Program No 650-S Term 06/13/13 To 05/31/14										
TITLE: Veterans Health Identification Cards (VHIC)										
			KNIGHTSBRIDGE							
			GRAPHICS		**LEE DISTRIBUTING**		**NPC, INC.**		**3M COGENT, INC.**	
			High Point, NC		**Dallas, TX**		**Claysburg, PA**		**St. Paul, MN**	
		BASIS OF								
ITEM NO.	DESCRIPTION	AWARD								
I.	**PRINTING/IMAGING, BINDING AND CONSTRUCTION:**		UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
(a)	Daily makeready/setup charge…….	365	$0.00	**$0.00**	$250.00	**$91,250.00**	$500.00	**$182,500.00**	$0.00	**$0.00**
(b)	VIC Legacy card……....per 1000 cards	70	$894,250.00	**$62,597,500.00**	$1,150.00	**$80,500.00**	$1,612.50	**$112,875.00**	$905.88	**$63,411.60**
(c)	Interim VHIC Card……..……per 1000 cards	2	$171,500.00	**$343,000.00**	$1,120.00	**$2,240.00**	$1,612.50	**$3,225.00**	$905.88	**$1,811.76**
(d)	WEDI VHIC Card……..……per 1000 cards	1747	$4,900.00	**$8,560,300.00**	$1,120.00	**$1,956,640.00**	$1,765.88	**$3,084,992.36**	$905.88	**$1,582,572.36**
(e)	Carrier Sheet (Face only)……..……per 1000 sheets	1455	$0.00	**$0.00**	$21.02	**$30,584.10**	$67.00	**$97,485.00**	$43.61	**$63,452.55**
(f)	Carrier Sheet (Face and back)……..…..per 1000 sheets	364	$0.00	**$0.00**	$33.02	**$12,019.28**	$67.00	**$24,388.00**	$43.61	**$15,874.04**
(g)	Mail-out Envelope, including cost of envelope									
	……..per 1000 sheets	1819	$0.00	**$0.00**	$33.23	**$60,445.37**	$17.25	**$31,377.75**	$70.51	**$128,257.69**
II.	**INSERTING AND MAILING:**									
	Mailers……per 1000 mailers	1819	$0.00	**$0.00**	$69.08	**$125,656.52**	$54.50	**$99,135.50**	$0.00	**$0.00**
III.	**PROGRESS REPORTS:**									
	Progress Report…….per report	16	$0.00	**$0.00**	$175.00	**$2,800.00**	$625.00	**$10,000.00**	$0.00	**$0.00**
	CONTRACTOR TOTALS			**$71,500,800.00**		**$2,362,135.27**		**$3,645,978.61**		**$1,855,380.00**
	DISCOUNT		0.0%	**$0.00**	0.0%	**$0.00**	0.25%	**$9,114.95**	2.0%	**$37,107.60**
	DISCOUNTED TOTALS			**$71,500,800.00**		**$2,362,135.27**		**$3,636,863.66**		**$1,818,272.40**
										AWARDED

U.S. GOVERNMENT PRINTING OFFICE

Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Veterans Health Identification Cards (VHIC)

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

U.S. Department of Veterans Affairs

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning Date of Award and ending May 31, 2014, plus up to four (4) optional 12-month extension periods that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

BID OPENING: Bids shall be publicly opened at 11:00 a.m., prevailing Washington, DC time, on **June 13, 2013**.

BID SUBMISSION: Submit bid in pre-addressed envelope furnished with solicitation or send to: U.S. Government Printing Office, Bid Section, Room C-161, Stop: PPSB, 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.

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

For information of a technical nature, call AST-4, Linda Rodano (202) 512-0310. (No collect calls.) or via lrodano@gpo.gov

SECTION 1. - GENERAL TERMS AND CONDITIONS

GPO CONTRACT TERMS: Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 6-01)) and GPO Contract Terms, Quality Assurance Through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (revised August 2002)).

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 the printing of the static information on the cards only and the 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. Prior to production samples/O.K. Proofs/ Average type dimension/Electronic media
P-8. Halftone Match (Single and Double Impression)	O.K. Prior to production samples/O.K. Proofs/ Electronic media
P-9. Solid and Screen Tint Color Match	Pantone Matching System
P-10. Process Color Match	O.K. Prior to production samples/O.K. Proofs/ Electronic media

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

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

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

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from Date of Award to May 31, 2014, 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 February 28, 2013, 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 post award conference between the Contracting Officer and the responsible contractor representative.

(b) The contractor shall process all confidential information obtained from VA in the performance of this contract under the immediate supervision and control of authorized personnel, and in a manner that will protect the confidentiality of the records in such a way that unauthorized persons cannot retrieve any such records.

(c) The contractor shall inform all personnel with access to the confidential information obtained from VA in the performance of this contract of the confidential nature of the information and the safeguards required to protect this information from improper disclosure.
(d) For knowingly disclosing information in violation of the Privacy Act, the contractor and the contractor employees may be subject to the criminal penalties as set forth in 5 U.S.C Section 552a (i)(1), which is made applicable to contractors by 5 U.S.C. 552a (m)(1) to the same extent as employees of the VA. For knowingly disclosing confidential information as described in section 1106 of the Social Security Act (42 U.S.C. 1306), the contractor and contractor's employees may also be subject to the criminal penalties as set forth in that provision.

(e) The contractor shall assure that each contractor employee with access to confidential information knows the prescribed rules of conduct, and that each contractor employee is aware that he/she may be subject to criminal penalties for violations of the Privacy Act.

(f) All confidential information obtained from VA for use in the performance of this contract shall, at all times, be stored in an area that is physically safe from unauthorized access. (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 an 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) n 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.

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.

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. 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 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.ees-learning.net/.

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. You 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 or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility of all of the contractor's/subcontractor'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 the *Contractor Security Control Assessment (CSCA), Self-Assessment Questionnaire for Contract Service Providers* (Attachment C) for VA review and use during the preaward survey security review.

The preaward survey will include a review of: all subcontractors involved, along with their specific functions; and the contractor's/subcontractor's mail, material, personnel, production, quality control/recovery program, security, and backup facility 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 Veterans Identification Cards 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 backup facility with the capability of producing the cards.

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 cards 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, and/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/VHIC 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, and/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. Samples should be in unsealed envelopes with handbooks or inserts. 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 cards and carrier sheets 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 cards in a set.
2. Validating the count of carrier sheets in a set.
3. Validating the sequence of cards in a set.
4. Validating the sequence of sets in a production batch.
5. Interrupting production if variances are detected.

Mailing integrity shall be defined as follows: All records received from VA that are designated for hard copy printing were printed, inserted and entered correctly into the United States 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 hard copy printing were printed, inserted and mailed correctly. The contractor's inserting equipment must have automated systems that include coding and scanning technology capable of –

1. Reconciling card 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 VHIC Unique ID (UID) for Management Information (MI) reporting.

Recovery System – A recovery system will be required to ensure all defective, missing, and/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 pick-up/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 cards, 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 VHIC mailers. The contractor may produce other products besides the VHIC in this area, but all personnel must be cleared and identified in the Personnel Plan and adhere to the Security Control Plan.

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.

Option Years: For each option year that may be exercised, the contractor will be required to re-submit, in writing, the above plans detailing any changes and/or revisions that may have occurred. The contractor should be prepared to submit these revised plans at each year's meeting (See "PRE-PRODUCTION MEETING"). THE REVISED PLANS ARE SUBJECT TO GOVERNMENT APPROVAL. If the meeting is waived by the Government, the revised plans must be submitted to GPO within five (5) workdays of notification of the option year being exercised.

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

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 transmissions; verify addresses; monitor the printing, folding, packaging, mail processing, quality control, sample selections and inspections; and, monitor the packing and staging of the mail and processing of undeliverable mail and secure destruction of undeliverable mail and defective/mutilated pieces. 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 or escorted access to all production areas where work on this program is being performed.

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. A print order will be issued monthly and will indicate the total number of identification cards produced that month. The print order will also indicate any other information pertinent to the particular order.

ORDERING: Items to be furnished under the contract shall be ordered by the issuance of monthly print orders by the Government. Orders may be issued under the contract from Date of Award through May 31, 2014, 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 will be issued monthly and shall detail the monthly volume of cards required. 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.

BILLING: Within the first five (5) workdays of each month, the contractor shall submit an itemized statement for billing for the previous month's production to the ordering agency for examination and certification as to the correctness of the billing. Submit billing to: Jeffrey.Pace@va.gov (unless otherwise specified on the print order).

Once a print order has been closed, the billing invoice must be submitted to the U.S. Government Printing Office for payment. Submit to: U.S. Government Printing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401. (NOTE: GPO offers a Contractor Fax Billing System. Please visit the GPO website for more information.)

NOTE: Contractor will NOT be allowed to submit billing on any print order that has not been closed.

SECTION 2. - SPECIFICATIONS

SCOPE: These specifications cover the production of current, interim, and new Veterans Health Identification Card mailers consisting of a card, carrier sheet, and mail-out envelope requiring such operations as receiving and transmitting data, electronic prepress, printing (including four-color process), variable imaging, binding/construction, inserting, and distribution.

TITLE: Veterans Health Identification Cards.

BACKGROUND: VA began issuing Veterans a Veterans Identification Card (VIC) in 2004. The VIC is used by Veterans within the VA health care facility as proof of identity for such activities as checking in with a person or by kiosk for lab work, diagnostic tests and appointments, or to pick up prescriptions and durable medical equipment. Card readers at VA health care facilities read the magnetic stripe or bar code to access quickly the Veteran's electronic record from VA information systems thereby providing operational efficiencies. This action can also be used to print automatically armbands and labels. This contract covers the issuance of the three (3) phases of cards (the current VIC and the new VHIC) resulting from implementation of new software and business processes. Cards will initially be issued utilizing two software packages with separate card data file coming from each system. As sites complete transition to the new software package (scheduled to be completed no later than September 30, 2013), the old system (used for the VIC) will be retired, and the new cards (used for the VHIC) will be issued only from the new software data files. Each card is described below:

Current State/Old VIC **(hereinafter referred to as the "VIC Legacy" card) –** The current state/old card request process typically begins at the VA health care facility when a clerk takes a Veteran's photo and enters his/her card request into a VA information system. The Veteran's card request information (e.g. requesting facility information, personal information, and photo) are transmitted from the requesting VA health care facility's information system to the National Card Management Directory (NCMD). It is then transmitted to a Secure FTP site for retrieval by the contractor. The contractor retrieves the card request, manufactures the card according to current VA's specifications, and after confirming the address is a valid mailing address, mails the card to the Veteran's address. In the event the Veteran's address is found to be invalid, the contractor mails the card to the requesting VA health care facility address. The Veteran's Identification Card bears a color photo (1x 1") of the Veteran and displays the Veteran's name and, if applicable, indicators of the Veteran's service-connected disability, Former Prisoner of War and/or Purple Heart status on the front of the card. The front of the card contains a background image with microtext, VA Logo, black text, and bar code with the Veteran's social security number (SSN). The back of the card contains a 3-track high coercivity magnetic stripe with the Veteran's name, SSN, date of birth, service-connected disability indicator, and Integration Control Number (ICN). *(See Attachment D (VIC Legacy sample) and Attachment E (NCMD Schema v3) for complete card details.)*

Between October 1, 2008 and September 30, 2009, 839,000 cards were produced. Over 5.5 million of the 7.8 million Veterans enrolled in the VA health care system have been issued a card. Card requests generally range between 2,400 and 2,800 per day. The contractor will begin issuing VIC Legacy cards no later than 45 calendar days after contract award and will continue issuing to sites that have not transitioned to the new software during the deployment of the new VHIC application by VA. Production will be for new enrolled Veterans and replacement of lost or damaged cards. As VA facilities transition to the new software and begin issuing the new card, production of the old card will cease. Printing of old cards will continue until all sites complete the transition, which is expected to occur in 2013. VA is testing and piloting its new software. The schedule may vary depending upon success of the new software.

Interim VHIC Card – The Interim VHIC card will be a bridge between the VIC Legacy card and WEDI VHIC card (see Future State/New WEDI VHIC Card below). It includes the implementation of the new web-based software that will send separate card request data files to the contractor and a redesigned card. VA will need time to make updates to several key systems to make them compatible with the use of the new Member ID (EDIPI, which replaces the SSN). Use of the Interim card allows the new VHIC software conversion to proceed on schedule and provide a more secure card to be issued to Veterans. The Interim VHIC and WEDI VHIC cards are identical except that certain data elements will not be included on the Interim VHIC. ***It is possible that changes needed to implement the final card may be in place in sufficient time that the Interim VHIC will not be utilized (except for pilot sites), and production will start with the WEDI VHIC.***

The process for receiving card request information is similar to that of the Legacy system above, but the file will be

processed by the new VHIC 4.0 database instead of the NCMD. It is then transmitted to a Secure FTP site for retrieval by the contractor. The contractor retrieves the card request, manufactures the card according to the new VA's specifications, presorts mail, and mails the card to the Veteran's address. In the event the Veteran's address is found to be invalid, the contractor mails the card to the requesting VA health care facility address.

The Interim VHIC card bears a color photo (1 x 1") of the Veteran and displays the Veteran's name and, if applicable, indicators that the Veteran is a VA Healthcare Enrollee, Service Connected, Medal of Honor, Purple Heart and/or Former Prisoner of War status placed on the front of the card in all capitals. "VA Healthcare Enrollee" is currently not a field that will be transmitted in the data file from VA. All cards will have VA Healthcare Enrollee printed on them as the first indicator. Future VA enhancements may include this field as a variable field to be added to the data file sent from the VA. The front of the card contains a background image with microtext "U.S. DEPARTMENT OF VETERANS AFFAIRS," VA Logo, black text, and bar code with the Veteran's Member ID (EDIPI) and card number. The Member ID and Plan ID will not be printed on the face of the card. (This file information will be ignored for the Interim VHIC Card.) The back of the card contains a 3-track high coercivity magnetic stripe with WEDI compliant data. *(See Attachment F (Interim VHIC - Face), Attachment G (Interim VHIC and WEDI VHIC – Back), and Attachment H (VHIC Card Standards) for complete card details.)* The design of the Interim VHIC Card may be changed if delays in implementing the Future State/WEDI VHIC card occurs.

NOTE: The contractor will begin issuing Interim VHIC cards no later than 45 calendar days after contract award. The production of Interim VHIC cards will be concurrent with production of the Legacy cards.

Future State/New Workgroup for Electronic Data Interchange (WEDI) VHIC Card **(hereinafter referred to as the "WEDI VHIC" card)** – The future state/new card request process utilizes the web-based software system and the redesigned card deployed as part of the Interim VHIC card. The process is similar to the current system which typically begins at the VA health care facility when a clerk proofs the Veteran with approved identification documents then takes a Veteran's photo and enters his/her card request into a VA information system. The Veteran's card request information (e.g. requesting facility information, personal information, and photo) are transmitted from the VHIC 4.0 software application to a Secure FTP site for retrieval by the contractor. (NOTE: The change in program/card name to VHIC was after the VHIC 4.0 application was developed. It is currently referred to as either VIC 4.0 or VHIC 4.0. Future release may vary the name of the application.) The contractor retrieves the card request, manufactures the card according to the new VA's specifications, and mails the card to the Veteran's address. In the event the Veteran's address is found to be invalid, the contractor mails the card to the requesting VA health care facility address.

The WEDI VHIC bears a color photo (1 x 1") of the Veteran and displays the Veteran's name and, if applicable, indicators that the Veteran is VA Healthcare Enrollee, Service Connected, Medal of Honor, Purple Heart and/or Former Prisoner of War status placed on the front of the card in all capitals. All cards will have VA Healthcare Enrollee printed on them as the first indicator. The front of the card contains a background image with microtext "U.S. DEPARTMENT OF VETERANS AFFAIRS," VA Logo, black text, and bar code with the Veteran's Member ID (EDIPI), and card number. The card will comply with WEDI standards and include a Member ID, Plan ID, and expiration date printed on the face of the card. The Veteran will have an option to elect a variable service indicator emblem (or none at all) that will be placed on the face of the card in color. VA will provide authorized images upon contract award. Braille "VA" will be personalized on each card to the left of the service indicator to help visually impaired Veterans recognize the card as their VHIC. The back of the card contains a 3-track high coercivity magnetic stripe with WEDI compliant data. *(See Attachment I, (WEDI VHIC – Face), Attachment G, (Interim VHIC and WEDI VHIC – Back), and Attachment H, (VHIC Card Standards), for complete card details.)*

The contractor will begin issuing new WEDI VHIC no later than 30 calendar days after notification by VA, but will have a minimum of 45 calendar days from contract award. Transition of all VA sites to the new software is scheduled to be completed no later than September 30, 2013. Deployment schedule will be provided by VA within 10 calendar days of contract award. The contractor will be issuing old and new cards concurrently until all sites have transitioned to the new software. Interim cards shall be used in place of the new WEDI VHIC until VA systems are updated to recognize data on the new cards. After full transition, only new WEDI VHIC will be issued. The contractor shall maintain capability to issue old cards for a minimum of six (6) months after final transition to new system or sooner, if approved by a VA representative.

NOTE: The Workgroup for Electronic Data Interchange is the recognized standard for HIPAA compliant health benefit cards. Information about WEDI can be found by accessing the following link:

http://www.wedi.org/topics/health-id-card.

FREQUENCY OF ORDERS:

It is anticipated that approximately 12 print orders (monthly) per year will be issued.

Files will be available on the VA network on a daily basis. A file consists of all cards requests placed during the previous 24 hours. Typically, one file will be transmitted daily; however, on occasion, more than one file may be transmitted.

When the print order is issued each month, it will be for that month's files. Contractor is not to start production of received files until the print order for that month's files has been issued. The print order will be for the production of the cards, carrier sheets, and mail-out envelopes required for that month's production.

Due to the high volume of cards that will require production on a daily basis, the print order issued each month will be an "open" print order to cover all work performed during that month. At the end of each month, the contractor must notify the ordering agency via email, as specified on the open print order, with the total quantity of all work produced in that month in order to "close" the print order (see "BILLING" in SECTION 1).

Contractor will NOT be allowed to submit billing on any print order that has not been closed.

QUANTITY:

Approximately 2,000 to 10,000 cards per day. (NOTE: An occasional daily transmission may be for up to 25,000 cards.)

Exact quantities will not be known until each file is electronically transmitted to the VA network. NO SHORTAGES WILL BE ALLOWED.

NOTE: At the beginning of the contract, typical daily transmissions will be for approximately 2,000 to 3,000 cards. When the transition to the WEDI VHIC is complete, VA anticipates an increase in production of 1 million to 2 million additional cards ordered annually (if option years are exercised) until all Legacy cards have been replaced.

The Government reserves the right to increase or decrease the quantity by up to 20% of the total cards ordered annually for the VIC Legacy, Interim VHIC, and WEDI VHIC cards.

NUMBER OF PAGES:

Identification Cards (VIC Legacy, Interim VHIC, and WEDI VHIC): Face and back.
Carrier Sheet: Face only or face and back.
Mail-out Envelope: Face only (after construction).

TRIM SIZE:

Identification Cards (VIC Legacy, Interim VHIC, and WEDI VHIC): 3.37 x 2.125".
Carrier Sheet: 8-1/2 x 11".
Mail-out Envelope: 4-1/8 x 9-1/2" (No. 10), plus flap.

GOVERNMENT TO FURNISH: File(s) for the variable data will be transmitted electronically to the VA network using the One-VA VPN or other secure VPN network. The contractor shall utilize their network resources to access the VA network to retrieve the card request file(s) by 6:00 p.m., Eastern Time, each calendar day. Typically, one (1) file each day is created by the VA for the contractor. However, there may be more than one (1) file, if it is necessary. The contractor will pick up multiple files if more than one file exists for that day.

The files will be furnished as follows:

- Each card print request file transmitted will contain a header record and a trailer record. Both the header and trailer records indentify the name of the file, the date/time stamp of the file, and the number of records in the file. The header record also contains eight (8) fields that specify a special message that will occupy eight (8) lines on the card carrier. If no special text is to be placed on the card carrier, these fields will contain no characters. Any card request records follow the header record. All records will be variable in length, tab delimited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control codes 0x000D and 0x000A). *(See Attachment J, (VIC Legacy Print File Specifications v2) and Attachment K (VHIC Print File Specifications v3.8).)*

- Each card print request file transmitted will be responded to with a card print request acknowledgement file. The acknowledgement file will contain a header record and a trailer record that identifies the name of the file, date/time stamp of the file, the number of records in the file, and the card print request file tht is being acknowledged. If a corrupt card print request file cannot be processed, the acknowledgement rile should contain a null data recored and a header and trailer specifying a record count of zero. Each record will be in variable length, tab delimited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control code 0x000D and 0x000A). *(See Attachment J (VIC Legacy Print File Specifications v2) and Attachment K (VHIC Print File Specificationsv3.8).)*

A file (created in Adobe Illustrator CS 6) will be furnished via FTP or email for all card artwork and static text matter. All printer and screen fonts will be furnished. Files will be furnished in PostScript and native application format. Visuals may be furnished. Color identification system used is Pantone Matching System and CMYK. NOTE: The file will be furnished once at the beginning of the contract and held for re-use throughout the term of the contract. If the artwork changes during the term of the contract, a new file will be furnished.

A final template will be furnished for the carrier sheet text and layout at contract award.

One reproduction proof, Form 905 (R. 6/03), with labeling and marking specifications.

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

EXHIBITS (Attachments): The facsimiles of samples pages shown as Attachments D through L are representative of the requirements which will be ordered under this contract. However, it cannot be guaranteed that future orders will correspond exactly to these attachments.

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.

PRE-PRODUCTION (KICK-OFF) MEETING: VA and GPO shall schedule the date and time of the pre-production meeting (30 calendar days of contract award) with the contractor, which shall be hosted by the contractor at the contractor's VHIC production facility. The contractor and the Government will introduce key project personnel. The contractor will conduct a tour of their manufacturing facility demonstrating compliance with VA security and privacy requirements, quality assurance standards, and card production.

The VA will conduct its initial on-site inspection of the contractor's production and subcontractor's facilities. The visit will review information, security, and privacy compliance.

Pre-Production Meeting Briefs: The contractor shall brief the VA project team on their Business Plan, Project Schedule, Risk Management Plan, Security Plan and Quality Management/Quality Control Plan (as specified below under "CONTRACT PLANS") during the pre-production meeting describing their plan for fulfillment of the project requirements. The contractor shall provide the Contracting Officer and VA a hardcopy of each of the documents at the pre-production meeting and with electronic versions of these documents via email. VA shall review and provide feedback as to their acceptance or required amendments to the plans. The contractor shall provide amended plans to GPO and VA, via email, within five (5) calendar days of receiving VA's requested edits.

CONTRACT PLANS: The contractor shall develop, review, analyze, finalize and maintain the following contract plans and make submit to the Government at the pre-production meeting:

Business Plan: The contractor shall establish a detailed business plan which documents the contractor's plan for accomplishing the tasks and deliverables specified in this contract. The business plan will address short term and long term project goals and metrics incorporating project milestones and deliverables. The business plan shall describe the approach and dependencies for the project implementation and ongoing publication of the cards and specification compliance. The approach will include identification of roles and responsibilities.

The plan will include how the data and cards will be managed, from receipt of Veteran data from the VA through to mailing of the cards and provision of card status to VA, availability of contractor resources (including network connectivity options), hours of operation, contractor response to contractor system outages, contractor response to technical issues regarding exchange of files with the VA, notification to the client for necessary downtime due to upgrades or other service requirements. The Business Plan will be documented in MS Word and hard copy.

Project Schedule: The contractor shall provide a project schedule for implementing publication of the VHIC cards (VIC Legacy, Interim VHIC, and VHIC WEDI). The project schedule will identify the tasks, assignments, durations, and dependencies necessary to complete the Prior to Production (Proof of Concept) samples and implement the full production deployment of the cards. The project schedule will be developed in MS Project. The project schedule will provide information in both Gantt charts and CPM (Critical Path Method). Contractor will also be responsible for providing hard copies of the project schedule.

Risk Management Plan: The contractor shall develop a risk management plan that provides a framework to identify and mitigate the risks associated with the project and that are compliant with the Committee of Sponsoring Organizations (COSO) internal control risk management standards and practices. The contractor shall ensure risks are identified and recorded in a Risk Registry with appropriate mitigation strategies according to the risk management plan. The risks shall be re-evaluated based on probability, likelihood, and impact, and any new risks identified and communicated on a monthly basis. The contractor shall review the Risk Management Plan at least quarterly and update it as soon as changes are indicated. The risk management plan will be maintained throughout the life of the contract.

Security Plan: The contractor shall provide a security plan that addresses all aspects of physical and logical/data file handling, processing and transfer, including, card publication and all associated 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 card production.

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.

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 the cards.

The contractor shall include in the security plan how each of the specifications for VHIC (VA ISO 7816) is met for the information to be encoded on the card (http://www.iso.org/iso/home.html).

Quality Management/Quality Control Plan: The contractor shall establish an integrated quality assurance/quality management plan to advance the contractor's ability to meet or exceed customer requirements, including that Veteran information is correctly contained on the card; card stock is compatible with VA specifications; card bears the VA approved card design and applicable design features; and, meets VA card carrier standards and mailing functions. The quality management/quality control plan will describe the contractor's quality assurance process for measuring and monitoring and continuously improving all facets of card production including but not limited to job run, and statistical sampling for all phases of card production and mailing. Cards rejected due to the quality assurance process will be reproduced and mailed within 24 hours of rejection. Cards rejected due to the quality assurance process will be destroyed at the end of the day's production run.

The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this contract. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's quality control program is the means by which he assures himself that his work complies with the requirement of the contract.

The contractor shall reject cards that do not meet contract specifications identified in the quality management/quality control plans. Cards that are found to not meet quality standards will be re-produced by the contractor at no cost to the Government, including poor photo quality if result of contractor personalization process. Contractor will be reimbursed for cards that are rejected due to poor photo quality/standards in the images received from VA.

The contractor shall provide confirmation information to VA within two (2) hours of receipt of VA's card request file, and information related to the mailing of each card within 24 hours of the mailing.

The contractor shall review the plan at least quarterly and update it as soon as changes are indicated. The quality management/quality control plan will be maintained throughout the life of the contract.

After acceptance of the quality management/quality control plan, the contractor shall inform the Contracting Officer and VA representative, in writing, within five (5) calendar days of changes made to the document.

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.

All halftones are to be 300 dpi or finer.

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: ***Proofs will be required one time only for each card (VIC Legacy, Interim VHIC, and WEDI VHIC). Proofs for the VIC Legacy and Interim VHIC will be required at the same time requiring the same schedule.***

One (1) Adobe Acrobat (current version) PDF soft proof each of the 25 cards specified for the Prior to Production Samples (specified herein). PDF proof of each card must show all artwork, static information, and variable information and photo. Proof will be transferred to the agency via email. The PDF proof will be evaluated for text flow, image position and color breaks. Proofs will not be used for color match.

For the WEDI VHIC, PDF proofs must show placement of Braille "VA."

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

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

PRIOR TO PRODUCTION SAMPLES (PROOF OF CONCEPT): ***Prior to production samples will be required one time only for each card (VIC Legacy, Interim VHIC, and WEDI VHIC). Samples for the VIC Legacy and Interim VHIC cards will be required at the same time requiring the same schedule.***

Prior to the commencement of production of the contract production quantity for each card (VHIC Legacy, Interim, VHIC, and WEDI VHIC), the contractor shall submit not less than 25 sample card mailers consisting of the card attached to the carrier sheet, folded, and inserted into the mail-out envelope. (DO NOT SEAL ENVELOPES.) All samples will be tested for conformance of material(s) and/or for construction.

Each sample is to be printed/imaged, bound, constructed, and packaged, as specified herein. NOTE: Each card and carrier sheet sample will be imaged with different individuals' name and information.

All samples shall be printed and constructed as specified and must be of the size, kind, and quality that the contractor will furnish. Samples will be inspected and tested for conformance of materials and must comply with the specifications as to construction, kind, and quality of materials.

Within three (3) calendar days of the pre-production meeting, VA shall make their Proof of Concept card request file available to the contractor. The contractor shall utilize their network resources to access the VA network using the One-VA Virtual Private Network (VPN) to retrieve the Proof of Concept card request file.

The contractor shall provide confirmation via email to VA within two (2) hours of receipt of VA's Proof of Concept card request file.

For the VIC Legacy, contractor must have samples available at the Preproduction Meeting (30 calendar days of contract award).

For the Interim VHIC, contractor must submit samples (via traceable means) within 30 calendar days of notification by VA. Samples must be delivered f.o.b. destination to: VHA, Health Eligibility Center, Attn: MBD, VHIC Program Manager, 2957 Clairmont Road, Suite 200, Atlanta, GA 30329. The container and accompanying documentation shall be marked "PREPRODUCTION SAMPLES" and shall include the GPO Purchase Order, Jacket, Program, and Print Order Number.

For the WEDI VHIC, contractor must submit samples (via traceable means) within 30 calendar days of notification by VA. Samples must be delivered f.o.b. destination to: VHA, Health Eligibility Center, Attn: MBD, VHIC Program Manager, 2957 Clairmont Road, Suite 200, Atlanta, GA 30329. The container and accompanying documentation shall be marked "PREPRODUCTION SAMPLES" and shall include the GPO Purchase Order, Jacket, Program, and Print Order Number.

The Government will approve, conditionally approve, or disapprove the samples within 10 calendar days of the receipt thereof. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons therefore.

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

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

In the event the Government fails to approve, conditionally approve, or disapprove the samples within the time specified, the Contracting Officer shall automatically extend the shipping schedule in accordance with article 12

"Notice of Compliance with Schedules" of contract clauses in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 6-01)).

Manufacture of the final product prior to approval of the sample submitted is NOT allowed. Samples will not be returned to the contractor. All costs, including the costs of all samples, shall be included in the contract price for the production quantity.

All samples shall be manufactured at the facilities and on the equipment in which the contract production quantities are to be manufactured.

TEST SAMPLES: On occasion, the Government shall request "test" cards to be utilized to verify compatibility with VA software modifications. A separate test file will be provided with appropriate data to produce the test cards.

These requests will be limited to 10 to 25 cards per request.

Cards are to be produced on plain white card stock, as specified herein, (no background image) with personalization of data to the magnetic stripe and bar code. Printed information will be limited to a test name only for identification of the card.

Contractor must ship test cards within 24 hours of request via reimbursable overnight shipping using traceable means, and samples must be received within 48 hours of notification of email request.

VA will provide location and method of shipment for test cards. Such requests will be authorized through the VA representative. Contractor must notify VA of all shipping information including tracking numbers when test cards are picked up by small package carrier. Contractor will be reimbursed for all shipping costs by submitting shipping receipts with billing invoice for payment.

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.

Identification Cards (VIC Legacy, Interim VHIC, and WEDI VHIC): White Standard PVC, 0.030 mil thick.

Carrier Sheet: White Writing, basis weight: 24 lbs. per 500 sheets, 17 x 22, equal to JCP Code D10.

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

PRINTING/VARIABLE IMAGING:

NOTE: Digital printing of the carrier sheets and mail-out envelopes is acceptable provided the digital printing has a minimum of 600 x 600 resolution and a minimum of 150-line screen. Inkjet and toner based inks are acceptable.

GPO imprint is waived and must not print on the finished product.

VIC Legacy: Print face and back. Face of card prints in four-color process. Printing consists of text matter, agency logo, artwork. Variable image face only. Variable imaging consists of text and bar code in black and photo in four-color process. Back of card prints in four-color process. Printing consists of text and line matter and magnetic strip (T-3 HICO).

Interim VHIC: Print face and back. Face of card prints in four-color process. Printing consists of text matter, agency logo/seal, optional flag or other image, and optional military branch emblem. Variable image face only. Variable imaging consists of text and bar code in black and photo in four-color process. Back of card prints in black only. Printing consists of text and line matter and magnetic strip (T-3 HICO).

WEDI VHIC: Print face and back. Face of card prints in four-color process. Printing consists of text matter, agency logo/seal, optional flag or other image, and optional military branch emblem. Variable image face only. Variable imaging consists of text and bar code in black and photo in four-color process. Back of card prints in black only. Printing consists of text matter and magnetic strip (T-3 HICO).

Carrier Sheet: Print face only or face and back, as ordered, in black ink only. Printing consists of text matter, halftones, and agency logo/seal. Variable image face only in black only. Variable imaging consists of text matter (date, VA facility address, and Veteran's name/address). *(See Attachment L (Carrier Sheet – Face).)*

Carrier Sheet: Print face only or face and back, as ordered, in black ink only. Printing consists of text matter, halftones, and agency logo/seal. Variable image face only in black only. Variable imaging consists of text matter (date, VA facility address, Veteran's name/address, and variable text).

Mail-out Envelope: Print envelopes face only (after construction) in black ink only. Printing consists of mailing indicia.

Mail-out 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.

Printing 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.

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

BINDING/CONSTRUCTION:

Identification Cards (VIC Legacy, Interim VHIC, and WEDI VHIC): Trim four sides. Round all corners with a radius of 2.88 to 3.48 mm.

Top Coat: After printing, top coat the entire surface (face and back minus magnetic stripe) of the card with Datacard® Cardgard, having a thickness of 0.5 mil (suitable to protect cards). The topcoat product must have no distortion of the printed matter and must remain clear and legible. Lamination is acceptable as an option but must be of equivalent or better quality of topcoat and must be trimmed flush to card.

Carrier Sheet: Trim four sides. Attach card to lower left corner (or mid-sheet, as specified) of carrier sheet with repositionable adhesive so that card remains attached to sheet during mailing, but removes easily without damage to card. Letter-fold carrier sheet with attached card with a "Z-fold" with Veteran's name and address facing out and card facing in.

NOTE: It is the contractor's responsibility to assure that the name on the card corresponds with the name on the carrier sheet.

Mail-out Envelope: Envelopes must be open side, diagonal 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.

Face of envelope contain one die-cut address window with slightly rounded corners (3-1/8 x 4-1/2" in size) located 1/2" from the left edge and 5/8" from the bottom edge of the envelope. (Long dimension of window is parallel to long dimension of envelope.) Die-cut window is to be located in alignment with the return address and mailing address location on the carrier sheet. NOTE: Die-cut window on all envelopes must allow for the viewing of the return address and mailing address on the carrier sheet.

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: Insert folded carrier sheet (with attached card) into mail-out envelope.

NOTE: It is the contractor's responsibility to assure that only the return address and the Veteran's name/address and bar code are visible through the window on the mail-out envelope and that only one carrier sheet/card is inserted into each envelope.

After inserting, seal mail-out envelopes.

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

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

Contractor is required to apply the appropriate postage to each mailing. Contractor will be reimbursed for postage by submitting a properly completed postal service form (or equivalent) with billing invoice for payment.

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.

CASS Certification – Contractor is required to perform the Coding Accuracy Support System (CASS) certification using USPS certified ZIP+4 software to generate ZIP+4 Codes and Delivery Point Barcodes. Contractor is required to furnish USPS with any required CASS certificates. All related costs to perform this operation must be included in submitted bid pricing. No additional reimbursement will be authorized.

NOTE: In the event that a mailing address is determined to be undeliverable as a result of the CASS operations, contractor must mail the card to the VA facility used as the return address.

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 650-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 picking up and returning materials, as applicable, submitting proofs, and furnishing prior to production samples must be borne by the contractor.

SCHEDULE: Adherence to this schedule must be maintained. Contractor must not start any monthly production prior to receipt of the individual monthly print order (GPO Form 2511).

Print order and all furnished materials will be provided via email or FTP.

The contractor shall retrieve the first files(s) from VA to begin production within approximately 45 calendar days of contract award.

Workday - The term "workday" is defined as Sunday through Saturday each week, exclusive of the days on which Federal Government holidays are observed. Also excluded are those days on which the Government is not open for the transaction of business, such as days of national mourning, hazardous weather, etc. (NOTE: In the event that the mail date (in accordance with the below schedules) falls on a Sunday or on a day when the Government is not open, contractor is to mail the following workday.

Proofs and Prior to Production Samples Only –

The following schedule begins the SAME workday as receipt of file transmissions.

When required, contractor must submit (via email) all required PDF soft proofs within 10 calendar days of notification of availability of print order and furnished materials.

PDF soft proofs will be withheld no longer than 10 calendar days of receipt by the Government.

Contractor must furnish prior to production samples within 30 calendar days of contract award (VIC Legacy) or implementation of new software (Interim VHIC and WEDI VHIC).

The Government will approve, conditionally approve, or disapprove the samples within 10 calendar days of the receipt thereof.

Card Production –

The following schedule begins the SAME workday as receipt of daily file transmissions.

- Contractor to complete production and distribution for each daily transmission up to and including 10,000 cards within 48 hours of receipt of the file transmission(s).

- Contractor to complete production and distribution for each daily transmission for 10,001 up to and including 25,000 cards within 96 hours of receipt of the file transmission(s).

- Contractor to complete production and distribution for each daily transmission for 25,001 up to and including 50,000 cards within 144 hours of receipt of the files transmission(s).

- Contractor to complete production and distribution for each daily transmission 50,001 up to and including 100,000 cards within 192 hours of receipt of the file transmission(s).

NOTE: On approximately 5 to 10 occasions per year, the contractor will be required to produce up to 10 cards within a 24 hour period. When this is required, the VA will notify the contractor via email specifying that a "RUSH" 24-hour schedule is required. These cards will be produced from data from previous cards transmitted within the previous 60 calendar days. These RUSH cards must be shipped via reimbursable overnight shipping using traceable means and must be received within 48 hours of notification of email request. Contractor must notify VA of all shipping information including tracking numbers when cards are picked up by small package carrier. Contractor will be reimbursed for all shipping costs by submitting all shipping receipts with billing invoice.

The ship/deliver date indicated on the print order is the date products ordered for mailing f.o.b. contractor's city must be delivered to the U.S. Post Office.

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

For compliance reporting purposes, 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.

REJECTED CARDS: Cards rejected due to poor photo quality from the file received from the VA will be collected and shipped each Friday to arrive by the following Monday. Contractor to ship (reimbursable) by express carrier to the appropriate VA health care facility. Poor photo quality standards are to be documented in the quality management/quality control plan. Minimum standards shall include a rejection of any cards where any part of the face (not hair) is touching an edge of the photo, any blank or white out of image, any image too dark or blurred that facial features cannot be recognized to allow a positive identification match. These cards will be identified as "mailed" once shipped to the appropriate VA health care facility.

PROJECT CONFERENCE CALLS: The contractor's key personnel will participate in weekly conference calls with the VA program office until production has started, at which time the frequency of the calls will progress to monthly. The VA will schedule the calls with the contractor.

PROGRESS REPORTS: The contractor shall provide VA with electronic weekly and monthly progress reports via email as specified. The reports are to be furnished as follows:

Weekly Progress Reports:

During the first 30 calendar days of production on the contract, the contractor shall submit weekly progress reports that cover all work completed during the previous week, and work to be accomplished during the subsequent week and month. The contractor's report shall identify accomplishments, actual vs. planned project schedule, project risks, quality and security issues and resolutions, escalation process for outstanding issues and remediation for any issues that cause the project to be delayed. The contractor shall submit the first report to VA within seven (7) calendar days after the pre-production meeting.

After retrieval of the first file(s), the weekly progress report shall include the following processing information:

- On time delivery percentage (for the reporting period and Fiscal Year To Date (FYTD)
- Number of cards requested (for the reporting period and FYTD)
- Total Number of cards mailed (for the reporting period and FYTD)
- Number of cards mailed by facility ID (for the reporting period and FYTD)
- Average Number of calendar days from card request file retrieval to mailing (for the reporting period and FYTD)
- Percentage of cards mailed on the day of card request file retrieval (for the reporting period)
- Percentage of cards mailed within 24 hours of card request file retrieval (for the reporting period)
- Percentage or cards mailed within 48 hours of card request file retrieval (for the reporting period)
- Number of cards created but not mailed due to poor card quality (for printing/variable imaging) upon inspection (for the reporting period and FYTD)
- Number of cards created and shipped to the appropriate VAMC due to poor photo quality upon inspection (results of rejected photo quality from VA furnished data files) (for the reporting period and FYTD)
- Number of cards mailed to the Facility address (other than rejects) with counts by facility number and overall total (for the reporting period and FY TD)

Monthly Progress Reports:

The contractor shall provide monthly progress reports that cover all work completed during the preceding month and shall present the work to be accomplished during the subsequent month and following quarter. The contractor's report shall identify accomplishments, actual vs. planned project schedule, project risks, quality and security issues and resolutions, escalation process for outstanding issues and remediation for any issues that cause the project to be delayed. The contractor shall submit the monthly progress reports to VA.

- On time delivery percentage (for the reporting period and Fiscal Year To Date (FYTD)
- Number of cards requested (for the reporting period and FYTD)
- Total number of cards mailed (for the reporting period and FYTD)
- Number of cards mailed by facility ID (for the reporting period and FYTD)
- Average number of calendar days from card request file retrieval to mailing (for the reporting period and FYTD)
- Percentage of cards mailed on the day of card request file retrieval (for the reporting period)
- Percentage of cards mailed within 24 hours of card request file retrieval (for the reporting period)
- Percentage or cards mailed within 48 hours of card request file retrieval (for the reporting period)
- Number of cards created but not mailed due to poor card quality (for printing/variable imaging) upon inspection (for the reporting period and FYTD)
- Number of cards created and shipped to the appropriate VAMC due to poor photo quality upon inspection (results of rejected photo quality from VA furnished data files) (for the reporting period and FYTD)
- Number of cards mailed to the Facility address (other than rejects) (for the reporting period and FYTD)
- Pull and Expedite: overnight shipping requests from VA Project Manager
- File and Image Destruction Question: The contractor shall report that all electronic files and media have been destroyed according to VA Security and Privacy Laws and Regulations
- Card Print Request Files (30 Day archive) - list of file names
- Acknowledgement Files (60 Day archive) - list of file names
- Mail Confirmation Files (60 Day archive) - list of file names
- Transmission Confirmation Files with Error Report
- Error Reports

SITE PRODUCTION VISITS: The VA will conduct on-site inspections of all production no less than annually. VA will schedule the visit no less than 48 hours in advance. VA will review quality management/quality control activities, risk management, security plans, and privacy compliance. *(See Attachment M (Facility Physical Security Checklist) and Attachment N (Facility Inspection Checklist.))* The contractor will conduct a facility card production tour to provide a security briefing, and assist the VA in sampling 100 of the current day's VHIC production.

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 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)	365
	(b)	70
	(c)	2
	(d)	1,747
	(e)	1,455
	(f)	364
	(g)	1,819
II.		1,819
III.		16

THIS PAGE IS INTENTIONALLY BLANK.

SECTION 4. - SCHEDULE OF PRICES

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

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

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

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

I. PRINTING/IMAGING, BINDING AND CONSTRUCTION: Prices offered must be all inclusive and include the cost of materials and operations (including proofs, prior to production samples, test samples, and paper) necessary for the printing/imaging, binding and construction listed in accordance with these specifications.

(a) *Daily makeready/setup charge .....$_____

*Contractor will be allowed only one (1) makeready/setup charge per calendar day. This combined charge shall include all materials and operations necessary to makeready and/or setup the contractor's equipment for the Veterans Identification Card mailers run each day. Invoices submitted with more than one makeready/setup charge per calendar day will be disallowed.

(b) VIC Legacy Card .....per 1,000 cards.....$_____

(c) Interim VHIC Card .....per 1,000 cards.....$_____

(d) WEDI VHIC Card .....per 1,000 cards.....$_____

(e) Carrier Sheet (Face only) ..... per 1,000 sheets.....$_____

(f) Carrier Sheet (Face and back)..... per 1,000 sheets.....$_____

(g) Mail-out Envelope, including cost of envelope..... per 1,000 sheets.....$_____

_____
(Initials)

II. 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 card mailers including cost of attaching card to carrier sheet, folding carrier sheet to required size in accordance with these specifications, insertion into mail-out envelope, and mailing, in accordance with these specifications.

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

III. PROGRESS REPORTS:

Progress Report .....per report.....$_____

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

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

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.

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)

Table of Contents

Executive Summary 1
Purpose 1
Scope 1
Attestation of Compliance 2
Action Plan for Non-compliance 4
Self-Assessment Questionnaire 5
Requirement 1: Install and maintain a firewall configuration 5
Requirement 2: VA Information Hosting, Operation, Maintenance or Use 6
Requirement 3: Use and regularly update antivirus software 6
Requirement 4: Implement Access Controls 7
Requirement 5: Conduct Risk Assessments 8
Requirement 6: Institute Information Security Protection 10
System and Communications Protection 10
System and Information Integrity 10
Physical Security 11
Requirement 7: Privacy Regulation for Storage of Veterans' Sensitive Information 12
Access to VA Information and VA Information Systems 12
Custodial Requirements 12
Security Incident Investigation 13
Training 13
Appendix A. References 15

Contractor Security Control Assessment (CSCA)

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 (CSCA)

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

Contractor Security Control Assessment (CSCA)

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)

VA INFORMATION PROTECTION

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

System and Information Integrity

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

Contractor Security Control Assessment (CSCA)

VA INFORMATION PROTECTION

Physical Security

Question	Response: (Select One) 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)

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

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.*

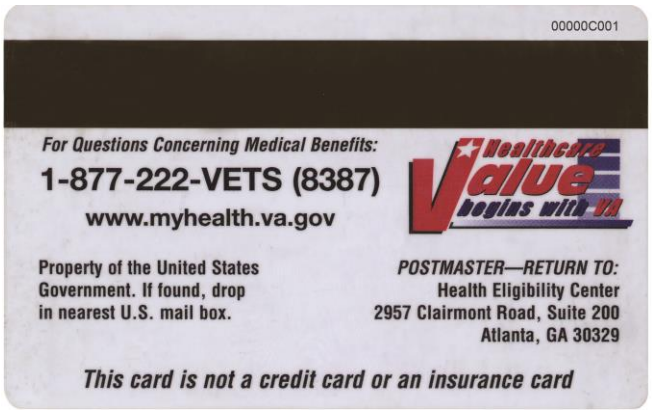
NIST SP 800-73, *Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV Card Application Namespace, Data Model and Representation, 2- End-Point PIV Card Application Interface, 3- End-Point PIV Client Application Programming Interface, 4- The PIV Transitional Data Model and Interfaces.*

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.*

ATTACHMENT D
VIC Legacy (Face and Back)



National Card Management Directory
SCHEMA GUIDE

Author: Ali Khawaja

Creation Date: April 5, 2004

Last Updated: March 4, 2011

Version: 3

Document Control

Change Record

Date	Author	Version	Change Reference
4/5/04	Michael Boone	1.0	Initial Version
5/26/05	Mike Boone	2.0	Adding attributes to support printing of POW and Purple Heart indicators on the card
6/1/05	Mike Boone	2.1	Adding pending status value for POW and Purple Heart indicators.
6/7/05	Mike Boone	2.2	Adding support for the VistA Imaging tracking id
3/4/11	Ali Khawaja	3	Update

Reviewers

Name	Position
Howell Russ	Project Manager
Michael Boone	Architect

Distribution

Copy No.	Name	Location

Contents

Document Control 2
Introduction 4
Purpose 4
Background 4
Veteran Class: dvancmdVeteran 5
Veteran Class: dvancmdCard 7

Introduction

Purpose

This schema guide describes the storage of data within the National Card Management Directory (NCMD).

Background

The NCMD houses data that is used to produce Veteran Identification Cards (VIC). The NCMD has been implemented with Microsoft's Active Directory LDAP data store. The Active Directory schema was extended with two classes: dvancmdVeteran and dvancmdCard. A single dvancmdVeteran object is created and stored in the LDAP for each veteran that has requested a VIC card. For each VIC card request a dvancmdCard object is created and stored in the LDAP. The attributes of these two classes are described below.

Veteran Class: dvancmdVeteran

The default Active Directory schema is extended to include a Veteran container for storing Veteran objects. The CN of a Veteran object is set using the veteran's SSN followed by a hyphen and the veteran's last name (e.g. CN=555443333-Smith). There is a one to many relationship with Card objects.

Field Name	*Type*	*Length*	*Index*	*Required to create record*	*Source*	*Send to card print vendor*	*Magnetic Stripe*	*Bar Code*	*Comments*
VET_NameFull	Varchar	30	Yes	Yes	PIMS (via PICS)	Yes	Magnetic Strip		VistA name field 3-30 characters w/ optional punctuation VistA truncating rules applied to format of Family_name,Given_name<space>Middle_name <space>Suffix(es)
VET_NamePrefix	Varchar	10	No	No	PIMS (via PICS)	No			Mr, Mrs, etc
VET_GivenName	Varchar	25	No	No	PIMS (via PICS)	No			First name
VET_MiddleName	Varchar	25		No	PIMS (via PICS)	No			Middle name "NMI" – no middle initial "NMN" – no middle name
VET_FamilyName	Varchar	35	Yes	Yes	PIMS (via PICS)	No			Last name
VET_NameSuffix	Varchar	10	No	No	PIMS (via PICS)	Yes			Jr., Sr,, etc
VET_SSN	Varchar	10	Yes	Yes	PIMS (via PICS)	Yes	Magnetic Strip	Bar Code	Must accommodate pseudo SSNs which have 9 numbers followed by a 'P'
VET_DateOfBirth	Date	8	No	Yes	PIMS (via PICS)	Yes	Magnetic Strip		Date of Birth Format of mmddyyyy
VET_ICN	Number	23	Yes	No (Required prior to card print request submission)	PIMS (via PICS) or directly from PIMS via HL7	Yes	Magnetic Strip		Number between 1 and 999999999999 If Card_PrintReleaseStatus initially set to 'P' then source was PICS. If Card_PrintReleaseStatus initially set to 'H' then source will be PIMS via HL7 message
VET_Picture	Binary	No li	No	Yes	PICS	Yes			JPG file

		m it							
VET_City	Varchar	50	No	Yes	PIMS (via PICS)	Yes			City 2-15 chars from VistA
VET_State	Varchar	30	No	Yes	PIMS (via PICS)	Yes			VistA 2 character state code
VET_Email	Varchar	10 0	No	No	PIMS (via PICS)	No			Email address
VET_Street1	Varchar	50	No	Yes	PIMS (via PICS)	Yes			Street address (line 1)
VET_Street2	Varchar	50	No	No	PIMS (via PICS)	Yes			Street address (line 2)
VET_Street3	Varchar	50	No	No	PIMS (via PICS)	Yes			Street address (line 3)
VET_ZIP	Varchar	10	No	Yes	PIMS (via PICS)	Yes			Zip code 5 numbers or 5 numbers followed by a hyphen and 4 additional numbers
VET_Service Connected	Boolean	1	No	Yes	PIMS (via PICS)	Yes	Magnetic Strip		True if service connected, otherwise False (Yes/No in VistA)
VET_ImageT rackingID	Varchar	10 0	No	No	PICS	No			PICS constructs this id to submit along with the photo to VistA Imaging

Note: Eligibility data is not retained in Veteran object. PIMS determines CARD_PrintReleaseStatus of child Card object based upon eligibility rules and national ICN availability.

Veteran Class: dvancmdCard

The default Active Directory schema is extended to include a Card container for storing Card objects. A Card object is named using the corresponding Veteran object name followed by a dash and a card sequence number.

Field Name	*Type*	*Len*	*Index*	*Required to create record*	*Source*	*Send to card print vendor*	*Comments*
CARD_CardID	**Varchar**	**64**	**Yes**	**Yes**	**PICS**	**Yes**	**Format of VET_SSN-VET_FamilyName-SequenceNumber**
CARD_Location	**Varchar**	**80**	**No**	**Yes**	**PIMS (via PICS)**	**No**	**Source facility name**
CARD_LocationNumber	**Varchar**	**7**	**Yes**	**Yes**	**PIMS (via PICS)**	**No**	**Source facility number**
CARD_VISN	**Varchar**	**200**	**Yes**	**Yes**	**PIMS (via PICS)**	**No**	**Source VISN name**
CARD_Station	**Varchar**	**25**	**No**	**Yes**	**PICS**	**No**	**Machine name**
CARD_Issuer	**Varchar**	**40**	**No**	**Yes**	**PICS**	**No**	**Full VistA user name of the card issuer**
CARD_IssuerNT	**Varchar**	**50**	**No**	**Yes**	**PICS**	**No**	**Windows network account of card issuer in format <domain>\<username>**
CARD_Status	**Varchar**	**12**	**Yes**	**Yes**	**PICS/NCMD**	**No**	**'Request', 'Processing', 'Active', 'Inactive'**
CARD_Version	**Varchar**	**4**	**No**	**No**	**PICS**	**No**	**Set to '2.0'**
CARD_Type	**Varchar**	**10**	**No**	**No**	**PICS**	**No**	**Set to 'PLAIN'**
CARD_Manufacturer	**Varchar**	**15**	**No**	**No**	**PICS**	**No**	**Set to 'PLAIN'**
CARD_ExpirationDate	**Date**	**8**	**No**	**No**		**No**	**Currently no value to be assigned Format of yyyymmdd**
CARD_StatusChangeDate	**Date**	**8**	**No**	**Yes**	**PICS/NCMD**	**No**	**Date of change in CARD_Status. Format of yyyymmdd**
CARD_StatusChangeBy	**Varchar**	**40**	**No**	**Yes**	**PICS/NCMD**	**No**	**Domain / username Set to 'NCMD' if due to daily server jobs.**

Field Name	*Type*	*Len*	*Index*	*Required to create record*	*Source*	*Send to card print vendor*	*Comments*
CARD_PrintReleaseStatus	Char	1	Yes	Yes	PIMS (via PICS) or directly from PIMS via HL7	No	'P' – request can be sent to Card Print Site for printing 'H' – request is being held awaiting an update from PIMS 'C' – request is cancelled 'S' – request has been sent to Card Print Site 'A' – Card Print Site has acknowledged receipt of the request 'M' – card has been mailed 'E' – error due to data integrity, record not sent to Card Print Site 'R' – record was rejected by the Card Print Site 'I' – ineligible for card/photo and data stored
CARD_WorkstationRequestDT	DateTime	14	Yes	Yes	PICS	No	DateTime of card workstation request Format of yyyymmddhhmmss
CARD_RequestFileDT	DateTime	14	Yes	No	NCMD	No	DateTime of creation of file request containing this record prior to shipment to vendor Format of yyyymmddhhmmss
CARD_RequestFileName	Varchar	17	Yes	No	NCMD	No	Name of file sent to card print vendor
CARD_AckReceiptDT	DateTime	14	No	No	NCMD	No	DateTime of creation of acknowledgement file from vendor showing receipt of this record Format of yyyymmddhhmmss
CARD_AckFileName	Varchar	20	No	No	NCMD	No	Name of initial confirmation file received from card print vendor
CARD_AcceptRejectCode	Numeric	14	No	No	NCMD	No	Used to report on error conditions that occurred when handling the request. 0 – Error condition did not occur 1 – Request rejected due to error condition Multiple error conditions are reported by the character position of a 0 or 1 in the string. The following 12 error codes are defined by position: Position 1 - Every card request shall be in a format that can be read by the card print vendor (images in standard jpg format).

Field Name	*Type*	*Len*	*Index*	*Required to create record*	*Source*	*Send to card print vendor*	*Comments*
							Position 2 - Every card request shall have an associated picture with a matching image file name. **Position 3 - Every card request shall have a valid SSN or pseudo SSN (10 digit claim number) (nine digits plus optional alpha for the pseudo SSN).** **Position 4 - Every card request shall have a valid date of birth in MMDDYYYY format with valid month/day combinations.** **Position 5 - Every card request shall have a valid first and last name (format should have no more than 30 characters).** **Position 6 - Every card request shall have a valid facility id (3 digits plus up to 4 optional alphanumeric characters).** **Position 7 - Every card request shall have a valid card id.** **Position 8 - Every card request shall have a valid service connected indicator (format either Y or N).** **Position 9 - Every card request shall have a valid street address (as determined by CASS).** **Position 10 - Every card request shall have a valid city (as determined by CASS).** **Position 11 - Every card request shall have a valid state (as determined by CASS).** **Position 12 - Every card request shall have a valid zip code (as determined by CASS).** **Position 13 – Every card request shall have a valid**

Field Name	*Type*	*Len*	*Index*	*Required to create record*	*Source*	*Send to card print vendor*	*Comments*
							POW indicator ('Y', 'N', 'P', or 'U'). Position 14 – Every card request shall have a valid Purple Heart indicator ('Y', 'N', 'P', or 'U').
CARD_CompletedDT	DateTime	14	Yes	No	NCMD	No	DateTime of card mailing. Format of yyyymmddhhmmss
CARD_CompletedFileName	Varchar	20	No	No	NCMD	No	Name of final confirmation file from card print vendor
CARD_TransmitAttempts	Number	2	No	No	NCMD	No	Number of transmissions to card print vendor
CARD_VetDFN	Varchar	200	No	Yes	PIMS (via PICS)	No	Unique identifier, within facility, of the veteran VistA PATIENT file record number
Card_POW	Char	1	No	Yes	PIMS via HL7	Yes	'Y'=POW status 'N'=not a POW 'P'=pending 'U'=Unknown
Card_PH	Char	1	No	Yes	PIMS via HL7	Yes	'Y'=a Purple Heart recipient 'N'=not a Purple Heart recipient 'P'=pending 'U'=Unknown
Card_ClientVersion	Char	15	Yes	Yes	PICS	No	Version of the client software that submitted the request
Card_reissue	Char	1	No	No	PICS	No	Set to Y if automatic reissuance

ATTACHMENT F
Interim VHIC (Face)

ATTACHMENT G
Interim VHIC/WEDI VHIC (Back)

This is not a credit card 76637C003/CP33293

For Questions Concerning Health Benefits:

1-877-222-VETS (8387)

www.va.gov/healthbenefits

Veterans Crisis Line 1-800-273-8255

Foreign Medical Program 1-877-345-8179

In emergency call 911 or go to nearest medical facility

Report any emergency care to your VA treatment team within 24 hours.

For questions concerning non-health care VA benefits 1-800-827-1000

Property of the U.S. Government. If found, drop in nearest U.S. mail box.

POSTMASTER - RETURN TO:

Health Eligibility Center, 2957 Clairmont Road, Suite 200, Atlanta, GA 30329

VHIC Card Standards

1. Face of Card Requirements

   1.1 The barcode shall no longer store the SSN.

   1.2 The barcode shall store the unique card number.

   1.3 The barcode shall store the EDIPI.

   1.4 The barcode shall be DoD Compliant Code 3 of 9 Barcode Layout as specified in 2.1.2.3 below.

   1.5 Card face shall have a symbol or letter to designate it as a pilot card. Symbol or letter shall only be for cards produced in phase 1 of the pilot for the eight (8) pilot sites.

2. DoD Compliant Code 3 of 9 Barcode Layout

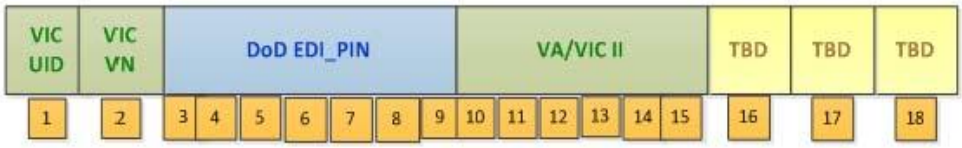
   2.1 The DoD compliant layout shall comply with the fomat listed below with characters 16, 17 and 18 not used.

   2.2 The data elements will consist of the EDIPI then the unique card number.

   2.3 DoD Compliant Barcode Layout

The following diagram depicts the barcode layout for the VIC Card.

VA/VIC CARD BAR CODE 39 FORMAT (18 CHARACTERS)



VIC UID = %
VIC VN = Version #
DoD EDI_PIN (compressed) (Base 32^2 coding of a DEERS-assigned numeric 10-digit numeric identifier)
VA/VIC II = VIC Card Number (Compressed)

Value	Decimal		Value	Decimal
0	0		G	16

1	1		H	17
2	2		I	18
3	3		J	19
4	4		K	20
5	5		L	21
6	6		M	22
7	7		N	23
8	8		O	24
9	9		P	25
A	10		Q	26
B	11		R	27
C	12		S	28
D	13		T	29
E	14		U	30
F	15		V	31

Base 32 values and decimal equivalent

3. Magnetic Stripe

3.1 The magnetic stripe shall be located on the back of the card and shall comply with Section 12 of the WEDI Health ID Card Implementation Guide standards.

3.2 The magnetic stripe shall include 3 high-coercivity, machine-readable tracks.

3.3 All card data required on the magnetic stripe shall be assigned to one of these 3 tracks.

3.4 The magnetic stripe's variable data will not be modified by VA applications.

4 Data structure for the Magnetic Stripe

4.1 Encoded data for Track 3 is detailed in the table below. Note an LRC error detection character will be included within the character count of 82 maximum. An LRC immediately follows the end sentinel of each Track. A magnetic stripe card reader checks the LRC to ensure accuracy but does not send the LRC along with the data. LRC calculation is specified in ISO/IEC 7811-6. Refer to underlying standard, INCITS 284.

Data	Max Length	Fixed/Variable	Format
Start Sentinel	1	Fixed	%
Format Code	2	Fixed	WH
Card Issuer Identifier	10	Fixed	Numeric
Cardholder ID Number (EDIPI)	10	Fixed	Numeric
Field Separator	1	Fixed	^

Cardholder Name	36	Variable	A/N composite
Field Separator	1	Fixed	^
Qualifier Code	2	Fixed	DH
Card Expires	8	Fixed	ccyymmdd
End Sentinel	1	Fixed	?
Longitudinal Redundancy Check	1	Fixed	Any 7-bit combination

NOTE: Section highlighted in yellow for Card Expires date is future enhancement to VA VHIC application. Data will be added in future release. Until data is transferred from VA contractor shall enter the date the file is received as the expiration date for VHIC WEDI Card only. Once VA begins transmitting the date contractor will utilize VA provided date. Contractor shall receive 30 day notice of transition.

4.2 ***Start Sentinel***. Many card reader software drivers change the % start sentinel to # in the data sent to the application.

4.3 ***Format code***. This 2-character code indicates the structure of machine-readable data on the card. The *same* standard format is used regardless of technology. Allows computer to be able to determine the card is a health ID card.

4.4 ***Variable Data Element Length and Delimiters***. Variable data elements are left justified and not padded with extra spaces to the right. The card issuer shall ensure that no data element contains the field separator character ("^") or End Sentinel ("?").

4.5 ***Card issuer identifier***, 10-digit ISO Standard U.S. Healthcare Identifier without "80840" prefix.

4.6 ***Cardholder identifier***. The Electronic Data Interchange Personal Identifier (EDIPI) shall be used.

4.7 ***Cardholder name***. Includes hyphen or apostrophe when significant as in "JONES-SMITH" or "O'NEILL". The machine-readable cardholder name may not include accented characters Accented characters shall be replaced by their base character values. Cardholder name uses composite name format consisting of Surname "/" Given Name "/" Middle Name "/" Suffix, in which "/" is delimiter between components of the name. For example, "JOHN Q PUBLIC JR" is "PUBLIC/JOHN/Q/JR". Use surname when a person has only a single name. No component may contain the delimiter, "/". A double middle name is 1 component. Remove leading and trailing spaces from all components. Empty fields are null. For example, "JOHN PUBLIC JR" is "PUBLIC/JOHN//JR".

Do not end with delimiters. For example, "JOHN PUBLIC" (no middle name, no suffix) is "PUBLIC/JOHN".

4.8 ***Truncation***. Use the following requirements for name truncation. This sequence retains the suffix, at least one initial for the given or middle name, whichever appears most important, and as much of the surname as space permits. If the given name is more than an initial, truncate the middle name from the right as needed but leave at least the middle initial. Then if the name still exceeds the space, truncate the given name from the right as needed but leave at least its initial. If the name still exceeds the space, eliminate the middle initial. If the given name began as only an initial, truncate the middle name from the right as needed but leave at least the middle initial. If the name still exceeds the space, eliminate the given name initial. If both the given and middle names began as initials or empty, eliminate the middle initial. If the name still exceeds the space, truncate the surname from the right as needed until the name fits.

4.9 Encoded data for Track 1 is detailed in the table below.

Data	Max Length	Fixed/Variable	Format
Start Sentinel	1	Fixed	%
Unique Card Number	9	Fixed	Numeric
Field Separator	1	Fixed	^
Integrated Control Number (ICN)	17	Fixed	Alphanumeric
End Sentinel	1	Fixed	?

4.10 ***Start Sentinel Character sent to Application for Track 3 Magnetic Stripe20.*** The start sentinel that is physically on the card is "%" for Track 3, and the LRC is the last character on the track. When a card reader reads the card, it checks the LRC. In the data stream sent to the application, the card reader may change the Track 3 start sentinel from "%" to "#", to indicate to the application the start of Track 3, and it removes the LRC.

4.11 The start and end sentinels that are physically encoded on the card for all three tracks are:

Track Start Sentinel End Sentinel
Track 1 (7-bit alphanumeric) % ?
Track 2 (5-bit numeric) ; ?
Track 3 (7-bit alphanumeric) % ?

4.12 ***Physical View***: The following illustrates physical encoding of the magnetic stripe for Track 3 in which Tracks 1 and 2 are null:

Track 1 (7-bit alphanumeric) %?x
Track 2 (5-bit numeric) ;?x
Track 3 (7-bit alphanumeric)
%WH9210567898XJBH3AB572^PUBLIC/JOHN/Q^DB195805

17?x
[where x is the LRC for each track]

4.13 ***Application View***: The card reader software driver converts the data to 8-bit ASCII and sends it to the application as a single character stream. and it may change the Track 3start sentinel from "%" to "#":

Track 1 (8-bit ASCII) %?
Track 2 (8-bit ASCII) ;?
Track 3 (8-bit ASCII)
#WH9210567898XJBH3AB572^PUBLIC/JOHN/Q^DB195805
17?

5 Applicable Standards

WEDI Standards: The Workgroup for Electronic Data Interchange (WEDI) was established in 1991 in response to a challenge from then Secretary of Health and Human Services, Louis Sullivan, MD. The challenge was to bring together a consortium of leaders within the Healthcare industry to identify practical strategies for reducing administrative costs in Healthcare through the implementation of EDI. WEDI quickly became a major advocate in promoting the acceptance and implementation of the standardization of administrative and financial health care data. The Health Identification Card Implementation Guide, Version 1.1, dated February 16, 2011 shall be used for reference.

ATTACHMENT I
WEDI VHIC (Face)

Revised 7 June 2005
Version 2.1

Attachment B
VIC Card SOW
Print File Specification
June 7, 2005

Change Record

Date	Author	Version	Change Reference
4/5/04	Mike Boone	1.0	Initial Version
5/26/05	Mike Boone	2.0	Adding fields to support version 2 of PICS. POW, Purple Heart and service connected indicators will be printed on the card
6/7	Mike Boone	2.1	Added pending value for POW and Purple Heart fields

Card Print Request file format

Each card print request file transferred to the Card Print Site will contain a header record and a trailer record. Both the header and trailer records identify the name of the file, the date/time stamp of the file and the number of records in the file.

The header record also contains 8 fields that specify a special message that will occupy 8 lines on the card carrier. If no special text is to be placed on the card carrier these fields will contain no characters. Any card request records follow the header record.

All records will be in variable length, tab de-limited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control codes 0x000D and 0x000A).

Record layouts are contained in tables 1, 2 and 3.

Table 1 – Header record

Header Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'H' for header
File Name	Varchar	13	'VIC' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VIC200401091)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time
Count	Number	9	Count of the number of records in this file
Card carrier message line 1	Varchar	60	Line 1 of the special text section on the card carrier.
Card carrier message line 2	Varchar	60	Line 2 of the special text section on the card carrier.
Card carrier message line 3	Varchar	60	Line 3 of the special text section on the card carrier.
Card carrier message line 4	Varchar	60	Line 4 of the special text section on the card carrier.
Card carrier message line 5	Varchar	60	Line 5 of the special text section on the card carrier.
Card carrier message line 6	Varchar	60	Line 6 of the special text section on the card carrier
Card carrier message line 7	Varchar	60	Line 7 of the special text section on the card carrier
Card carrier message line 8	Varchar	60	Line 8 of the special text section on the card carrier
File version number	Varchar	2	The version of the specification used to produce this file.

Table 2 – Card Request Record

Data Record Field	Data type	Max Length	Loaded on Mag-stripe	Barcode	Comments
Record Type Indicator	Char	1			'D' for data
Name	Varchar	30	X		Format on card will be Last, First<space>Middle<space> Suffix(es)
Social Security Number	Varchar	10	X	X	Format accounts for both normal SSNs as well as C numbers.
DOB	Date	8	X		Format of mmddyyyy
ICN	Number	12	X		National Integration Control Number Number between 1 and 999999999999
Street Address [Line 1]	Varchar	35			
Street Address [Line 2]	Varchar	30			
Street Address [Line 3]	Varchar	30			
City	Varchar	30			
State	Char(2)	2			
ZIP+4	Varchar	10			5 numbers or 5 numbers followed by a hyphen and 4 additional numbers
Service Connected	Char	1	X		An indicator if the veteran is non-service connected or service connected. N = non-service connected, Y = service connected
Facility ID	Varchar	7			3 Numbers w/optional 4 AlphaNumeric Number assigned to the facility that originated the card request. Used to locate the facility mailing address if veteran mailing address does not pass CASS validation.
Image file name	Varchar	53			File name of the veteran photo for the card request. e.g. *SSN-LastName-SequenceNumber.jpg*

Data Record Field	Data type	Max Length	Loaded on Mag-stripe	Barcode	Comments
Card ID	Varchar	49			Unique identifier of the card request e.g. *SSN-LastName-SequenceNumber*
Addressable Name	Varchar				VistA name components concatenated in format Prefix<space>FirstName<space>MI<space>LastName<space>Suffix
POW Indicator	Char	1			Valid values are: 'Y'=POW 'N'=not a POW 'U'=Unknown The POW indicator will be printed on the card only if the value is 'Y'.
PH Indicator	Char	1			Valid values are: 'Y'=a Purple Heart recipient 'N'=not a Purple Heart recipient 'U'=Unknown The Purple Heart indicator will be printed on the card only if the value is 'Y'.

Table 3 – Trailer record

Trailer Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'T' for trailer
File Name	Varchar	13	'VIC' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VIC200401091)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time
Count	Number	9	Count of the number of records in this file
File version number	Varchar	2	The version of the specification used to produce this file.

			specification.

Sample Card Print Request file

H<TAB>VIC200401091<TAB>20040109203015<TAB>2<TAB>Text for line 1 of message.
<TAB><TAB>Text for line 3 of message.<TAB><TAB><TAB><TAB><TAB><CR><LF>
D<TAB>Doe, John William<TAB>222334444<TAB>06151930<TAB>1001178082<TAB>123
Main Street<TAB><TAB><TAB>AnyTown<TAB>AnyState<TAB>12345-
1234<TAB>Y<TAB>123<TAB>222334444-Doe-1.jpg<TAB>222334444-Doe-1<TAB>John
Willian Doe<TAB>Y<TAB>Y<CR><LF>
D<TAB>Smith, Sally <TAB>333884444<TAB>07011970<TAB>2158977564<TAB>123 Center
Ave.<TAB><TAB><TAB>AnyTown<TAB>AnyState<TAB>55555-
4444<TAB>Y<TAB>123<TAB>333884444-Smith-2.jpg<TAB>333884444-Smith-2<TAB>Sally
Smith<TAB>U<TAB>U<CR><LF>
T<TAB>VIC200401091<TAB>20040109203015<TAB>2<CR><LF>

1. Card Print Request Acknowledgement file format

Each card print request file transferred to the Card Print Site will be responded to with a card print request acknowledgement file. The acknowledgement file will contain a header record and a trailer record that identifies the name of the file, date/time stamp of the file, the number of records in the file, and the card print request file that is being acknowledged. If a corrupt card print request file cannot be processed, the acknowledgement file should contain a null data record and a header and trailer specifying a record count of zero.

Each record will be in variable length, tab de-limited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control code 0x000D and 0x000A).

Record layouts are contained in tables 5, 6, and 7.

Table 5 – Acknowledgement File Header

Header Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'H' for header
File Name	Varchar	16	'VICACK' concatenated with a date stamp of format yyyymmdd date and a sequence number (e.g. VICACK200401091)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time
Card Request File Name	Varchar	13	Name of the original Card Print Request file transmitted from NCMD. The acknowledgement file is in response to this file. (e.g. VIC200319201)
Count	Number	9	Count of the number of records in

			this file

Table 6 - Acknowledgement File Data

Data Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'D' for Data
Card ID	Varchar	49	Unique identifier for the card request
Card Request Accept/Reject Code	Varchar		Denotes card request acceptance or rejection. 0 – Error condition did not occur 1 – Request rejected due to error condition Multiple error conditions are reported by the character position of a 0 or 1 in the string. The following 12 error codes are defined by position: Position 1 - Every card request shall be in a format that can be read by the card print vendor (images in standard jpg format). Position 2 - Every card request shall have an associated picture with a matching image file name. Position 3 - Every card request shall have a valid SSN or pseudo SSN (10 digit claim number) (nine digits plus optional alpha for the pseudo SSN). Position 4 - Every card request shall have a valid date of birth in MMDDYYYY format with valid month/day combinations. Position 5 - Every card request shall have a valid first and last name (format should have no more than 30 characters). Position 6 - Every card request shall have a valid facility id (3 digits plus up to 4 optional alphanumeric characters). Position 7 - Every card request shall have a valid card id.

			Position 8 - Every card request shall have a valid service connected indicator (format either Y or N). Position 9 - Every card request shall have a valid street address (as determined by CASS). Position 10 - Every card request shall have a valid city (as determined by CASS). Position 11 - Every card request shall have a valid state (as determined by CASS). Position 12 - Every card request shall have a valid zip code (as determined by CASS). Position 13 – Every card request shall have a valid POW indicator Valid data are: 'Y'=POW 'N'=Not a POW 'U'=Unknown Position 14 – Every card request shall have a valid Purple Heart indicator. Valid data are: 'Y'=Purple Heart recipient 'N'=not a Purple Heart recipient 'U'=Unknown

Table 7 – Acknowledgement File Trailer

Trailer Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'T' for trailer
File Name	Varchar	16	VICACK concatenated with a date stamp of format yyyymmdd and a sequence number (VICACK200319201)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time
Card Request File Name	Varchar	13	Name of the original Card Print Request file transmitted from NCMD. The acknowledgement file is in response to this file. (e.g. VIC200319201)
Count	Number	9	Count of the number of records in

			this file

Sample Card Print Request Acknowledgement file

H<TAB>VICACK200401091<TAB>20040109221530<TAB>VIC200401091<TAB>2<CR><LF>
D<TAB>222334444-Doe-1<TAB>00000000010100<CR><LF>
D<TAB>333884444-Smith-2<TAB>00000000000000<CR><LF>
T<TAB>VICACK200401091<TAB>20040109221530<TAB>VIC200401091<TAB>2<CR><LF>

2. Mail Confirmation file format

The Card Print Site will provide a mail confirmation file for cards that have been mailed. The file will contain a header record and a trailer record that identifies the name of the file, date/time stamp of the file and the number of records in the file.

Each record will be in variable length, tab de-limited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control code 0x000D and 0x000A).

Record layouts are contained in tables 8, 9, and 10.

Table 8 –Mail Confirmation Header Record

Header Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'H' for header
File Name	Varchar	16	'VICCOM' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICCOM200319201)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time
Count	Number	9	Count of the number of records in this file

Table 9 - Mail Confirmation File Data

Data Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'D' for Data
Card Request File Name	Varchar	16	Name of the original Card Print Request file transmitted from NCMD. (e.g. VIC200319201)
Card Request File Creation Time Stamp	DateTime	14	Date/time stamp of the original Card Print Request file transmitted from NCMD. Format is YYYYMMDDHHMMSS.

Card ID	Varchar	49	Unique identifier for the card request
Mail Date/Time stamp	DateTime	14	Date/time stamp of card mailing to the veteran or medical center. Format is YYYYMMDDHHMMSS using 24 hour time.

Table 10 – Mail Confirmation File Trailer

Trailer Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'T' for trailer
File Name	Varchar	16	'VICCOM' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICCOM200319201)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time
Count	Number	9	Count of the number of records in this file

Sample Mail Confirmation file

H<TAB>VICCOM200401121<TAB>20040112095022<TAB>2<CR><LF>
D<TAB>VIC200401091<TAB>20040109203015<TAB>222334444-Doe-1<TAB>20040112082010<CR><LF>
D<TAB>VIC200401091<TAB>20040109203015<TAB>333884444-Smith-2<TAB>20040112082010<CR><LF>
T<TAB>VICCOM200401121<TAB>20040112095022<TAB>2<CR><LF>

Revised 30 April 2013
Version 3.8

Department of Veterans Affairs

Veteran Identification Card (VICE)
VIC Enhancement

Print File Specification (Draft)

Change Record

Date	Author	Version	Change Reference
4/5/2004	Mike Boone	1.0	Initial Version
5/26/2005	Mike Boone	2.0	Adding fields to support version 2 of PICS. POW, Purple Heart and service connected indicators will be printed on the card
6/7/2005	Mike Boone	2.1	Added pending value for POW and Purple Heart fields
6/14/2012	Randy Sims	3.0	VIC-E version
6/29/2012	David Green	3.1	Added base-32 fields for barcode and magnetic stripe
7/3/2012	David Green	3.2	Revisions to specification based upon meeting w/print vendor
7/5/2012	David Green	3.3	Revisions to specification based upon feedback from print vendor
7/8/2012	David Green	3.4	Added Second Member Benefit Plan ID (Formatted) field
7/23/2012	David Green	3.5	Updated the sample request file to reflect recent specification changes
8/9/2012	David Green	3.6	Corrections added (mostly to error codes)
3/26/2013	Linda Allen	3.7	Changed size of the ICN from 12 to 17 characters and Member Benefit Plan ID (unformatted) to 10 characters, error codes for Table 6 were incomplete: Position 3 was supposed to be EDIPI not Card ID.
4/30/2013	Mike Walker	3.8	Updated for errors found during testing: Table 2, first occurrence of member benefit plan ID should be unformatted, 10 characters; Table 6, Acknowledge file, card request accept/reject code (field 6, card id) validation was not well defined; clarified. Merged duplicate changes made by Linda Allen.

DRAFT

Card Print Request file format

Each card print request file transferred to the Card Print Site will contain a header record and a trailer record. Both the header and trailer records identify the name of the file, the date/time stamp of the file and the number of records in the file. Header and Trailer records are to be present, even if there are no card requests for the given day.

The header record also contains 8 fields that specify a special message that will occupy 8 lines on the card carrier. If no special text is to be placed on the card carrier these fields will contain no characters. Any card request records follow the header record.

All records will be in variable length, tab de-limited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control codes 0x000D and 0x000A).

Record layouts are contained in tables 1, 2 and 3.

Table 1 – Header record

Header Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'H' for header (e.g. H)
File Name	Varchar	14	'VICE' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICE201206141)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time (e.g. 20120614095022)
Card carrier message line 1	Varchar	60	Line 1 of the special text section on the card carrier.
Card carrier message line 2	Varchar	60	Line 2 of the special text section on the card carrier.
Card carrier message line 3	Varchar	60	Line 3 of the special text section on the card carrier.
Card carrier message line 4	Varchar	60	Line 4 of the special text section on the card carrier.
Card carrier message line 5	Varchar	60	Line 5 of the special text section on the card carrier.
Card carrier message line 6	Varchar	60	Line 6 of the special text section on the card carrier
Card carrier message line 7	Varchar	60	Line 7 of the special text section on the card carrier
Card carrier message line 8	Varchar	60	Line 8 of the special text section on the card carrier
Count	Number	9	Count of the number of records in this file (e.g. 10)
File version number	Varchar	2	The version of the specification used to produce this file. (e.g. 01)

DRAFT

Table 2 – Card Request Record

Data Record Field	Data type	Max Length	Loaded on Mag-stripe	Barcode	Comments
Record Type Indicator	Char	1			'D' for data (e.g. D)
Card Version Number	Varchar	3			Version of the card. (e.g. *3.0)*
Name	Varchar	36			Format on card will be First Name<space>Middle Initial<space>Last Name<space>Suffix(es) (e.g. JOHN W DOE)
Name -- Mag Stripe	Varchar	36	X		Format on card will be Last Name<slash>First Name<Slash>Middle Initial (e.g. DOE/JOHN/W)
EDIPI	Varchar	10	X		New identifier from DoD that replaces the Social Security Number. (e.g. 1234567890)
EDIPI Base 32	Varchar	10		X	New identifier from DoD that replaces the Social Security Number, in Base 32 format. (e.g. 14PC0MI)
DOB	Date	8			Format of yyyymmdd (WEDI standard) (e.g. 19580517)
ICN	Number	17	X		National Integration Control Number Number between 1 and (e.g. 99999999999999999)
Member Benefit Plan ID	Varchar	10	X		Unformatted Benefit Plan ID (WEDI standard) (e.g. 1111222333)
Member Benefit Plan ID Formatted	Varchar	12			Formatted Benefit Plan ID {Future Use} (e.g. 1111 222 333)
Street Address [Line 1]	Varchar	35			
Street Address [Line 2]	Varchar	30			
Street Address [Line 3]	Varchar	30			

DRAFT

Data Record Field	Data type	Max Length	Loaded on Mag-stripe	Barcode	Comments
City	Varchar	30			
State	Char(2)	2			
ZIP+4	Varchar	10			5 numbers or 5 numbers followed by a hyphen and 4 additional numbers (e.g. 23061-3200)
Service Connected	Char	1			An indicator if the veteran is non-service connected or service connected. N = non-service connected, Y = service connected (e.g. Y)
Facility ID	Varchar	7			3 Numbers w/optional 4 AlphaNumeric Number assigned to the facility that originated the card request. Used to locate the facility mailing address if veteran mailing address does not pass CASS validation.
Image file name	Varchar	53			File name of the veteran photo for the card request. e.g. card id-*LastName-SequenceNumber.jpg* (e.g. 244-Smith-2.jpg)
Card ID	Varchar	40			Unique identifier of the card request (e.g. 1000563)
Card ID Base 32	Varchar	40	X	X	Unique identifier of the card request in base 32 format (e.g. UH3J)
Card Issuance Counter	Number	2			Number of times a card has been issued to the veteran. From 1 to 99. (e.g. 5)
Addressable Name	Varchar				VistA name components concatenated in format Prefix<space>FirstName<space>Middle Name<space>LastName<space>Suffix (e.g. John William Doe)

DRAFT

Data Record Field	Data type	Max Length	Loaded on Mag-stripe	Barcode	Comments
POW Indicator	Char	1			Valid values are: 'Y'=POW 'N'=not a POW 'U'=Unknown The POW indicator will be printed on the card only if the value is 'Y'.
PH Indicator	Char	1			Valid values are: 'Y'=a Purple Heart recipient 'N'=not a Purple Heart recipient 'U'=Unknown The Purple Heart indicator will be printed on the card only if the value is 'Y'.
MOH Indicator	Char	1			Valid values are: 'Y'=a Medal of Honor recipient 'N'=not a Medal of Honor recipient 'U'=Unknown The Medal of Honor indicator will be printed on the card only if the value is 'Y'

Table 3 – Trailer record

Trailer Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'T' for trailer
File Name	Varchar	14	'VICE' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICE201206141)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using

DRAFT

			24 hour time (e.g. 20120614095022)
Count	Number	9	Count of the number of records in this file (e.g. 10)
File version number	Varchar	2	The version of the specification used to produce this file specification. (e.g. 01)

DRAFT

Sample Card Print Request file

```
H	VICE201206141	20120614095022	Card carrier message line 1.	Card
carrier message line 2.	Card carrier message line 3.	Card carrier message line 4.	Card
carrier message line 5.	Card carrier message line 6.	Card carrier message line 7.	Card
carrier message line 8.	10	01
D	3.0	JAMES MALLARD	MALLARD/JAMES	1684266983	1I67NV7
	19801223	136684741536	NOGF236841	NOGF 236 841	4847 Tully Street
	Livonia	MI	48150	Y	315	1684266983-Mallard-1.jpg	654
	KE	2	James Mallard	Y	N	N
D	3.0	JOSEPH R SMITH	SMITH/JOSEPH/R	5477881368	5383LGO
	19750825	115987456325	YUNS456952	YUNS 456 952	1342 Duncan Avenue
	Garden City	NY	11530	Y	148	5477881368-Smith-2.jpg
	125	3T	15	Joseph Richard Smith	Y	Y	N
D	3.0	FRANK S JAMES	JAMES/FRANK/S	1689945211	1IBL13R
	19651208	356487412395	VAWE782395	VAWE 782 395	4761 Ashwood Drive
	Spirit Lake	IA	51360	Y	669	1689945211-James-3.jpg
	2214	256	4	Frank Samual James	Y	Y	Y
D	3.0	SUSAN MCCLOUD	MCCLOUD/SUSAN	6682478965	674T2BL
	19870624	491687153698	PMIN415987	PMIN 415 987	2032 Colony Street
	Madison	CT	6443	Y	457	6682478965-McCloud-4.jpg
	146	4I	6	Susan McCloud N	N	Y
D	3.0	WENDY E SAMSON	SAMSON/WENDY/E	1648995214	1H4JASE
	19550403	894677412235	VBIY147896	VBIY 147 896	1345 Emeral Dreams
Drive	Gardner	IL	60424	Y	241	1648995214-Samson-
5.jpg	8426	87A	23	Wendy Elizabeth Samson	N	Y	N
D	3.0	THOMAS L YANNER	YANNER/THOMAS/L	9877462357	96BS7AL
	19770316	446988523311	TIUN285396	TIUN 285 396	2808 Hartway Street
	Rapid City	SD	57702	Y	364	9877462357-Yanner-6.jpg
	25	P	25	Thomas Lenard Yanner N	N	N
D	3.0	JESICA MILHOUSE	MILHOUSE/JESICA	4698521765	4C0RG55
	19480627	312235478945	LPOM741295	LPOM 741 295	1458 Creekside Lane
	San Luis Obispo	CA	93401	Y	124	4698521765-Milhouse-
7.jpg	1588	1HK	1	Jesica Milhouse N	U	U
D	3.0	BENJAMIN D FLETCHER	FLETCHER/BENJAMIN/D	4658953147
	4AR3UTR	19620118	153369852147	VAZZ164987	VAZZ 164 987	2496
Simons Hollow Road	Pittston PA	18640	Y	142	4658953147-
Fletcher-8.jpg	1348	1A4	44	Benjamin David Fletcher	Y	U	N
D	3.0	JUSTIN P KASINSKY	KASINSKY/JUSTIN/P	7142896354	6KRVSN2
	19680903	142536987456	IUNV712584	IUNV 712 584	2327 Romrog Way
	Grand Island	NE	68801	Y	168	7142896354-Kasinsky-9.jpg
	39941	1705	12	Justin Patrick Kasinsky	Y	U	N
D	3.0	JACOB W BLACKBURN	BLACKBURN/JACOB/W	9456385412
	8PQ9VC4	19880306	451236987452	HGSD396584	HGSD 396 584	2712
Hiddenview Drive	Philadelphia	PA	19106	Y	194
	9456385412-Blackburn-10.jpg	2584	2GO	17	Jacob William Blackburn
	Y	U	N
T	VICE201206141	20120614095022	10	01
```

1. Card Print Request Acknowledgement file format

Each card print request file transferred to the Card Print Site will be responded to with a card print request acknowledgement file. The acknowledgement file will contain a header record and a trailer record that identifies the name of the file, date/time stamp of the file, the number of records in the file, and the card print request file that is being acknowledged. If a corrupt card print request file cannot be processed, the acknowledgement file should contain a null data record and a header and trailer specifying a record count of zero.

Each record will be in variable length, tab de-limited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control code 0x000D and 0x000A).

Record layouts are contained in tables 5, 6, and 7.

Table 5 – Acknowledgement File Header

Header Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'H' for header (e.g. H)
File Name	Varchar	17	'VICEACK' concatenated with a date stamp of format yyyymmdd date and a sequence number (e.g. VICEACK201206141)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time (e.g. 20120614095022)
Card Request File Name	Varchar	14	Name of the original Card Print Request file transmitted from VIC-E. The acknowledgement file is in response to this file. (e.g. VICE201206141)
Count	Number	9	Count of the number of records in this file (e.g. 10)

Table 6 - Acknowledgement File Data

Data Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'D' for Data
Card ID	Varchar	40	Unique identifier for the card request
Card Request Accept/Reject Code	Varchar		Denotes card request acceptance or rejection. 0 – Error condition did not occur 1 – Request rejected due to error

DRAFT

			condition Multiple error conditions are reported by the character position of a 0 or 1 in the string. The following 15 error codes are defined by position: Position 1 - Every card request shall be in a format that can be read by the card print vendor (images in standard jpg format). Position 2 - Every card request shall have an associated picture with a matching image file name. Position 3 - Every card request shall have a valid EDIP (at least 1 alpha numeric character) Position 4 - Every card request shall have a valid first and last name (format should have no more than 36 characters). Position 5 - Every card request shall have a valid facility id (3 digits plus up to 4 optional alphanumeric characters). Position 6 - Every card request shall have a valid card id (at least 1 digit) Position 7 - Every card request shall have a valid service connected indicator (format either Y or N). Position 8 - Every card request shall have a valid street address (as determined by CASS). Position 9 - Every card request shall have a valid city (as determined by CASS). Position 10 - Every card request shall have a valid state (as determined by CASS). Position 11 - Every card request shall have a valid zip code (as determined by CASS). Position 12 – Every card request

DRAFT

			shall have a valid POW indicator Valid data are: 'Y'=POW 'N'=Not a POW 'U'=Unknown Position 13 – Every card request shall have a valid Purple Heart indicator. Valid data are: 'Y'=Purple Heart recipient 'N'=not a Purple Heart recipient 'U'=Unknown Position 14 – Every card request shall have a valid Medal of Honor indicator. Valid data are: 'Y'=Medal of Honor recipient 'N'=not a Medal of Honor recipient 'U'=Unknown Position 15 – Every card request shall have a valid date of birth in YYYYMMDD format with valid month/day combinations.

Table 7 – Acknowledgement File Trailer

Trailer Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'T' for trailer (e.g. T)
File Name	Varchar	17	VICEACK concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICEACK201206141)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time (e.g. 20120614095022)
Card Request File Name	Varchar	14	Name of the original Card Print Request file transmitted from VIC-E. The acknowledgement file is in response to this file. (e.g. VICE201206141)
Count	Number	9	Count of the number of records in this file (e.g. 10)

Sample Card Print Request Acknowledgement file

H<TAB>VICEACK201206141<TAB>20120614095022<TAB>VICE201206141<TAB>2<CR><LF>
D<TAB>2223344444-Doe-1<TAB>00000000010100<CR><LF>

D<TAB>3338844444-Smith-2<TAB>00000000000000<CR><LF>
T<TAB>VICEACK201206141<TAB>20120614095022<TAB>VICE201206141<TAB>2<CR><LF>

DRAFT

2. Mail Confirmation file format

The Card Print Site will provide a mail confirmation file for cards that have been mailed. The file will contain a header record and a trailer record that identifies the name of the file, date/time stamp of the file and the number of records in the file.

Each record will be in variable length, tab de-limited format. Each record will be terminated by a carriage return and line feed sequence (ASCII control code 0x000D and 0x000A).

Record layouts are contained in tables 8, 9, and 10.

Table 8 –Mail Confirmation Header Record

Header Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'H' for header (e.g. H)
File Name	Varchar	17	'VICECOM' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICECOM201206141)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time (e.g. 20120614095022)
Count	Number	9	Count of the number of records in this file (e.g. 10)

Table 9 - Mail Confirmation File Data

Data Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'D' for Data (e.g. D)
Card Request File Name	Varchar	14	Name of the original Card Print Request file transmitted from VIC-E. (e.g. VICE201206141)
Card Request File Creation Time Stamp	DateTime	14	Date/time stamp of the original Card Print Request file transmitted from VIC-E. Format is YYYYMMDDHHMMSS. (e.g. 20120614095022)
Card ID	Varchar	40	Unique identifier for the card request
Mail Date/Time stamp	DateTime	14	Date/time stamp of card mailing to the veteran or medical center. Format is YYYYMMDDHHMMSS using 24 hour time. (e.g. 20120614095022)

DRAFT

Table 10 – Mail Confirmation File Trailer

Trailer Record Field	Data Type	Max Length	Comments
Record Type Indicator	Char	1	'T' for trailer
File Name	Varchar	17	'VICECOM' concatenated with a date stamp of format yyyymmdd and a sequence number (e.g. VICECOM201206141)
File Creation	DateTime	14	Date/time stamp format of YYYYMMDDHHMMSS using 24 hour time (e.g. 20120614095022)
Count	Number	9	Count of the number of records in this file

Sample Mail Confirmation file

H<TAB>VICECOM201206141<TAB>20120614095022<TAB>2<CR><LF>
D<TAB>VICE201206141<TAB>20120614095022<TAB>2223344444-Doe-1<TAB>20120614095022<CR><LF>
D<TAB>VICE201206141<TAB>20120614095022<TAB>3338844444-Smith-2<TAB>20120614095022<CR><LF>
T<TAB>VICECOM201206141<TAB>20120614095022<TAB>2<CR><LF>

DRAFT

ATTACHMENT L
Carrier Sheet (Face)

VA | U.S. Department of Veterans Affairs

<Facility Name>
<Facility Address>
<Facility City> <Facility State> <Facility Zip>

<First Name> <Last Name>
<Address 1>
<Address 2>
<City> <State> <Zip>

This card is only for use as a means of identification when reporting for your appointment at VA medical facilities. Please bring this card each time you have a VA appointment so we may ease your appointment check-in process.

This card cannot be used as a credit card or an insurance card, and it does not authorize or pay for care at non-VA facilities.

If you have questions regarding VA health care benefits, please call 1-877-222-VETS (8387). You may also access health care information on the web at: www.myhealth.va.gov.

Attached is your new
Veterans Identification Card

ATTACHMENT M
Facility Physical Security Checklist

Facility Physical Security Checklist

Physical Security	Yes	No	Evaluate?	Comments
Camera monitoring the computer operations room?				
All security systems are located in a secure room with ingress and egress readers?				
Closed-circuit TV (CCTV) system?				
Burglary/intrusion alarm system, directly connected to a 24-hour alarm system?				
Burglary system includes back-up radio notification and uses contacts, passive infrared, glass break and vibration detection?				
Fully-lighted, free standing building?				
Exterior camera monitoring?				
Internal camera monitoring?				
Internal card readers have anti-passback? (only one employee can access the building with their employee identification card. Multiple use of the same card by different personnel not allowed.)				
Shipping and receiving area is camera monitored?				
Man-trap area entering the production floor?				
Camera monitoring on the production floor?				
Dual locking vault with camera surveillance?				
Motion detectors?				
Proximity cards and readers to access the premises?				
Duress emergency alarm system?				
Semi-annual inspections are conducted of all facets of the card access, CCTV, burglary/intrusion and fire systems?				

Safeguards	Yes	No	Evaluate?	Comments
Dual Control For Plastics Shipments Received?				
Dual Control For All Vault Access?				
Electronic Vault And Warehouse Inventory Logs?				
Card Personalization Process?				
Order Receipt?				
Order Acknowledgement?				
Pre-Processing?				
Production/ Machine/Operator set up of VIC/VHIC Order ?				
Card verification?				
Card count balance?				
Quality Assurance?				
Inspection?				
Personalized carriers?				
Load completed carriers?				
Remake of spoiled cards?				
Collateral material issuance?				

ATTACHMENT M
Facility Physical Security Checklist

Insert equipment setup and vision verification?				
Inspection?				
Close order?				
Secure order?				
Mail Confirmation?				
PII destruction?				
Job Tracking System – Production Order Tracking, Audit, And Reporting System ? (tracks each step in the personalization process At each step, operator must balance to systems total for their portion of the job Job cannot advance to next step until prior step is complete and balanced.)				

Information Security	Yes	No	Evaluate?	Comments
Network Security?				
Privacy Training?				
Access to VA VIC/VHIC data?				
Moderate Background Investigation?				
Data Deletion?				

Disaster Recovery and Contingency Plans	Yes	No	Evaluate?	Comments
Plan Activation?				
Recovery Sites?				
Material and Supplies?				
Card Data?				

ATTACHMENT N
Facility Inspection Checklist

Facility Inspection Checklist

Facility Inspection Checklist

Observations	Yes	No	Comments / Recommendations
Were there any unattended computers logged on?			
Are any computer screens with PII visible to visitors?			
Can the computer screen be turned or be relocated?			
Are VIC/VHIC cards left in any unattended open areas or unsecured offices?			
Are workstations locked or logged off when staffs are not present in room?			
Is there a sign-in sheet for visitors? How is it maintained?			
Are visitors able to handle/receive VICs/VHICs?			
Are passwords visible around workstation or under mouse pads?			
Does staff properly refuse to give their password when asked?			

ATTACHMENT N
Facility Inspection Checklist

Staff provides a correct response when asked where they keep password.			
The processing rooms for VIC/VHICs and the computer areas are secure areas and not accessible to housekeeping or other ancillary staff after hours?			
Were any PII/VICs/VHICs found in regular recycle container or unmanned areas?			
Are badges controlled by being logged in/out?			
How long is the badge log maintained?			
Does staff ask for identification before giving access to controlled areas?			
Visitors and others not recognized are asked for identification when accessing restricted areas?			
Does the server have encryption? At what type/level?			
Does staff use removable media?			
Is all PII stored in an encrypted manner?			

ATTACHMENT N
Facility Inspection Checklist

Does staff use removable media?			
Is there an available list of employees with access to server information?			
Do the file cabinets lock? Where are the key(s) for cabinets/desks kept?			
Can the staff explain the process for reporting information security incidents?			
Does the staff know how to contact the ISOs and how to contact on all shifts?			
When was the last Privacy and Security training conducted?			
Are bins/shredding materials in secure area(s)?			