Program:	284-S									
Term:	DATE OF AWARD to October 31, 2016									
Title:	VA Survey Mailers									
										WBC, INC. dba
			CENVEO, LOS ANGELES		**DATA INTEGRATORS INC.**		**GRAY GRAPHICS**		**LITHEXCEL**	
ITEM		BASIS OF	LOS ANGELES, CA		FREDERICKSBURG, VA		CAPITOL HEIGHTS, MD		ALBUQUERQUE, NM	
NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
I.	**PROOFS:**									
(a)	Digital one-piece composite laminated color proof / digital one-off.....per trim/page-size unit.....	**15**	$50.00	$750.00	No Charge	$0.00	$15.00	$225.00	$20.00	$300.00
(b)	Adobe Acrobat PDF soft proof.....per item / per proof.....	**890**	$5.00	$4,450.00	No Charge	$0.00	$5.00	$4,450.00	$10.00	$8,900.00
II.	**PRINTING, VARIABLE IMAGING, BINDING, AND CONSTRUCTION:**									
(a)	Postcards: Printing face and back in a single ink color, including variable imaging in black and binding.....per postcard.....									
(1)	**Makeready and/or Setup.....**	**33**	$125.00	$4,125.00	$25.00	$825.00	$150.00	$4,950.00	$40.00	$1,320.00
(2)	**Running Per 1,000 Copies.....**	**350**	$50.00	$17,500.00	$14.00	$4,900.00	$25.00	$8,750.00	$48.00	$16,800.00
(b)	Cover Letters: Printing face only in black ink only, including binding .....per letter.....									
(1)	**Makeready and/or Setup.....**	**116**	$125.00	$14,500.00	$25.00	$2,900.00	$175.00	$20,300.00	$30.00	$3,480.00
(2)	**Running Per 1,000 Copies.....**	**742**	$40.00	$29,680.00	$12.00	$8,904.00	$22.00	$16,324.00	$25.00	$18,550.00
(c)	Cover Letters: Printing face only in black ink and one additional color, including binding.....per letter.....									
(1)	**Makeready and/or Setup.....**	**29**	$125.00	$3,625.00	$25.00	$725.00	$200.00	$5,800.00	$68.00	$1,972.00
(2)	**Running Per 1,000 Copies.....**	**186**	$60.00	$11,160.00	$12.00	$2,232.00	$30.00	$5,580.00	$30.00	$5,580.00
(d)	Four-Page Questionnaires: Printing in two ink colors, including variable imaging in black and binding .....per questionnaire.....									
(1)	**Makeready and/or Setup.....**	**73**	$125.00	$9,125.00	$25.00	$1,825.00	$225.00	$16,425.00	$48.00	$3,504.00
(2)	**Running Per 1,000 Copies.....**	**515**	$80.00	$41,200.00	$58.00	$29,870.00	$110.00	$56,650.00	$240.00	$123,600.00
(e)	Six-Page Questionnaires: Printing in two ink colors, including variable imaging in black and binding .....per questionnaire.....									
(1)	**Makeready and/or Setup.....**	**72**	$125.00	$9,000.00	$30.00	$2,160.00	$250.00	$18,000.00	$68.00	$4,896.00
(2)	**Running Per 1,000 Copies.....**	**413**	$80.00	$33,040.00	$83.00	$34,279.00	$125.00	$51,625.00	$360.00	$148,680.00
(f)	BRE Envelope: Printing face only in a single ink color, including construction.....per envelope.....									
(1)	**Makeready and/or Setup.....**	**145**	$35.00	$5,075.00	No Charge	$0.00	$150.00	$21,750.00	$30.00	$4,350.00
(2)	**Running Per 1,000 Copies.....**	**928**	$13.60	$12,620.80	$22.00	$20,416.00	$45.00	$41,760.00	$37.00	$34,336.00
(g)	OME Envelope: Printing face only in a single ink color, including construction.....per envelope.....									
(1)	**Makeready and/or Setup.....**	**145**	$35.00	$5,075.00	No Charge	$0.00	$200.00	$29,000.00	$30.00	$4,350.00
(2)	**Running Per 1,000 Copies.....**	**928**	$17.30	$16,054.40	$24.00	$22,272.00	$55.00	$51,040.00	$46.00	$42,688.00
III.	**INSERTING AND MAILING:**									
	Per 1,000 Survey Mailers.....	**928**	$40.00	$37,120.00	$21.00	$19,488.00	$40.00	$37,120.00	$189.00	$175,392.00
	CONTRACTOR TOTALS			**$254,100.20**		**$150,796.00**		**$389,749.00**		**$598,698.00**
	DISCOUNT		**0.00%**	$0.00	**2.00%**	$3,015.92	**2.00%**	$7,794.98	**1.00%**	$5,986.98
	DISCOUNTED TOTALS			**$254,100.20**		**$147,780.08**		**$381,954.02**		**$592,711.02**

Program:	284-S							
Term:	DATE OF AWARD to October 31, 2016							
Title:	VA Survey Mailers							
			MPM COMM. LLC		**NPC, INC.**		**CURRENT CONTRACTOR**	
ITEM		BASIS OF	WALDORF, MD		CALYSBURG, PA		NPC, INC.	
NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
I.	**PROOFS:**							
(a)	Digital one-piece composite laminated color proof / digital one-off.....per trim/page-size unit.....	**15**	$75.00	$1,125.00	$10.00	$150.00	$10.00	$150.00
(b)	Adobe Acrobat PDF soft proof.....per item / per proof.....	**890**	$10.00	$8,900.00	$5.00	$4,450.00	$5.00	$4,450.00
II.	**PRINTING, VARIABLE IMAGING, BINDING, AND CONSTRUCTION:**							
(a)	Postcards: Printing face and back in a single ink color, including variable imaging in black and binding.....per postcard.....							
(1)	**Makeready and/or Setup.....**	**33**	$100.00	$3,300.00	$500.00	$16,500.00	$90.00	$2,970.00
(2)	**Running Per 1,000 Copies.....**	**350**	$20.00	$7,000.00	$40.00	$14,000.00	$17.50	$6,125.00
(b)	Cover Letters: Printing face only in black ink only, including binding .....per letter.....							
(1)	**Makeready and/or Setup.....**	**116**	$100.00	$11,600.00	$90.00	$10,440.00	$62.85	$7,290.60
(2)	**Running Per 1,000 Copies.....**	**742**	$15.00	$11,130.00	$45.00	$33,390.00	$11.80	$8,755.60
(c)	Cover Letters: Printing face only in black ink and one additional color, including binding.....per letter.....							
(1)	**Makeready and/or Setup.....**	**29**	$100.00	$2,900.00	$115.00	$3,335.00	$84.75	$2,457.75
(2)	**Running Per 1,000 Copies.....**	**186**	$15.00	$2,790.00	$50.00	$9,300.00	$12.65	$2,352.90
(d)	Four-Page Questionnaires: Printing in two ink colors, including variable imaging in black and binding .....per questionnaire.....							
(1)	**Makeready and/or Setup.....**	**73**	$100.00	$7,300.00	$600.00	$43,800.00	$212.50	$15,512.50
(2)	**Running Per 1,000 Copies.....**	**515**	$70.00	$36,050.00	$135.00	$69,525.00	$72.75	$37,466.25
(e)	Six-Page Questionnaires: Printing in two ink colors, including variable imaging in black and binding .....per questionnaire.....							
(1)	**Makeready and/or Setup.....**	**72**	$100.00	$7,200.00	$1,450.00	$104,400.00	$250.00	$18,000.00
(2)	**Running Per 1,000 Copies.....**	**413**	$85.00	$35,105.00	$175.00	$72,275.00	$103.50	$42,745.50
(f)	BRE Envelope: Printing face only in a single ink color, including construction.....per envelope.....							
(1)	**Makeready and/or Setup.....**	**145**	$100.00	$14,500.00	$50.00	$7,250.00	$30.50	$4,422.50
(2)	**Running Per 1,000 Copies.....**	**928**	$27.50	$25,520.00	$40.00	$37,120.00	$31.80	$29,510.40
(g)	OME Envelope: Printing face only in a single ink color, including construction.....per envelope.....							
(1)	**Makeready and/or Setup.....**	**145**	$100.00	$14,500.00	$50.00	$7,250.00	$30.50	$4,422.50
(2)	**Running Per 1,000 Copies.....**	**928**	$30.00	$27,840.00	$55.00	$51,040.00	$39.00	$36,192.00
III.	**INSERTING AND MAILING:**							
	Per 1,000 Survey Mailers.....	**928**	$39.50	$36,656.00	$125.00	$116,000.00	$39.50	$36,656.00
	CONTRACTOR TOTALS			**$253,416.00**		**$600,225.00**		**$259,479.50**
	DISCOUNT		**0.00%**	$0.00	**0.25%**	$1,500.56	**0.25%**	$648.70
	DISCOUNTED TOTALS			**$253,416.00**		**$598,724.44**		**$258,830.80**
				AWARDED				

U.S. GOVERNMENT PUBLISHING OFFICE

Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

VA Survey Mailers

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

U.S. Department of Veterans Affairs (VA)

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning **Date of Award** and ending **October 31, 2016**, plus one (1) optional 12-month extension period 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 publicly opened at 11:00 a.m., prevailing Washington, DC time, on **November 12, 2015**.

BID SUBMISSION: Submit bid in pre-addressed envelope furnished with solicitation or send to: U.S. Government Publishing Office, Bid Section, Room C-848, Stop: PPSGB, 732 North Capitol Street, NW, Washington, DC 20401. Facsimile bids in response to this solicitation are permitted. Facsimile bids may be submitted directly to the GPO Bid Section, Fax No. (202) 512-1782. The program number and bid opening date must be specified with the bid. Refer to Facsimile Bids in Solicitation Provisions of GPO Contract Terms, GPO Publication 310.2, as revised June 2001. Hand delivered bids are to be taken to: GPO Bookstore, 710 North Capitol Street, NW, Washington, DC, between the hours of 8:00 a.m. and 4:00 p.m., prevailing Washington, DC, time, Monday through Friday. The contractor is to follow the instructions in the Bid Submission/Opening area. If further instruction or assistance is required, call (202) 512-0526.

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

Abstracts of contract prices are available at http://www.gpo.gov/gpo/abstracts/abstract.action?region=DC

For information of a technical nature call **David Love** (202) 512-0310 (No collect calls).

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. 6-01)) and GPO Contract Terms, Quality Assurance through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (Rev. 8-02)).

GPO Contract Terms (GPO Publication 310.2) – http://www.gpo.gov/pdfs/vendors/sfas/terms.pdf.

GPO QATAP (GPO Publication 310.1) – http://www.gpo.gov/pdfs/vendors/sfas/qatap.pdf.

DISPUTES: GPO Publication 310.2, GPO Contract Terms, Contract Clause 5. Disputes, is hereby replaced with the June 2008 clause found at www.gpo.gov/pdfs/vendors/contractdisputes.pdf. This June 2008 clause also cancels and supersedes any other disputes language currently included in existing contractual actions.

SUBCONTRACTING: Subcontracting is allowed for manufacturing of the envelopes only.

GPO IMPRINT REQUIREMENTS: The GPO imprint requirement, GPO Contract Terms, Supplemental Specifications, No. 9, is waived.

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

Product Quality Levels:

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

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

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

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

Attribute	Specified Standard
P-7. Type Quality and Uniformity	O.K. Proofs/Average type dimension/ Electronic media
P-9. Solid and Screen Tint Color Match	Pantone Matching System

Prior to award, contractor may be required to provide information related to specific equipment that will be used for production.

OPTION TO EXTEND THE TERM OF THE CONTRACT: The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed **two (2) years** as a result of, and including, any extension(s) added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustment(s).

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

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

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from **Date of Award** to **October 31, 2016**, 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 **July 31, 2015**, 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.

SECURITY – PRIVACY REQUIREMENTS:

General - 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.

SECURITY REQUIREMENTS: 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 postaward 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. (See "PREAWARD SURVEY, *Security Control Plan - Production Area*" for more information.)

(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. (See "PREAWARD SURVEY" for more information.)

SECURITY REQUIREMENTS: This contract has been designated Public Trust Position Level 1 (Limited). Due to the sensitive nature of the information contained in the products produced under this contract, contractor employees performing under this contract will be subject to a thorough civil and criminal background check. "Performing under this contract" is defined as working on-site at a VA facility (including visiting the VA site for any reason) or having access to Government programmatic or sensitive information.

The contractor shall submit a completed Background Investigation Request Worksheet (Attachment A) for each contractor employee who will be working on this contract within seven (7) calendar days of contract award. VA will process all required background checks. Contractor employees are required to be fingerprinted within 14 calendar days of contract award, unless otherwise notified by VA. It is the responsibility of the contractor to ensure fingerprint cards are processed through their local police departments or other authorized fingerprinters. VA will provide additional information on fingerprinting requirements at contract award.

The general requirements as listed above are required of any new and current contractor employees performing contract work, and any project supervisors and management officials who have access to Government sensitive information.

The contractor is responsible for updating the background investigation template as personnel are added to the contract. The contractor must submit the updated roster to the Contracting Officer within seven (7) calendar days after the added personnel are approved by VA. The background investigation forms and fingerprinting must be completed within seven (7) calendar days of the personnel being added to the contract.

Access to VA Information and VA Information System –

1. A contractor shall request logical (technical) and/or physical access to VA information and VA information systems for employees only to the extent necessary: (1) to perform the services specified in the contract; (2) to perform necessary maintenance functions for electronic storage or transmission media necessary for performance of the contract; and, (3) for individuals who first satisfy the same conditions, requirements and restrictions that comparable VA employees must meet in order to have access to the same type of VA information.

2. All contractor employees working with VA Sensitive Information are subject to the same investigative requirements as those of regular VA appointees or employees who have access to the same types of information. The level of background security investigation will be in accordance with VA Directive 0710, Handbook 0710, which are available at: http://www1.va.gov/vapubs/ and VHA Directive 0710 and implementing Handbook 0710.01 which are available at: http://www1.va.gov/vhapublications/index.cfm. Contractors are responsible for screening their employees. The following are VA's approved policy exceptions for meeting VA's background screenings/investigative requirements for certain types of contractors:

    - Contract personnel not accessing VA information resources such as personnel hired to maintain the medical facility grounds; construction contracts; utility system contractors; etc.

    - Contract personnel with limited and intermittent access to equipment connected to facility networks on which no VA sensitive information is available, including contractors who install, maintain, and repair networked building equipment, such as fire alarm; heating, ventilation, and air conditioning equipment; elevator control systems, etc. If equipment to be repaired is located within sensitive areas of a VA facility (e.g., computer room/communications closets), VA IT staff must escort contractors while on site.

    - Contract personnel with limited and intermittent access to equipment connected to facility networks on which limited VA sensitive information may reside including medical equipment. Contractors who install, maintain, and repair networked medical equipment such as CT scanners, EKG systems, ICU monitoring, etc. In this case, Veterans Health Administration facilities must have a duly executed VA business associate agreement (BAA) in place with the contractor in accordance with the VHA Handbook 1600.01, Business Associates, to assure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in addition to this contract. Contract personnel, if on site, must be escorted by VA IT staff.

3. Contract personnel who require access to national security programs must have a valid security clearance. The National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. Defense Security Service (DSS) administers the NISP on behalf of the Department of Defense and 23 other federal agencies within the Executive Branch. VA will verify clearance through DSS.

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).

Information System Design and Development –

1. Information systems that are designed or developed for, or on behalf of, VA at non-VA facilities shall comply with all VA policies developed in accordance with Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle, a privacy impact assessment will be completed, provided to the VA representative, and approved by the VA Privacy Service in accordance with VA Privacy Impact Assessment Handbook 6500.3.

2. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37 and VA Handbook 6500.

3. The contractor will be required to design, develop, or operate a System of Records on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties. *(NOTE: Contractor is to retain 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.)*

4. The contractor agrees to –

    a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies the systems of records; and the design, development, or operation work that the contractor is to perform;

    b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and,

    c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

5. In the event of violations of the Act, a civil action may be brought against the agency involved when 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 when 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 is considered to be an employee of the agency.

6. "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.

7. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

8. "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.

Information System Hosting, Operation, Maintenance and/or Use –

1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. The contractor security control procedures must be identical, not equivalent, to those procedures used to secure VA systems (see Attachment B, *"Contractor Rules of Behavior"*). A privacy impact assessment (PIA) must also be provided to the VA representative and approved by VA Privacy Service prior to operational approval. All external Internet connections involving VA information must be reviewed and approved by VA prior to implementation.

2. Adequate security controls for collecting, processing, transmitting, and storing of personally identifiable information, as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls need to be stated within the PIA and supported by a risk assessment. If these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

3. Outsourcing (contractor facility/contractor equipment/contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation of the contractor's systems in accordance with NIST Special Publication 800-37 and VA Handbook 6500 and a privacy impact assessment of the contractor's systems prior to operation of the systems. Government-owned (Government facility/Government equipment), contractor-operated systems, third party or business partner networks require a system interconnection agreement and a memorandum of understanding (MOU) which detail what data types will be shared, who will have access, and the appropriate level of security controls for all systems connected to VA networks.

4. The contractor must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA Contracting Officer and the Information Security Officer (ISO) for entry into VA's Plan of Action and Milestone management process. The contractor will use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor procedures will be subject to periodic, unannounced assessments by VA officials. The physical security aspects associated with contractor activities will also be subject to such assessments. As updates to the system occur, an updated PIA must be submitted to the VA Privacy Service through the VA representative for approval.

5. All electronic storage media used on non-VA leased or owned IT equipment that is used to store, process, or access VA sensitive information must have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with VA policies and procedures upon: (1) completion or termination of the contract or (2) disposal or return of the IT equipment by the contractor or any person acting on behalf of the contractor, whichever is earlier.

6. Contractor must have physical and environmental security controls to protect system, buildings and related infrastructures from individuals and environmental threats. Building physical security requirements will meet or exceed the physical security standards and practices as established with VA Directives and Handbook 0730, Security and Law Enforcement. There will be an Annual physical security survey conducted. Specific requirements and options are found in VA Directive and Handbook 0730 appendix B (Agent Cashier).

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 Controls Compliance Testing – On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within this contract. With 10 workday's notice, at the request of the Government, the contractor will fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by VA in the event of a security incident or at any other time.

Security Training –

1. All contractor employees requiring access to VA sensitive information and/or VA information systems shall complete the following before being granted access to VA networks or sensitive information:

   - Sign and acknowledge understanding of, and responsibilities for, compliance with the *Contractor Rules of Behavior* (Attachment B) relating to access to VA information and information systems;
   - Successfully complete VA Cyber Security Awareness training and annual refresher training as required;
   - Successfully complete VA General Privacy training and annual refresher training as required; and
   - 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 Contracting Officer a copy of the training certificates for each applicable employee (for the required training as stated above) within seven (7) calendar days 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.

Contractor Personnel Security –

1. All contractor employees who require access to the Department of Veterans Affairs' computer systems shall be the subject of a background investigation and must receive a favorable adjudication from the VA Security and Investigations Center (07C). The level of background security investigation shall be in accordance with VA Directive 0710, dated May 18, 2007, and is available at:

   http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1569 (VA Handbook 0710, Appendix A, and Tables 1 - 3).

   Appropriate Background Investigation (BI) forms shall be provided upon contract award and are to be completed and returned to the VA Security and Investigations Center (07C) within three (3) calendar days for processing. Contractor shall be notified by 07C when the BI has been completed and adjudicated. If the security clearance investigation is not completed prior to the start date of the contract, the employee **shall not work** on the contract while the security clearance is being processed. Work will commence as soon as the contractor and the contractor employee receives an email message that states the following: "*We show that the background investigation request on the individual listed below has been completed, and the case has been initiated by the Security Investigations Center*." When the case is completed, all adjudicative paperwork will be returned to the requesting office. The contractor can provide this email to the Station ISO as proof the investigation has been initiated and access can be granted. This notice does NOT ensure completion of VetPro or other required security training. Those individuals that require VetPro Credentialing or additional security training must receive those completion notifications from the proper authority prior to start date of contract.

2. The investigative history for contractor personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Security Service (DSS). Should the contractor use a vendor other than OPM or DSS to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

Background Investigation –

The position sensitivity impact for this effort has been designated as **Low Risk** and the level of background investigation is **NACI.**

Contractor Responsibilities –

1. The contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by OPM through the VA, the contractor shall reimburse the VA within 30 calendar days of receipt of invoice from VA.

2. Background investigations from investigating agencies other than OPM/DSS are permitted if the agencies possess an OPM and Defense Security Service certification. The Vendor Cage Code number must be provided to the Security and Investigations Center (07C), which shall verify the information and advise the Contracting Officer whether access to the computer systems can be authorized.

3. The contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain a U.S. citizenship and are able to read, write, speak, and understand the English language.

4. After contract award but prior to contract performance, the contractor shall submit a completed Background Investigation Request Worksheet (Attachment A) for each contractor employee who will be working on this contract.

5. The contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration from working under the contract.

6. Failure to comply with the contractor personnel security requirements may result in termination of the contract for default.

7. Further, the contractor shall be responsible for the actions of all individuals provided to work for the VA under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor shall be responsible for all resources necessary to remedy the incident.

Government Responsibilities –

1. The VA Security and Investigations Center (07C) shall provide the necessary forms to the contractor or to the contractor's employees after receiving a list of names and addresses.

2. Upon receipt, the VA Security and Investigations Center (07C) shall review the completed forms for accuracy and forward the forms to OPM to conduct the background investigation. The VA facility shall pay for investigations conducted by the OPM in advance. In these instances, the contractor shall reimburse the VA facility within 30 calendar days of receipt of invoice from VA.

3. The VA Security and Investigations Center (07C) shall notify the VA representative and contractor after adjudicating the results of the background investigations received from OPM.

4. The VA representative will ensure that the contractor provides evidence that investigations have been completed or are in the process of being requested.

ELECTRONIC AND INFORMATION TECHNOLOGY STANDARDS:

Intranet/Internet –

1. The contractor shall comply with the U.S. Department of Veterans Affairs Directive 6102 and VA Handbook 6102 (Internet/Intranet Services).

2. VA Directive 6102 sets forth policies and responsibilities for the planning, design, maintenance support, and any other functions related to the administration of a VA Internet/Intranet Service Site or related service (hereinafter referred to as "Internet"). This directive applies to all organizational elements in the Department. This policy applies to all individuals designing and/or maintaining VA Internet Service Sites, including but not limited to, full time and part time employees, contractors, interns, and volunteers. This policy applies to all VA Internet/Intranet domains and servers that utilize VA resources. This includes, but is not limited to, va.gov and other extensions such as, ".com, .eddo, .mil, .net, .org," and personal Internet service pages managed from individual workstations.

3. VA Handbook 6102 establishes Department-wide procedures for managing, maintaining, establishing, and presenting VA Internet/Intranet Service Sites or related services (hereafter referred to as "Internet"). The handbook implements the policies contained in VA Directive 6102, Internet/Intranet Services. This includes, but is not limited to, File Transfer Protocol (FTP), Hypertext Markup Language (HTML), Simple Mail Transfer Protocol (SMTP), Web pages, Active Server Pages (ASP), e-mail forums, and list servers.

4. VA Directive 6102 and VA Handbook 6102 are available at:

   Internet/Intranet Services Directive 6102
   http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

   Internet/Intranet Services Handbook 6102
   http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

5. Internet/Intranet Services Handbook 6102 Change 1 – updates VA's cookie use policy, Section 508 guidelines, guidance on posting of Hot Topics, approved warning notices, and minor editorial errors. Internet/Intranet Services Handbook 6102 Change 1 is available at:
   http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

6. In addition, any technologies that enable a Network Delivered Application (NDA) to access or modify resources of the local machine that are outside of the browser's "sand box" are strictly prohibited. Specifically, this prohibition includes signed-applets or any ActiveX controls delivered through a browser's session. ActiveX is expressly forbidden within the VA while .NET is allowed only when granted a waiver by the VA CIO **PRIOR** to use.

7. JavaScript is the preferred language standard for developing relatively simple interactions (i.e., forms validation, interactive menus, etc.) and Applets (J2SE APIs and Java Language) for complex network delivered applications.

SECTION 508 COMPLIANCE:

1. The contractor shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998.

2. In December 2000, the Architectural and Transportation Barriers Compliance Board (Access Board), pursuant to Section 508(2) (A) of the Rehabilitation Act Amendments of 1998, established Information Technology accessibility standards for the Federal Government. Section 508(a)(1) requires that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology (EIT), they shall ensure that the EIT allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. The Section 508 requirement also applies to members of the public seeking information or services from a Federal department or agency.

3. Section 508 text is available at:

   - http://www.opm.gov/HTML/508-textOfLaw.htm

   - http://www.section508.gov/index.cfm?FuseAction=Content&ID=14

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.

PREAWARD SURVEY: In order to determine the responsibility of the contractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's facility of all of the contractor's computer, printing, and mailing equipment which will be used on this contract or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract. Attending the preaward survey will be representatives from the GPO and the VA.

Contractors must complete Attachment C "*Contractor Security Control Assessment (CSCA), Self-Assessment Questionnaire for Contract Service Providers*" for VA review and use during the preaward survey security review.

The preaward survey will include a review of the contractor's backup facility, quality control, mail, recovery program, computer systems, material, personnel, production, and security plans, as required by this specification.

The contractor shall present, in writing, to the Contracting Officer within seven (7) calendar days of being notified to do so by the Contracting Officer or his/her representative, detailed plans for each of the following activities. The workday after notification to submit will be the first day of the schedule.

THESE PROPOSED PLANS ARE SUBJECT TO REVIEW AND APPROVAL BY THE GOVERNMENT AND AWARD WILL NOT BE MADE PRIOR TO APPROVAL OF SAME.

Backup Facility – The failure to distribute the postcards and mailers in a timely manner would have an impact on the daily operations of VA. Therefore, if for any reason(s) (act of God, labor disagreements, etc.) the contractor is unable to perform at said location for a period of longer than seven (7) calendar days, the contractor must have a contingency plan in place for a backup facility with the capability of producing the postcards and mailers.

Plans for this contingency production must be prepared and submitted to the Contracting Officer as part of the preaward survey. These plans must include the location of the facility to be used, security plans at the facility, equipment available at the facility, and a timetable for the start of production at that facility. Part of the plan must also include the transportation of Government materials from one facility to the other. The contractor must produce items from a test file at the new facility for verification of software prior to producing the postcards and mailers at this facility.

NOTE: All terms and conditions of this contract will apply to the backup facility.

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 and recovery plans 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. 6-01)). A recovery system is required to replace all defective, missing, or mutilated pieces. This control system must 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 (postcard or mailer) 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 daily, 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.

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. 6-01)).

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 and 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 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 a 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.

Computer System Plan – This plan must include a detailed listing of the contractor's operating software platform and file transfer system necessary to interface with VA's File Transfer Management System (FTMS) for electronic transmission of files from VA. The plan must also include the media type on which files from VA will be received to the extent that operator intervention (e.g., a tape mount) is not required at VA or the contractor's production facility. The Computer System Plan shall demonstrate the contractor's ability to provide complete hardware and software compatibility with VA's existing network.

Included with the Computer System Plan shall be a resume for each employee responsible for the monitoring and the programming of the contractor's computer system and file transmissions.

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 listing of all personnel who will be involved with this contract. For any new employees the plan should include the source of these employees and a description of the training programs the employee's will be given to familiarize them with the requirements of this program.

NOTE: If employees have current and adequate security clearances, please notate.

Production Plan – The contractor is to provide a detailed plan of the following –

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

The contractor shall enter into a Business Associate Agreement (BAA) and establish an Interconnection Security Agreement (ISA) with the VA, and be in accordance with HIPAA with VA prior to initial production of VA's Health Benefits Communications materials. The system must comply with Federal Information Security Management Act (FISMA) requirements for Government systems.

The proposed Security Control Plan must address the following:

Materials – How 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 postcard and 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.

ON-SITE REPRESENTATIVES: One or two full-time Government representatives may be placed on the contractor's premises on a limited basis or throughout the term of the contract.

On-site representative(s) may be stationed at the contractor's facility to: provide project coordination in receipt of wire transmissions; verify addresses; monitor the printing, imaging, folding, inserting, mail processing, quality control, sample selections, and inspections; and monitor the packing and staging of the mail. These coordinators will not have contractual authority, and cannot make changes in the specifications or in contract terms, but will bring any and all defects detected to the attention of the company Quality Control Officer. The coordinators must have full and unrestricted access to all production areas where work on this program is being performed.

The contractor will be required to provide one private office of not less than 150 square feet, furnished with at least one desk, two swivel arm chairs, secure internet access for Government laptop computers, a work table, and two four-drawer letter-size files with combination padlock and pendaflex file folders or equal.

NOTE: In the event that a Government representative cannot be on-site, and upon completion of the individual print order, the contractor is to ship overnight the quality sample pulls from that print order and send to one destination in Washington, DC. The remainder of the mailers mail per contract requirements. (See "QUALITY SAMPLE PULLS.")

POSTAWARD CONFERENCE: Unless waived by the Government, the total requirements of the job as indicated in these specifications will be reviewed by Government representatives with the contractor's representatives at the contractor's facility immediately after award. The contractor will be notified of the exact date and time.

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 **Date of Award** through **October 31, 2016**, 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.

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

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

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

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

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

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

PRIVACY ACT NOTIFICATION: This procurement action requires the contractor to do one or more of the following: design, develop, or operate a system of records on individuals to accomplish an agency function in accordance with the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

PRIVACY ACT

(a) The contractor agrees:

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

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

(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.

SECTION 2. - SPECIFICATIONS

SCOPE: These specifications cover the production of postcards and survey mailers consisting of cover letters, questionnaires, business reply envelopes (BRE), and outbound mail envelopes (OME) requiring such operations as electronic prepress, printing, variable imaging, binding, construction, inserting, and distribution.

TITLE: VA Survey Mailers.

FREQUENCY OF ORDERS:

Postcards: Up to approximately 6 orders per month.
Survey Mailers: Approximately 5 to 15 orders per month.

NOTE: The first order placed will be for proofs only (see "PROOFS"). Multiple orders requiring the same schedule may be placed on the same day. Separate print orders will issued for the each different postcard and each different survey mailer.

QUANTITY:

Postcards: Approximately 3,000 to 60,000 copies per order.
Survey Mailers: Approximately 800 to 60,000 copies per order.

NUMBER OF PAGES:

Postcards: Face and back.
Cover Letters: Face only.
Questionnaires: 4 pages (2 face and back leaves) or 6 pages (3 face and back leaves) per order.
BRE Envelopes: Face only (after construction).
OME Envelopes: Face only (after construction).

NOTE: Number of pages for the questionnaire will vary between 4 or 6 pages depending on the survey mailer.

TRIM SIZES:

Postcards: 4-1/4 x 6".
Covers Letters: 8-1/2 x 11".
Questionnaires: 8-1/2 x 11". (NOTE: A variance of 1/16" or less on either side of the 11" dimension is allowed; however product cannot be larger than 8-1/2 x 11".)
BRE Envelopes: No. 9 (3-7/8 x 8-7/8"), plus flap.
OME Envelopes: No. 10 (4-1/8 x 9-1/2"), plus flap. (NOTE: OME envelopes will contain a window.)

GOVERNMENT TO FURNISH:

The static text matter and artwork for all items will be furnished as an electronic file via SFTP. Files will be furnished as an Adobe Acrobat PDF file (current/near current version). All fonts will be embedded. The contractor is cautioned that furnished fonts are the property of the Government and/or its originator. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract. NOTE: 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 variable data will be transferred to the contractor's SFTP site for retrieval by the contractor with each order. The variable data will be furnished as a flat (fixed column) ASCII file.

Identification markings such as register marks, commercial identification marks of any kind, etc., carried in the electronic files, must not print on finished product.

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

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

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

When required by the Government, the contractor shall make minor revisions to the electronic files. It is anticipated that the Government will make all major revisions.

Prior to making revisions, the contractor shall copy the furnished files and make all changes to the copy.

PROOFS:

On the First Order Only:

Contractor to submit proofs (as applicable below) for the postcard, cover letter, 4-page questionnaire, 6-page questionnaire, BRE envelope, and OME Envelope. NOTE: Proofs will be for the static text matter only.

If produced via conventional offset printing – One (1) set of digital one-piece composite laminated halftone proofs on the actual production stock (Kodak Approval, Polaroid PolaProof, CreoSpectrum, or Fuji Final Proof) with a minimum resolution of 2400 x 2400 dpi. 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. Proofs must show dot structure. NOTE: In lieu of digital one-piece laminated proofs, at contractor's option, inkjet proofs that are G7 profiled and use pigment-based inks may be submitted. 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. 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 2009.

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.

Pantone colors may be substituted with a similar color. (NOTE: This requirement does not apply to inkjet proofs.) Contractor to submit ink draw downs on actual production stock of Pantone color(s) used to produce the product.

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

On Every Order:

Contractor must submit proofs (as specified below) for the postcard (when ordered on a print order) or the 4- and 6-page questionnaires (when ordered on a print order). A PDF soft proof must be submitted for the first five (5) names in the furnished file and must include the variable data for those five (5) names.

One (1) Adobe Acrobat (current version) PDF soft proof. PDF proof must show all artwork, static information, and variable data, as applicable for each item. Proof will be transferred to the agency via SFTP site. The PDF proof will be evaluated for text flow, image position and color breaks. 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.

CONTRACTOR MUST NOT PRINT PRIOR TO THE RECEIPT OF AN "O.K. TO PRINT."

STOCK/PAPER: The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No. 12" dated March 2011.

Government Paper Specification Standards No. 12 – http://www.gpo.gov/pdfs/customers/sfas/vol12/vol_12.pdf.

Postcards: White Offset Cover, basis weight: 100 lbs. per 500 sheets, 20 x 26", equal to JCP Code L23.

Cover Letters: White Offset Book, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

Questionnaires: White Offset Book, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60. *EXCEPTION: Stock must NOT contain any recycled content. NOTE: Stock MUST match MOCR stock (24-lb.) in brightness and cleanliness.*

BRE Envelopes (No. 9): White Writing Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20.

OME Envelopes (No. 10): White Writing Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20.

PRINTING AND VARIABLE IMAGING: At contractor's option, the products 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.

GPO imprint is waived and must not print on the items in the mailer.

Match Pantone color as indicated on the print order.

NOTE: For products that contain variable data, the contractor must print and variable image in a single pass.

Postcards: Print face and back in a single ink color. Printing consists of text and line matter, and agency seal. Variable image face only in black. Imaging consists of text and line matter (name, address, eSurvey passcode, and barcode).

Cover Letters: Print face only in black ink only, or in black ink and one additional Pantone color. Printing consists of text and line matter, and agency seal. Majority of cover letters ordered will print in black ink only.

Questionnaires: Print head-to-head in black ink and Pantone 185U. Printing consists of text and line matter. Variable image in black on multiple pages throughout. Variable imaging consists of text and line matter (name, address, barcode, and survey sequence number).

BRE Envelopes: Print face only (after construction) in a single ink color. Printing consists of text and line matter. NOTE: Return envelopes must be printed in Business Reply Format.

OME Envelopes: Print face only (after construction) in single ink color. Printing consists of text and line matter, and agency seal.

Printing on envelopes shall be in accordance with the requirements for the style envelope ordered. All printing shall comply with all applicable U.S. Postal Service regulations, including automation guidelines/requirements. The envelope shall accept printing without feathering or penetrating to the reverse side.

Both the BRE and OME envelopes require a security tint printed on the inside (back - before manufacture) in black ink. Contractor may use his own design but must guarantee that the product will ensure complete opacity and prevent show through of any material contained therein.

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

BINDING (Postcards, Cover Letters, and Questionnaires):

Postcards: Trim four sides.

Cover Letters: Trim four sides.

Questionnaires: Trim four sides.

CONSTRUCTION (Envelopes):

All Envelopes (BRE and OME): Envelopes must be open side, side seam, with gummed fold-over flap for sealing. Flap depth is at the contractor's option but must meet all USPS requirements. Flap must be coated with suitable glue that will securely seal the envelope without adhering to contents, not permit resealing of the envelope, and permit easy opening by the recipient. Envelopes shall be sufficiently high cut so as to prevent the flap adhesive from coming in contact with the envelope's contents. The sealed seam shall not adhere to the inside of the envelope. Envelopes shall be free from cuts, folds, tears, machine marks, foreign matter, dirt, ink smears, and adhesive stains.

OME envelopes will require one die-cut window (1-3/8 x 4-1/2" in size) located 7/8"from left edge of envelope and 1/2" from bottom edge of envelope for viewing of mailing address on questionnaire. Window must have slightly rounded corners. Die-cut window is to be covered with a suitable poly-type, transparent, low-gloss material that must be clear of smudges, lines and distortions. Poly-type material must be securely affixed to the inside of the envelope so as not to interfere with insertion of contents. Window material must meet the current U.S. Postal Service's (USPS) readability standards/requirements.

INSERTING: Gather questionnaire leaves in sequence with cover letter behind and letter-fold (with a barrel fold) to 3-5/8 x 8-1/2", with mailing address (on page 1 of questionnaire) on top for visibility through window on OME envelope. Place folded questionnaire/letter on top of BRE envelope and insert into OME envelope. (NOTE: Face of BRE envelope should be facing the inside back of the OME envelope, when inserted.)

NOTE: It is the contractor's responsibility to assure that only the mailing address and barcode on the questionnaire is visible through the window on the OME envelope, and that only one questionnaire, cover letter, and BRE envelope is inserted into each OME envelope.

After inserting, seal OME envelopes.

QUALITY SAMPLE PULLS: The contractor will be required to pull one (1) test sample every 1,000 postcards or mailers, as applicable. NOTE: For orders placed with a quantity of less than 1,000 copies, contractor must pull 1 random test sample.

For quality sample pulls of mailers, the mailers must be complete – all required items printed/imaged, bound/constructed, and inserted in accordance with these specifications.

Quality sample pulls for an order must be signed and dated by the contractor operator and placed in a container. The Government on-site representative will review. Once approved, these samples will be mailed at a later date. (See "ON-SITE REPRESENTATIVES.")

The samples constitute a part of the total quantity ordered, and no additional charge will be allowed.

DISTRIBUTION:

- Mail f.o.b. contractor's city each individual postcard or survey mailer to domestic addresses nationwide. (NOTE: The contractor is responsible for all costs incurred in transporting the postcards and mailers to the U.S. Postal Service facility.)

- Deliver f.o.b. destination approximately 2 to 25 samples of the postcard and the complete survey mailer (as ordered) to: Clara Chafee, 2625 Townsgate Road, Suite 100, Westlake Village, CA 91361.

All mailing (postcards and mailers) shall be made at the Presorted First Class rate.

Contractor will mail using departmental mailing permit imprint through VA's Centralized Account Processing System (CAPS). Contractor is responsible for establishing the CAPS account.

NOTE: The contractor is required 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.

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

Orders which result in mailings of less than 200 pieces or less than 50 pounds will 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.

Certificate of Conformance: When using Permit Imprint Mail the contractor must complete GPO Form 712 - Certificate of Conformance (Rev. 2-91), supplied by GPO and the appropriate mailing statement or statements, supplied by USPS.

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

Upon completion of each order, the contractor must notify the ordering agency on the same day that the product mails via email to the email address specified on the print order. The subject line of the email shall be "Distribution Notice for Program 284-S, P.O. XXXXX, Jacket XXX-XXX, Print Order XXXXX." The notice must provide all applicable tracking numbers and mailing method. Contractor must be able to provide copies of all mailing receipts upon agency request.

All expenses incidental to submitting proofs 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).

Print order and all furnished materials will be provided via SFTP.

When required, PDF soft proofs must be sent via SFTP.

When required, hard copy proofs must be delivered to and picked up from: Clara Chafee, 2625 Townsgate Road, Suite 100, Westlake Village, CA 91361.

No definite schedule for pickup of material can be predetermined.

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.

Contractor must complete production and distribution within five (5) workdays.

- No specific date is set for submission of proofs. Proofs must be submitted as soon as possible to allow for revised proofs, if contractor's errors are judged serious enough to require them.

- Proofs will be withheld no more than two (2) workdays from their receipt at the ordering agency until they are made available for pickup or the corrections/changes/"O.K. to print" are provided to the contractor (via email), as applicable. (The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- All proof and transit time is included in the 5-workday schedule.

The ship/deliver date indicated on the print order is the date products ordered for delivery f.o.b. destination must be delivered to the destinations specified, and the date products ordered for mailing f.o.b. contractor's city must be delivered to the U.S. Postal Service.

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.

For compliance reporting purposes, contractors are to report information regarding each order with date of shipment or delivery, as applicable, in accordance with the contract requirements by contacting the Shared Support Services Compliance Section via email at compliance@gpo.gov, via telephone at (202) 512-0520, or via facsimile at (202) 512-1364. Personnel receiving the email, call, or facsimile will be unable to respond to questions of a technical nature or to transfer any inquiries.

SECTION 3. - DETERMINATION OF AWARD

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

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

I.	(a)	15
	(b)	890

		(1)	(2)
II.	(a)	33	350
	(b)	116	742
	(c)	29	186
	(d)	73	515
	(e)	72	413
	(f)	145	928
	(g)	145	928

III.		928

THIS PAGE IS INTENTIONALLY BLANK.

SECTION 4. - SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city for all mailing and f.o.b. destination for all other shipments.

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

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

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government. Bids submitted with NB (No Bid) or blank spaces for an item may be declared non-responsive.

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

All invoices submitted to the GPO shall be based on the most economical method of production. Fractional parts of 1,000 will be prorated at the per-1,000 rate.

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

I. PROOFS: For line item I.(a), the face of each envelope will be charged as one trim/page-size unit.

(a) Digital one-piece composite laminated color proof/
digital one-off ..... per trim/page-size unit .....$_____

(b) Adobe Acrobat PDF soft proof..... per item/per proof .....$_____

II. PRINTING, VARIABLE IMAGING, BINDING, AND CONSTRUCTION: Prices offered must be all inclusive and include the cost of materials and operations (including stock) necessary for the printing, variable imaging, binding, and construction listed in accordance with these specifications.

	Makeready and/or Setup (1)	Running Per 1,000 Copies (2)
(a) Postcards: Printing face and back in a single ink color, including variable imaging in black and binding ..... per postcard.....	$_____	$_____
(b) Cover Letters: Printing face only in black ink only, including binding..... per letter.....	$_____	$_____
(c) Cover Letters: Printing face only in black ink and one additional color, including binding ..... per letter.....	$_____	$_____

_____
(Initials)

	Makeready and/or Setup (1)	Running Per 1,000 Copies (2)
(d) Four-Page Questionnaires: Printing in two ink colors, including variable imaging in black and binding ..... per questionnaire	$_____	$_____
(e) Six-Page Questionnaires: Printing in two ink colors, including variable imaging in black and binding ..... per questionnaire	$_____	$_____
(f) BRE Envelope: Printing face only in a single ink color, including construction ..... per envelope	$_____	$_____
(g) OME Envelope: Printing face only in a single ink color, including construction ..... per envelope	$_____	$_____

III. INSERTING AND MAILING: Prices offered must be all inclusive and include the cost of all required materials and operations necessary for the mailing of the survey mailers, including cost of collating questionnaire leaves and cover letter, lettering-folding to required size in accordance with these specifications, insertion of questionnaires/cover letters and BRE envelopes into OME envelope, and mailing, in accordance with these specifications.

Per 1,000 Survey Mailers ..... $_____

INSTRUCTIONS FOR BID SUBMISSION: Fill out "SECTION 4.-SCHEDULE OF PRICES," initialing or signing each page in the space(s) provided. Submit two copies (original and one exact duplicate) of the "SCHEDULE OF PRICES" with two copies of the GPO Form 910 "BID" form. Do not enter bid prices on GPO Form 910; prices entered in the "SCHEDULE OF PRICES" will prevail.

Bidder _____

_____
(City - State)

By _____
(Signature and title of person authorized to sign this bid)

_____
(Person to be contacted) (Telephone Number)

ATTACHMENT A

Background Investigation Request Worksheet

Background Investigation Request Worksheet Page 1 of 1

Background Investigation Request Worksheet

If you need assistance, please call: 501.257.4017

VA Organization:

Please complete the following fields on all applicants:

Station where applicant will work -
Station Name - City: State: Station #:

Station to be billed for clearance -
Station Name - City: State: Station #:

Please complete the following fields on each VA or Contract Employee:

Applicant Name - Last: First: Middle: *If none (NMN)*
SSN: DOB: Email:
Place of Birth - City: State: Country:
Contractor Occupation:
Are you asking for a low risk clearance on a foreign national? ○ Yes ○ No
Type of Investigation requested: ○ High Risk (BI) ○ Moderate Risk (MBI) ○ Low Risk (NACI)

Please complete the following fields on all Contractor Personnel:

Contracting Officer/COTR: COTR Phone: COTR Email:
Complete Address: State: Zip Code:

Contracting Company Name:
Contracting Company POC: POC Phone: POC Email:
Complete Address: State: Zip Code:

Clear Form Submit Form

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

Contractor Security Control Assessment (CSCA)

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

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Table of Contents

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

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:	
Title:	
Telephone:	
Business Address:	
Email:	

Part 2. Contractor Organization Information	
Contact Name:	
Title:	
Telephone:	
Business Address:	
Email:	

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?:

Contractor Security Control Assessment

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	
Signature of Person Completing This Document	***Date***
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) YES	NO	Comment
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*			
3. If the firewall used is a software product:	☐	☐	
a) Is it set to download automatic updates?	☐	☐	
b) Is the firewall software product installed on your PC (i.e, McAfee, Norton)?	☐	☐	
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?	☐	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

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: 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?	☐ ☐ ☐	☐ ☐ ☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

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) YES	NO	Comment
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) YES	NO	Comment
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) YES	NO	Comment
1. Has a System of Records been created per the Privacy Act of 1974?	☐	☐	
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)

Question	Response: (Select One)		Comment
	YES	NO	
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)?			
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)?			
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?	☐	☐	
13. Does a contigency plan exist for your system(s)?	☐	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

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) YES	NO	Comment
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) YES	NO	Comment
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)

Physical Security

Question	Response: (Select One) YES	NO	Comment
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?	☐	☐	

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

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) YES	NO	Comment
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) YES	NO	Comment
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)

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)

VA INFORMATION PROTECTION

Question	Response: (Select One) YES	NO	Comment
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?	☐	☐	

Contractor Security Control Assessment (CSCA)

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.*