIPAA Privacy Rule if done by Covered Entity, except that it may use or disclose PHI:

(1) As required by law or to carry out its legal responsibilities;
(2) For the proper management and administration of Business Associate; or
(3) To provide Data Aggregation services relating to the health care operations of Covered Entity.

B. Must use or disclose PHI in a manner that complies with Covered Entity's minimum necessary policies and procedures.

C. May de-identify PHI created or received by Business Associate under this Agreement at the request of the Covered Entity, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

3. Obligations of Business Associate. In connection with any Use or Disclosure of PHI, Business Associate must:

A. Consult with Covered Entity before using or disclosing PHI whenever Business Associate is uncertain whether the Use or Disclosure is authorized under this Agreement.

B. Implement appropriate administrative, physical, and technical safeguards and controls to protect PHI and document applicable policies and procedures to prevent any Use or Disclosure of PHI other than as provided by this Agreement.

C. Provide satisfactory assurances that PHI created or received by Business Associate under this Agreement is protected to the greatest extent feasible.

D. Notify Covered Entity within twenty-four (24) hours of Business Associate's discovery of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Breach of PHI.

(1) Any incident as described above will be treated as discovered as of the first day on which such event is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate.

(2) Notification shall be sent to the **<Brian Mano at brian.mano@va.gov>** and to the VHA Health Information Access Office, Business Associate Program Manager by email at VHABAAIssues@va.gov**.**

(3) Business Associate shall not notify individuals or the Department of Health and Human Services directly unless Business Associate is not acting as an agent of Covered Entity but in its capacity as a Covered Entity itself.

E. Provide a written report to Covered Entity of any potential access, acquisition, use, disclosure, modification, or destruction of either secured or unsecured PHI in violation of this Agreement, including any Breach of PHI, within ten (10) business days of the initial notification.

(1) The written report of an incident as described above will document the following:

(a) The identity of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, disclosed, modified, or destroyed;

(b) A description of what occurred, including the date of the incident and the date of the discovery of the incident (if known);

(c) A description of the types of secured or unsecured PHI that was involved;

(d) A description of what is being done to investigate the incident, to mitigate further harm to Individuals, and to protect against future incidents; and

(e) Any other information as required by 45 C.F.R. §§ 164.404(c) and 164.410.

(2) The written report shall be addressed to:

<Brian Mano> and submitted by email to **brian.mano@va.gov** and to the VHA Health Information Access Office, Business Associate Program Manager at VHABAAIssues@va.gov**.**

F. To the greatest extent feasible, mitigate any harm due to a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate.

G. Use only contractors and Subcontractors that are physically located within a jurisdiction subject to the laws of the United States, and ensure that no contractor or Subcontractor maintains, processes, uses, or discloses PHI in any way that will remove the information from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing.

H. Enter into Business Associate Agreements with contractors and Subcontractors as appropriate under the HIPAA Rules and this Agreement. Business Associate:

(1) Must ensure that the terms of any Agreement between Business Associate and a contractor or Subcontractor are at least as restrictive as Business Associate Agreement between Business Associate and Covered Entity.

(2) Must ensure that contractors and Subcontractors agree to the same restrictions and conditions that apply to Business Associate and obtain satisfactory written assurances from them that they agree to those restrictions and conditions.

(3) May not amend any terms of such Agreement without Covered Entity's prior written approval.

I. Within five (5) business days of a written request from Covered Entity:

(1) Make available information for Covered Entity to respond to an Individual's request for access to PHI about him/her.

(2) Make available information for Covered Entity to respond to an Individual's request for amendment of PHI about him/her and, as determined by and under the direction of Covered Entity, incorporate any amendment to the PHI.

(3) Make available PHI for Covered Entity to respond to an Individual's request for an accounting of Disclosures of PHI about him/her.

J. Business Associate may not take any action concerning an individual's request for access, amendment, or accounting other than as instructed by Covered Entity.

K. To the extent Business Associate is required to carry out Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the provisions that apply to Covered Entity in the performance of such obligations.

L. Provide to the Secretary of Health and Human Services and to Covered Entity records related to Use or Disclosure of PHI, including its policies, procedures, and practices, for the purpose of determining Covered Entity's, Business Associate's, or a Subcontractor's compliance with the HIPAA Rules.

M. Upon completion or termination of the applicable contract(s) or agreement(s), return or destroy, as determined by and under the direction of Covered Entity, all PHI and other VA data created or received by Business Associate during the performance of the contract(s) or agreement(s). No such information will be retained by Business Associate unless retention is required by law or specifically permitted by Covered Entity. If return or destruction is not feasible, Business Associate shall continue to protect the PHI in accordance with the Agreement and use or disclose the information only for the purpose of making the return or destruction feasible, or as required by law or specifically permitted by Covered Entity. Business Associate shall provide written assurance that either all PHI has been returned or destroyed, or any information retained will be safeguarded and used and disclosed only as permitted under this paragraph.

N. Be liable to Covered Entity for civil or criminal penalties imposed on Covered Entity, in accordance with 45 C.F.R. §§ 164.402 and 164.410, and with the HITECH Act, 42 U.S.C. §§ 17931(b), 17934(c), for any violation of the HIPAA Rules or this Agreement by Business Associate.

4. Obligations of Covered Entity. Covered Entity agrees that it:

A. Will not request Business Associate to make any Use or Disclosure of PHI in a manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if made by Covered Entity, except as permitted under Section 2 of this Agreement.

B. Will promptly notify Business Associate in writing of any restrictions on Covered Entity's authority to use or disclose PHI that may limit Business Associate's Use or Disclosure of PHI or otherwise affect its ability to fulfill its obligations under this Agreement.

C. Has obtained or will obtain from Individuals any authorization necessary for Business Associate to fulfill its obligations under this Agreement.

D. Will promptly notify Business Associate in writing of any change in Covered Entity's Notice of Privacy Practices, or any modification or revocation of an Individual's authorization to use or disclose PHI, if such change or revocation may limit Business Associate's Use and Disclosure of PHI or otherwise affect its ability to perform its obligations under this Agreement.

5. Amendment. Business Associate and Covered Entity will take such action as is necessary to amend this Agreement for Covered Entity to comply with the requirements of the HIPAA Rules or other applicable law.

6. Termination.

A. Automatic Termination. This Agreement will automatically terminate upon completion of Business Associate's duties under all underlying Agreements or by termination of such underlying Agreements.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, at its discretion, upon review as provided by Section 9 of this Agreement.

C. Termination for Cause. In the event of a material breach by Business Associate, Covered Entity:

(1) Will provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Covered Entity, and;

(2) May terminate this Agreement and underlying contract(s) if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.

D. Effect of Termination. Termination of this Agreement will result in cessation of activities by Business Associate involving PHI under this Agreement.

E. Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate Agreement is in place.

7. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement confers any rights, remedies, obligations, or liabilities whatsoever upon any person or entity other than Covered Entity and Business Associate, including their respective successors or assigns.

8. Other Applicable Law. This Agreement does not abrogate any responsibilities of the parties under any other applicable law.

9. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date to determine the applicability and accuracy of the Agreement based on the circumstances that exist at the time of review.

10. Effective Date. This Agreement shall be effective on the last signature date below.

Department of Veterans Affairs **Veterans Health Administration** **<Veterans Crisis Line>**	**COMPANY/ORGANIZATION**
By: _____	**By:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____