SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.	PAGE 1 OF
481-12-1-4937-0011	60

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			VA244-12-Q-0344	03-05-2012

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
	Jennifer Balsiger	(814) 860-2977	03-14-2012 2:00 PM EST

9. ISSUED BY CODE 00562

Department of Veterans Affairs
Erie VAMC
Acquisitions (Bldg 9 90C)
135 E 38th St
Erie PA 16504-1559

10. THIS ACQUISITION IS

- ☐ UNRESTRICTED OR ☐ SET ASIDE: _____ % FOR:
- ☐ SMALL BUSINESS
- ☐ HUBZONE SMALL BUSINESS
- ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- ☐ ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
- ☐ 8(A)

NAICS: 561611

SIZE STANDARD: $12.5 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING
☒ SEE SCHEDULE		☐	N/A

14. METHOD OF SOLICITATION: ☒ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE

Department of Veterans Affairs
Erie VAMC Acquisitions (Bldg 9 90C)
135 E 38th St

Erie PA 16504-1559

16. ADMINISTERED BY CODE 00562

Department of Veterans Affairs
Erie VAMC
Acquisitions (Bldg 9 90C)
135 E 38th St
Erie PA 16504-1559

17a. CONTRACTOR/OFFEROR CODE _____ FACILITY CODE _____

TELEPHONE NO.

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE

Department of Veterans Affairs
Financial Services Center
PO Box 149971
Austin TX 78714-8971

PHONE: FAX:

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED
☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES (See CONTINUATION Page)	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Please read the entire solicitation document and submit the required documents. In order for your offer to be considered complete, a signed SF1449 (this page) is required. In addition, the offeror shall acknowledge the receipt of all amendments. (Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA See CONTINUATION Page

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

☒ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☐ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
		Jennifer Balsiger Contract Specialist	

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 CONTRACT ADMINISTRATION DATA

(Continuation from Standard Form 1449, block 18A.)

1. Contract Administration: All contract administration matters will be handled by the following individuals:

a. CONTRACTOR:

b. GOVERNMENT: Contracting Officer 00562 Jennifer Balsiger
Department of Veterans Affairs
Erie VAMC
Acquisitions (Bldg 9 90C)
135 E 38th St
Erie PA 16504-1559

2. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:

[x] 52.232-34, Payment by Electronic Funds Transfer - Other than Central Contractor Registration, or

[] 52.232-36, Payment by Third Party

3. INVOICES: Invoices shall be submitted in arrears:

a. Quarterly []

b. Semi-Annually []

c. Other [x] Monthly

4. GOVERNMENT INVOICE ADDRESS: All invoices from the contractor shall be mailed to the following address:

Department of Veterans Affairs
Financial Services Center
PO Box 149971
Austin TX 78714-8971

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

AMENDMENT NO DATE

_____ _____

STATEMENT OF WORK
DEPARTMENT OF VETERANS AFFAIRS (VA)
INVESTIGATION SERVICES

Purpose
The purpose of this contract is to document observations and conduct other forms of surveillance upon VA employees who are awaiting an outcome of a Worker's Compensation claim, or are receiving Workers' Compensation benefits as a result of a claim being favorably adjudicated. In addition, surveillance may be appropriate where an individual has been separated from their VA employment; however, they continue to receive Workers' Compensation benefits. Surveillance may also be appropriate if there is a concern regarding potential Workers' Compensation Beneficiary fraud, with a review of such issues as marital status and/or student status. The overall purpose for this acquisition is to follow the guidance set forth in the VA Office of Inspector General's report "Veterans Health Administration – Audit of Workers' Compensation Case Management (10-03850-298)" relating to enhancing the monitoring of cases and increasing VHA's fraud detection efforts.

Scope
Under this contract, the Contractor is required to observe and/or survey VA employees who are awaiting an outcome of a Worker's Compensation claim, or are receiving Workers' Compensation benefits as a result of a claim being favorably adjudicated. In addition, surveillance may be appropriate where an individual has been separated from their VA employment, however, they continue to receive Workers' Compensation benefits. Surveillance may also be appropriate if there is a concern regarding possible Workers' Compensation Beneficiary fraud, with a review of such issues as marital status and/or student status. Cases assigned will be for injured individuals who previously worked within the Veterans Integrated Service Network (VISN) 4. VISN 4 covers all of Pennsylvania and parts of Delaware and West Virginia. Hotel and food costs incurred by the Contractor can be reimbursed at the Government Per Diem rate.

Work will be assigned by a facility Worker's Compensation Coordinator, through the concurrence of the facility Human Resources Officer. Information to be provided to the Contractor includes the injured employee's full name, address, date of birth, and social security number (if available). In the case of fraudulent claims, the Contractor is required to support the case until the matter is fully resolved.

Work
After being assigned to a case, the Contractor shall provide a preliminary report to the Contracting Officer's Technical Representative (COTR) within fourteen (14) calendar days. The preliminary report will contain acknowledgement of assignment, a preliminary assessment of the case, and any relevant information for decision making reasons.

After the assignment of the case, but prior to the preliminary report, the Contractor shall hold a telephone conference and/or face-to-face meeting with the facility Worker's Compensation Coordinator. During this meeting, the case will be discussed.

The scope of the effort is to include observations and/or surveillance by the contractor of physical activities of injured individuals who are disabled from their employment with the Department of Veteran Affairs. Documenting the observations and/surveillance with a detailed written report accompanied by photographs and/or video is required. An investigation might include a statistical profile of an injured worker's current address, a neighborhood canvas to obtain information regarding daily activities, a check on past injuries and/or conditions, motor vehicle information, and anything else that may influence the outcome of a Worker's Compensation case. i.e. potential Worker's Compensation fraud. The investigator will provide necessary support, documentation and/or testimony until the potential fraudulent matter is fully concluded. Cases for investigation will be assigned by the facility Workers' Compensation Coordinator, through the

concurrence of the facility Human Resources Officer, at each site within the Network. The facility Workers' Compensation Coordinator will provide the contractor with, amongst other information, an injured worker's full name (to include middle name or middle initial), address (street, city/town, and state), date of birth (DOB), and social security number. The contractor shall acknowledge receipt of the assignment and provide a preliminary report within fourteen (14) calendar days of receipt of the assigned case. Prior to the issuance of a preliminary report, the contractor shall hold a telephone conference and/or face to face meeting with the facility Workers' Compensation Coordinator to discuss appropriate case particulars. The contractor shall provide status reports on assigned cases every thirty (30) days after the issuance of the preliminary report and will commence when the final report is delivered.

For each case, the Contractor shall provide a status report every thirty (30) days, beginning after the issuance of the preliminary report, and ending on the delivery of the final report. The status report will include any information relating to the investigation including the following: observations, photos, database checks and any other items which validate the appropriateness of the workers' compensation case. The report will be formatted in date sequence with locations of activities documented.

Each case shall include written documentation (reports). Photographs, video, and other forms of documentation are encouraged. Each case shall include the following information, at a minimum:

- Statistical profile of injured employee including:
    - Current address
    - Daily activities of injured employee
    - Motor vehicle information
- Research on past injuries
- Potential worker's compensation fraud issues

The final report will be a roll up of the preliminary report, all status reports and any further information gathered prior to the submission of the final report. The final report is due ten (10) days from the date that the Human Resources department announces to the Contractor that their services are complete on a particular case.

Travel is authorized under this agreement, as long as it is in accordance with FAR Part 31 and Pub. L. 99-234. Prior to incurring travel costs, the Contractor shall quote their estimated travel cost and receive approval from the Contracting Officer.

The Contractor is required to obtain/possess the certifications, security clearances, licenses, and accreditations that are necessary to perform the work, as required under this contract. All offerors are required to show that they have a license to practice in the state of Pennsylvania.

Period of Performance

The Government intends to award a Blanket Purchase Agreement (BPA) for one base year and four option year periods. The resulting agreement will be based off of the successful offeror's GSA schedule. This may result in a single or multiple award agreement.

Deliverable Schedule

After a case has been assigned, the Contractor has fourteen (14) days to discuss the case with the facility Worker's Compensation Coordinator and to turn in the preliminary report to the COTR.
Every thirty (30) days after the preliminary report is submitted, a status report will be completed and sent to the COTR.

For more information on the reports/deliverables, see the section titled, *Work.*

Applicable Standards

Since this will be considered an investigation, notification of employees and others does not need to take place.

Evaluation Criteria

Offers will be evaluated based on the following criteria.

1. Offerors shall submit a copy of their current GSA schedule
2. Offerors shall submit all relevant security clearances, accreditations, licenses, including their Pennsylvania State License
3. Offerors shall demonstrate their past performance in investigative work settings. Offerors shall submit the following information for up to three recent contracts:
    a. Name of contact at the company,
    b. Contact's phone number and email address
    c. Length of the contract
    d. Estimated number of cases
    e. Other relevant information
4. Offerors shall provide pricing information for one case. If discount terms apply after a certain number of cases, those should be noted, as well.
5. Service-disabled and veteran-owned company's offers will be evaluated in accordance with VAAR 852.215-70, which is included in this solicitation (Section C)

Security

The Contractor will be required to complete the Contractor Security Control Assessment (CSCA) prior to beginning work under this contract. This document can be found in Section D of this solicitation. In addition, the successful offeror will be required to sign a Business Associate Agreement (BAA) prior to starting the work required under this contract. A sample BAA can be found in Section D of this solicitation.

The following language from Appendix B (VA Handbook 6500.6) applies to this contract.

MARCH 12, 2010 VA HANDBOOK 6500.6
APPENDIX B
B-1

VA ACQUISITION REGULATION SOLICITATION PROVISION AND CONTRACT CLAUSE

NOTE: This clause will undergo official rule making by the Office of Acquisitions and Logistics. The below language will be submitted for public review through the *Federal Register*. The final wording of the clause may be changed from what is outlined below based on public review and comment. Once approved, the final language in the clause can be obtained from the Office of Acquisitions and Logistics Programs and Policy.

1. SUBPART 839.2 – INFORMATION AND INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

839.201 Contract clause for Information and Information Technology Security: a. Due to the threat of data breach, compromise or loss of information that resides on either VA-owned or contractor-owned systems, and to comply with Federal laws and regulations, VA has developed an Information and Information Technology Security clause to be used when VA sensitive information is accessed, used, stored, generated, transmitted, or exchanged by and between VA and a contractor, subcontractor or a third party in any format (e.g., paper, microfiche, electronic or magnetic portable media).

b. In solicitations and contracts where VA Sensitive Information or Information Technology will be accessed or utilized, the CO shall insert the clause found at 852.273-75, Security Requirements for Unclassified Information Technology Resources.

2. 852.273-75 - SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (INTERIM- OCTOBER 2008)
As prescribed in 839.201, insert the following clause:
The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

The following language, taken from Appendix C (VA Handbook 6500.6) applies to this contract.

MARCH 12, 2010 VA HANDBOOK 6500.6
APPENDIX C
C-1
VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE

1. GENERAL
Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS
a. A contractor/subcontrator shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All contractors, subcontractors, and third-party servicers and associates working with VA information is subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

3. VA INFORMATION CUSTODIAL LANGUAGE
a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance 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 VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract without

prior written approval by the VA. Any data destruction done on behalf of VA by a contractor/subcontractor 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*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization.* Self-certification by the contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must 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. 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 or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

f. 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 VA to withhold payment to the contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor is in receipt of a court order or other requests for the above mentioned information, that contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

6. SECURITY INCIDENT INVESTIGATION

a. 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/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and 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/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. The contractor/subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:
(1) Nature of the event (loss, theft, unauthorized access);
(2) Description of the event, including:
(a) Date of occurrence;

(b) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
(3) Number of individuals affected or potentially affected;
(4) Names of individuals or groups affected or potentially affected;
(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
(6) Amount of time the data has been out of VA control;
(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
(8) Known misuses of data containing sensitive personal information, if any;
(9) Assessment of the potential harm to the affected individuals;
(10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
(11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
(1) Notification;
(2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
(3) Data breach analysis;
(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

8. 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 the contract. With 10 working-day's notice, at the request of the government, the contractor must 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) as determined by VA in the event of a security incident or at any other time.

9. TRAINING
a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;
(2) Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and

(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

Contractor Personnel Background Investigation Requirement

A. All General/Prime Contractor employees to include subcontractor personnel who require unsupervised/unescorted, logical and/or physical access to the Department of Veterans Affairs facilities, computer systems or have access to sensitive information shall be the subject of a background investigation. Contractor personnel performing work under any contract shall satisfy all requirements for appropriate security eligibility in dealing with access to sensitive information and information systems belonging to or being used on behalf of the Department of Veterans Affairs.

B. Risk levels and the Personal Identity Verification (PIV) program will determine what level of investigation is required. At a minimum a ***Special Agreement Check (SAC)*** will be required for all contractor personnel prior to performing services under any resulting contract requiring unsupervised/unescorted logical and/or physical access to the facility or having access to sensitive information.

Position Sensitivity - The position sensitivity has been designated as LOW. Contracting Officer will insert one of the following **(Low Risk, Moderate Risk** or **High Risk) based on input from COTR**

Background Investigation - The level of background investigation commensurate with the required level of access is Low Risk - NACI.

Contracting Officer will insert required level of Background Investigation based on COTR input; **SAC** (low risk exempt from NACI investigations) **NACI** (low risk), **MBI** (moderate risk), or **BI** (high risk). Non-citizen contract personnel appointed to low risk positions will be subject to a National Agency Check with Law Enforcement and Credit Check **(NACLC).**

C. The General/Prime Contractor shall submit to the Contracting Officer and Contracting Officer's Technical Representative (COTR) within five (5) business days after award of contract a list of personnel including subcontractor's personnel who will be performing work on the contract. The list will include a brief description of the work to be performed and degree of access to information management systems and if remote access will be required. The Contractor will update and submit the list anytime changes are made in the level of access or personnel performing work on the contract.

D. Contractors who have a current favorable background investigation conducted by another Federal agency may be accepted through reciprocation. Information substantiating a current favorable background installation will be submitted to the Contracting Officer and Contracting Officer's Technical Representative (COTR will submit this information to HR for submission/validation with the Security and Investigation Center (SIC)). Members of the SIC staff will coordinate verification of existing favorable background investigations. Furthermore contractor may utilize a private investigating agency if such agency possesses an OPM and Defense Security Service certification. A Cage Code number of the private investigating agency must be provided to the VA Office of Security and Law Enforcement/Security and Investigation Center staff.

E. The Department of Veterans Affairs in conjunction with Office of Personnel Management (OPM) at the request of the General/Prime Contractor execute the required background investigation for contractor personnel employees to include subcontractor's personnel performing services under this contract. The General/Prime Contractor shall bear the expense of the background investigations initiated/scheduled regardless of the final adjudication determination. The VA facility will pay for investigations conducted by the Office of Personnel Management (OPM) in advance. In these instances, the General/Prime Contractor will reimburse the VA facility within 30 days of receiving the Bill of Collections from the VA. A Bill of Collections shall be generated by the VA after the investigation has been initiated / scheduled. We have determined this contract requires the following level of investigations and associated costs (per person):

NACI	$231.00
MBI	$825.00
BI	$3465.00

The amounts stated above are current for fiscal year 2010, and are subject to periodic price changes as established by the OPM in Federal Investigations Notices. Contractors shall be billed per OPM/SIC guidelines and should anticipate periodic increases. All fee schedule questions should be directed to the SIC at 501-257-4031 or vhalitsiccontracting@va.gov.

F. Based on COTR completion (in consultation with the Contractor) and submission of VA Form 2280 , Position Risk and Sensitivity Level Designation (or replacement form), COTR will determine level of background investigation required for all applicable personnel and will submit a background investigation request through HRM to the Security and Investigation Center and receive access to the Contractor Request Database (CRD) located at https://vaww.letc.little-rock.med.va.gov/. Upon receipt, the CRD will automatically generate an e-mail notification identifying the web site link that includes detailed instructions regarding completion of the application process and what level of background was requested.

G. For all contractor personnel requiring a National Agency Check with Written Inquiries (NACI) or higher background Investigations the contractor shall submit to the Security Investigations Center (SIC), the completed background investigation packet. Completed packages must be submitted promptly and in sufficient time to meet the contract performance or delivery schedule. If a delay is due to the failure of the Contractor to provide a complete application as soon as practicable after contract award, this delay shall not excuse the Contractor from meeting the contract performance or delivery schedule and may result in termination for default.

H. The contractor is encouraged to have its employee immediately download the background investigation packet from http://www.va.gov/vabackground_investigations upon notification of contract award. Contract performance shall not commence prior to confirmation from the SIC that

the investigative documents have been submitted. The SIC will notify the VA and the contractor upon receipt of the appropriate investigative documents. The investigation is not considered initiated until the contract employee submits his/her completed package to the SIC and it is accepted. The Contractors may be granted access prior to receiving final adjudication of the employee's background investigations.

I. The VA Security Investigations Center will notify the VA and Contractor after adjudicating the results of the background investigations received from OPM. Final adjudication results may take up to six months but are normally received within 90 days after submission

J. The General/Prime Contractor will be responsible for the actions of individuals performing 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 General/Prime Contractor will be responsible for all resources necessary to remedy the incident.

K. The Contractor, when notified of an unfavorable determination, will withdraw the employee from consideration from working under the contract.

L. Failure to comply with the Contractor Personnel Background Investigation Requirements section shall result in termination of the contract for default.

Performance Measures

The Contractor's performance will be evaluated for each contract year. Documentation will be maintained by the COTR on the Contractor's compliance with the following performance measurements. Failure to meet the performance requirements could result in the loss of future consideration for a contract. The performance measurements are:

1. The Contractor shall provide all deliverables required for each case, 100% of the time.

2. All recorded physical activity shall be available on one of the following media types, 100% of the time: CD-ROM, DVD-R, or VHS Tape. The date and time shall be captured, as well.

3. The Contractor will provide a cost savings report to the appropriate parties each year, 100% of the time.

Attached to this scope of work is an example of the Contractor's Performance Report. The Contractor's performance of the 3 measures will be documented, using this form, on an annual basis.

CONTRACTOR PERFORMANCE REPORT

GENERAL CONTRACT INFORMATION

DEPARTMENT: **TEAM:**
CONTRACTOR: **CONTRACT #:**
BASE YEAR: **OPTION:**
BRIEF DESCRIPTION OF SERVICE (SOW):
CURRENT YEAR: **QUARTER:**
AWARD FUTURE CONTRACTS? ☐ YES ☐ NO

RATINGS AND SUPPORTING DOCUMENTATION FOR RECOMMENDATION

(See Page 2 for Instructions)

PERFORMANCE ELEMENTS	1	2	3
A. Quality of Service/record accuracy/clinical pertinence	☐	☐	☐
B. Timeliness of performance/scheduling/consistency of visits	☐	☐	☐
C. Customer Service/patient satisfaction	☐	☐	☐
D. Business Relations/honors inquiries and requests for information	☐	☐	☐

Key:

1. *Performance DOES NOT meet SOME contractual requirements. The performance of the element being assessed reflects a problem for which the CONTRACTING OFFICE will address by corrective action request with follow-up to using service.*
2. *Performance meets contractual requirements with COTR oversight. The contractual performance of the element being assessed contains minor problems to be addressed by the using service within the parameters designated by the delegation of the COTR.*
3. *Performance meets contractual requirements The contractual performance of the element being assessed was accomplished with NO problems*

Performance Measure Description	Target/ Goal/ Contract Requirement	Current Data
1. Deliverables for each case were provided	100% of time	
2. Correct media type was used for physical activity recordings	100% of time	
3. Cost savings report submitted on time	100% of time	

COTR Comments:

Signature of rating official_____ Date: _____

FOR CONTRACT OFFICE USE ONLY

Reviewing Official:		Date:	
CO Comments & Actions Taken			

CONTRACTOR PERFORMANCE REPORT INSTRUCTIONS

"Outstanding Performance is measured by resourcefulness"

To be objective and fair in determining contract awards, we ask that you participate in our **Service Contract Performance Monitoring Program** by filling out this report on a quarterly basis. Completed reports should be returned to the **Contracting Office** by the end of the second week of the month following the end of the quarter. The completed reports can be sent hard copy or by email. It is important that the form be completed by the designated COTR or an associate who is technically or professionally capable of rating the performance of the service being provided.

"Contract monitoring is only as effective as the diligence of the COTR and/or designee". Please read the definitions of the ratings and rate appropriately. You will notice that ratings 1 through 3 specify additional action that must be taken. A rating of 3 and 2 requires action by the using service/COTR only. **A rating of 1 requires action by the contracting office based on valid documentation provided by the COTR.** Applicable performance measures should be monitored and included in this report.

The data from your reports will be compiled into one quarterly report for the Medical Executive Council (MEC). It is important to take immediate action when performance issues are identified. Action taken and the effectiveness of that action should be included in this report.

Thank you for your cooperation and please do not hesitate to call with any questions and or concerns regarding this reporting form.

Erie VA
Contracting Office

B.2 PRICE/COST SCHEDULE

Item No.	Description	Qty	Unit	Unit Price
1	Price per Case; Base Year Estimated Min: 10 cases; Estimated Max: 45 Cases	1	Case	
2	Price per Case; Option Year 1 Estimated Min: 10 cases; Estimated Max: 45 Cases	1	Case	
3	Price per Case; Option Year 2 Estimated Min: 10 cases; Estimated Max: 45 Cases	1	Case	
4	Price per Case; Option Year 3 Estimated Min: 10 cases; Estimated Max: 45 Cases	1	Case	
5	Price per Case; Option Year 4 Estimated Min: 10 cases; Estimated Max: 45 Cases	1	Case	

NOTE: All travel expenses need to be quoted, submitted to the Contracting Officer (CO), and approved by the CO PRIOR to incurring the expenses. This shall be done for each case.

SECTION C - CONTRACT CLAUSES

C.1 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (FEB 2012)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104 (g)).

(2) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Pub. L. 108-77, 108-78)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[] (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

[] (2) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010)(Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

[] (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

[] (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (FEB 2012) (Pub. L. 109-282) (31 U.S.C. 6101 note).

[] (5) 52.204-11, American Recovery and Reinvestment Act-Reporting Requirements (JUL 2010) (Pub. L. 111-5).

[] (6) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Dec 2010) (31 U.S.C. 6101 note).

[x] (7) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (JAN 2012) (41 U.S.C. 2313).

[] (8) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (section 740 of Division C of Public Law 111-117, section 743 of Division D of Public Law 111-8, and section 745 of Division D of Public Law 110-161)

[] (9) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

[] (10) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

[] (11) [Reserved]

[x] (12)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

[] (ii) Alternate I (NOV 2011).

[] (iii) Alternate II (NOV 2011).

[] (13)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

[] (ii) Alternate I (Oct 1995) of 52.219-7.

[] (iii) Alternate II (Mar 2004) of 52.219-7.

[] (14) 52.219-8, Utilization of Small Business Concerns (JAN 2011) (15 U.S.C. 637(d)(2) and (3)).

[] (15)(i) 52.219-9, Small Business Subcontracting Plan (JAN 2011) (15 U.S.C. 637(d)(4)).

[] (ii) Alternate I (Oct 2001) of 52.219-9.

[] (iii) Alternate II (Oct 2001) of 52.219-9.

[] (iv) Alternate III (JUL 2010) of 52.219-9.

[] (16) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

[] (17) 52.219-14, Limitations on Subcontracting (NOV 2011) (15 U.S.C. 637(a)(14)).

[] (18) 52.219-16, Liquidated Damages--Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

[] (19)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer.)

[] (ii) Alternate I (June 2003) of 52.219-23.

[] (20) 52.219-25, Small Disadvantaged Business Participation Program--Disadvantaged Status and Reporting (DEC 2010) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (21) 52.219-26, Small Disadvantaged Business Participation Program--Incentive Subcontracting (Oct 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).

[] (23) 52.219-28, Post Award Small Business Program Rerepresentation (APR 2009) (15 U.S.C 632(a)(2)).

[x] (24) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business Concerns (NOV 2011).

[] (25) 52.219-30, Notice of Set-Aside for Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (NOV 2011).

[] (26) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

[] (27) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (JUL 2010) (E.O. 13126).

[] (28) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

[] (29) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

[] (30) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

[] (31) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

[] (32) 52.222-37, Employment Reports on Veterans (SEP 2010) (38 U.S.C. 4212).

[] (33) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

[] (34) 52.222-54, Employment Eligibility Verification (Jan 2009). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

[] (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C.6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (36) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).

[] (37)(i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007) (E.O. 13423).

[] (ii) Alternate I (DEC 2007) of 52.223-16.

[x] (38) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)

[] (39) 52.225-1, Buy American Act--Supplies (FEB 2009) (41 U.S.C. 10a-10d).

[x] (40)(i) 52.225-3, Buy American Act--Free Trade Agreements-- Israeli Trade Act (JUN 2009) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C 3805 note, Pub. L. 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, and 110-138).

[] (ii) Alternate I (Jan 2004) of 52.225-3.

[] (iii) Alternate II (Jan 2004) of 52.225-3.

[] (41) 52.225-5, Trade Agreements (NOV 2011) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

[] (42) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

[] (43) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

[] (44) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

[] (45) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[] (46) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[] (47) 52.232-33, Payment by Electronic Funds Transfer--Central Contractor Registration (Oct 2003) (31 U.S.C. 3332).

[x] (48) 52.232-34, Payment by Electronic Funds Transfer--Other than Central Contractor Registration (May 1999) (31 U.S.C. 3332).

[] (49) 52.232-36, Payment by Third Party (FEB 2010) (31 U.S.C. 3332).

[] (50) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

[] (51)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

[] (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[x] (1) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

[] (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

Employee Class	Monetary Wage-Fringe Benefits

[x] (3) 52.222-43, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Multiple Year and Option Contracts) (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (4) 52.222-44, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

[] (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

[] (7) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247)

[] (8) 52.237-11, Accepting and Dispensing of $1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (DEC 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) [Reserved]

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

(ix) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements "(Nov 2007)" (41 U.S.C. 351, et seq.).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (FEB 2009)(41 U.S.C. 351, et seq.).

(xii) 52.222-54, Employee Eligibility Verification (JAN 2009)

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

C.2 52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011)

(a) Definitions. As used in this clause--

"Postconsumer fiber" means--(1) Paper, paperboard, and fibrous materials from retail stores, office buildings, homes, and so forth, after they have passed through their end-usage as a consumer item,

including: used corrugated boxes; old newspapers; old magazines; mixed waste paper; tabulating cards; and used cordage; or

(2) All paper, paperboard, and fibrous materials that enter and are collected from municipal solid waste; but not

(3) Fiber derived from printers' over-runs, converters' scrap, and over-issue publications.

(b) The Contractor is required to submit paper documents, such as offers, letters, or reports that are printed or copied double-sided on paper containing at least 30 percent postconsumer fiber, whenever practicable, when not using electronic commerce methods to submit information or data to the Government.

(End of Clause)

C.3 52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from date of contract award through 5 years later.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of Clause)

C.4 52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than 10 cases per year, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor--

(1) Any order for a single item in excess of 45 cases per year;

(2) Any order for a combination of items in excess of N/A; or

(3) A series of orders from the same ordering office within N/A days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the

ordering office within 15 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

C.5 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after N/A.

(End of Clause)

C.6 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days.

(End of Clause)

C.7 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 60 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years and 6 months.

(End of Clause)

C.8 52.232-18 AVAILABILITY OF FUNDS (APR 1984)

Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer.

(End of Clause)

C.9 52.237-3 CONTINUITY OF SERVICES (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to (1) furnish phase-in training and (2) exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

(End of Clause)

C.10 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

The bidder or offeror agrees that if a contract is awarded to him/her, as a result of this solicitation, he/she will not advertise the award of the contract in his/her commercial advertising in such a manner as to state or imply that the Department of Veterans Affairs endorses a product, project or commercial line of endeavor.

(End of Clause)

C.11 VAAR 852.215-70 SERVICE-DISABLED VETERAN-OWNED AND VETERAN-OWNED SMALL BUSINESS EVALUATION FACTORS (DEC 2009)

(a) In an effort to achieve socioeconomic small business goals, depending on the evaluation factors included in the solicitation, VA shall evaluate offerors based on their service-disabled veteran-owned or veteran-owned small business status and their proposed use of eligible service-disabled veteran-owned small businesses and veteran-owned small businesses as subcontractors.

(b) Eligible service-disabled veteran-owned offerors will receive full credit, and offerors qualifying as veteran-owned small businesses will receive partial credit for the Service-Disabled Veteran-Owned and Veteran-owned Small Business Status evaluation factor. To receive credit, an offeror must be registered and verified in Vendor Information Pages (VIP) database. (http://www.VetBiz.gov).

(c) Non-veteran offerors proposing to use service-disabled veteran-owned small businesses or veteran-owned small businesses as subcontractors will receive some consideration under this evaluation factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In addition, the proposed subcontractors must be registered and verified in the VetBiz.gov VIP database (http://www.vetbiz.gov).

(End of Clause)

C.12 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of Pennsylvania. Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

C.13 VAAR 852.273-76 ELECTRONIC INVOICE SUBMISSION (Interim - October 2008)

(a) To improve the timeliness of payments and lower overall administrative costs, VA strongly encourages contractors to submit invoices using its electronic invoicing system. At present, electronic submission is voluntary and any nominal registration fees will be the responsibility of the contractor. VA intends to mandate electronic invoice submission, subject to completion of the federal rulemaking process. At present, VA is using a 3rd party agent to contact contractors regarding this service. During the voluntary period, contractors interested in registering for the electronic system should contact the VA's Financial Services Center at http://www.fsc.va.gov/einvoice.asp.

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

BUSINESS ASSOCIATE AGREEMENT BETWEEN THE DEPARTMENT OF VETERANS AFFAIRS, VETERANS HEALTH ADMINISTRATION AND

Whereas, (Business Associate) provides services to the Department of Veterans Affairs Veterans Health Administration (Covered Entity); and

Whereas, in order for Business Associate to provide services to Covered Entity, Covered Entity discloses to Business Associate Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996), and its implementing regulations, 45 C.F.R Parts 160, 162, and 164, ("the HIPAA Privacy and Security Rules"); and

Whereas, the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009), pursuant to Title XIII of Division A and Title IV of Division B, called the Health Information Technology for Economic and Clinical Health (HITECH) Act, provides modifications to the HIPAA Privacy and Security Rules; and

Whereas, Department of Veterans Affairs Veterans Health Administration is a "Covered Entity" as that term is defined in the HIPAA implementing regulations, 45 C.F.R. 160.103; and

Whereas, , including its employees, officers, contractors, subcontractors, or any other agents, as a recipient of PHI from Covered Entity in order to provide services to Covered Entity, is a "Business Associate" of Covered Entity as that term is defined in the HIPAA implementing regulations, 45 C.F.R 160.103; and

Whereas, pursuant to the Privacy and Security Rules, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the Use and Disclosure of PHI and EPHI; and

Whereas, the purpose of this Agreement is to comply with the requirements of the Privacy and Security Rules, including, but not limited to, the Business Associate Agreement requirements at 45 C.F.R. 164.308(b), 164.314(a), 164.410, 164.502(e), and 164.504(e), as may be amended.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions. Unless otherwise provided in this Agreement, capitalized terms and phrases that are defined in the Privacy and Security Rules have the same meanings as set forth in the Privacy and Security Rules. When the phrase "Protected Health Information" and the abbreviation "PHI" are used in this Agreement, they include the phrase "Electronic Protected Health Information" and the abbreviation "EPHI."

2. Ownership of PHI. PHI provided by Covered Entity to Business Associate and its contractors, subcontractors, or other agents, or gathered by them on behalf of Covered Entity, under this Agreement are the property of Covered Entity.

3. Scope of Use and Disclosure by Business Associate of Protected Health Information. Unless otherwise limited herein, Business Associate may:

A. Make Uses and Disclosures of PHI that is disclosed to it by Covered Entity or received by Business Associate on behalf of Covered Entity as necessary to perform its obligations under this Agreement and all applicable agreements, provided that such Use or Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity and complies with Covered Entity's minimum necessary policies and procedures;

B. Use the PHI received in its capacity as a Business Associate of Covered Entity for its proper management and administration and to fulfill any legal responsibilities of Business Associate;

C. Make a Disclosure of the PHI in its possession to a third party for the proper management and administration of Business Associate or to fulfill any legal responsibilities of Business Associate; provided, however, that the Disclosure would not violate the HIPAA Privacy Rule if made by Covered Entity, or is Required by Law; and Business Associate has received from the third party written assurances that (a) the information will be held confidentially and used or further disclosed only for the purposes for which it was disclosed to the third party or as Required By Law, (b) the third party will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information may have been breached, and (c) the third party has agreed to implement reasonable and appropriate steps to safeguard the information;

D. Engage in Data Aggregation activities, consistent with the HIPAA Privacy Rule; and

E. De-identify any and all PHI created or received by Business Associate under this Agreement, provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule.

4. Obligations of Business Associate. In connection with its Use or Disclosure of PHI, Business Associate agrees that it will:

A. Consult with Covered Entity before making the Use or Disclosure whenever Business Associate is uncertain whether it may make a particular Use or Disclosure of PHI in performance of this Agreement;

B. Ensure any employee, officer, contractor, subcontractor, or other agent of Business Associate who has access to PHI receives at a minimum annual privacy and security awareness training that conforms to the requirements of Covered Entity;

C. Develop and document policies and procedures and use reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as provided by this Agreement;

D. To the extent practicable, mitigate any harmful effect of a Use or Disclosure of PHI by Business Associate in violation of this Agreement that is known or, by exercising reasonable diligence, should have been known to Business Associate;

E. Maintain a system or process to account for any Security Incident, Privacy Incident, or Use or Disclosure of PHI not authorized by this Agreement of which Business Associate becomes aware;

F. Notify Covered Entity within 24 hours of Business Associate's discovery any incident which may potentially be a data breach, including a HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI, whether secured (PHI which has been destroyed or in the alternative has been rendered unreadable, unusable or undecipherable) or unsecured

(PHI not secured through the use of a technology which renders it unusable, unreadable, or indecipherable through methodology specified by HHS in guidance issued under 13402(h)(2) of the HITECH Act), not provided for by this Agreement and promptly provide a report to Covered Entity within ten (10) business days of the notification;

(1) An incident will be considered any physical, technical or personal activity or event that increases risk of inappropriate or unauthorized use or disclosure of PHI or causes Covered Entity to be considered non-compliant with the HIPAA Privacy and Security Rules;

(2) A breach, as defined in 45 C.F.R. 164.402, is an unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI by posing a significant risk of financial , reputational, or other harm to the individual;

(3) A breach, consistent with 45 C.F.R. 164.410(a)(2), will be treated as discovered as of the first day on which such breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate, or any employee, officer, contractor, subcontractor, or other agent of Business Associate;

(4) Notification will be made by Business Associate to the Director, Health Data & Informatics by telephone, 202-461-5839 or secure fax of any HIPAA Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this Agreement; and

(5) A written report of the incident, submitted to the Director, Health Data & Informatics within ten (10) business days after initial notification, will document the following:

(a). The identification of each individual whose PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, used, or disclosed during the breach;

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

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

(d). Any steps that Business Associate believes individuals should take to protect themselves from potential harm resulting from the breach;

(e). A description of what is being done to investigate the breach, to mitigate further harm to individuals, and the reasonable and appropriate safeguards being taken to protect against future breaches; and

(f). Any other information described in 45 C.F.R. 164.404(c);

(g). This report should be documented as a letter and sent to:

Director, Health Data & Informatics Department of Veterans Affairs - Veterans Health Administration Office of Information (19F) 810 Vermont Avenue NW Washington, DC 20420 Phone: 202-461-5839 Fax: 202-273-9386

G. Implement administrative, physical, and technical safeguards and controls for the PHI that Business Associate receives, maintains, or transmits on behalf of Covered Entity, including policies, procedures, training, and sanctions, in compliance with Federal Information Security Management Act (FISMA), Pub. L. No. 107-347, 116 Stat. 2946 (2002); the HIPAA Privacy and Security Rules, 45 C.F.R. Parts 160, 162, and 164; standards and guidance from the Office of Management and Budget and the National Institute of Standards and Technology; and other laws, regulations, and policies pertaining to safeguarding VA Sensitive Data;

H. Require contractors, subcontractors, or other agents to whom Business Associate provides PHI received from Covered Entity to agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement, including implementation of administrative, physical, and technical safeguards and controls, including policies, procedures, training and sanctions, in compliance with the above-referenced legal authorities;

I. If Business Associate maintains PHI in a Designated Record Set or Privacy Act System of Records, within ten (10) business days of receiving a written request from Covered Entity:

(1) Make available PHI in the Designated Record Set or System of Records necessary for Covered Entity to respond to individuals' requests for access to PHI about them that is not in the possession of Covered Entity;

(2) Incorporate any amendments or corrections to the PHI in the Designated Record Set or System of Records in accordance with the Privacy Act and the HIPAA Privacy Rule; and

(3) Maintain the information necessary to document the disclosures of PHI sufficient to make an accounting of those disclosures as required under the Privacy Act, 5 U.S.C. 552a, and the HIPAA Privacy Rule, and within ten (10) days of receiving a request from Covered Entity, make available the information necessary for Covered Entity to make an accounting of Disclosures of PHI about an individual in the Designated Record Set or System of Records;

J. Utilize only contractors, subcontractors, or other agents who are physically located within a jurisdiction subject to the laws of the United States and ensure that no contractor, subcontractor, or agent maintains, processes, uses, or discloses PHI received from Covered Entity in any way that will remove the PHI from such jurisdiction. Any modification to this provision must be approved by Covered Entity in advance and in writing;

K. Provide satisfactory assurances that the confidentiality, integrity, and availability of the PHI provided by Covered Entity under this Agreement are reasonably and appropriately protected;

L. Upon completion or termination of the applicable contract(s) or agreement(s), return and/or destroy, at Covered Entity's option, the PHI gathered, created, received, or processed during the performance of the contract(s) or agreement(s). No data will be retained by Business Associate, or contractor, subcontractor, or other agent of Business Associate, unless retention is required by law or regulation and specifically permitted by Covered Entity. As deemed appropriate by and under the direction of Covered Entity, Business Associate shall provide written assurance that all PHI has been returned to Covered Entity or destroyed by Business Associate. If immediate return or destruction of all data is not possible, Business Associate shall notify Covered Entity and assure that all PHI retained will be safeguarded to prevent unauthorized Uses or Disclosures;

M. Be liable to Covered Entity for liquidated damages in the event of a data breach involving any PHI maintained or processed by Business Associate under this Agreement;

N. Be liable to Covered Entity for any civil or criminal penalties imposed on Covered Entity under the HIPAA Privacy and Security Rules in the event of a violation of the Rules as a result of any practice, behavior, or conduct by Business Associate;

O. For the purpose of determining compliance with this Agreement and underlying agreements, Business Associate will make available to Covered Entity its practices, policies and procedures; and

P. Make available to the Secretary of Health and Human Services Business Associate's internal practices, books, and records, including policies and procedures, relating to the Use or Disclosure of PHI for purposes of determining Covered Entity's compliance with the Privacy and Security Rules, subject to any applicable legal privileges.

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

A. Has obtained, and will obtain, from Individuals any consents, authorizations, and other permissions necessary or required by laws applicable to Covered Entity for Business Associate and Covered Entity to fulfill their obligations under this Agreement;

B. Will promptly notify Business Associate in writing of any restrictions on the Use and Disclosure of PHI about Individuals that Covered Entity has agreed to that may affect Business Associate's ability to perform its obligations under this Agreement; and

C. Will promptly notify Business Associate in writing of any change in, or revocation of, permission by an Individual to use or disclose PHI, if such change or revocation may affect Business Associate's ability to perform its obligations under this Agreement;

6. Material Breach and Termination.

A. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation;

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

(3) Immediately terminate this Agreement and underlying contract(s) if cure is not possible; or

(4) If Business Associate has breached a material term of this agreement and neither termination nor cure is feasible, Covered Entity will report the violation to the Secretary of Health and Human Services.

B. Termination Upon Review. This Agreement may be terminated by Covered Entity, if appropriate, upon review as defined in Section 12 of this Agreement.

C. Automatic Termination. This Agreement will automatically terminate upon completion of the Business Associate's duties under all underlying agreements or by mutual written agreement to terminate underlying agreements.

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

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

8. No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

9. Other Applicable Law. This Agreement does not and is not intended to abrogate any responsibilities of the parties under any other applicable law.

10. Effect of Agreement. With respect solely to the subject matter herein, in the case of any conflict in terms between this Agreement and any other previous agreement or addendum between the parties, the terms of this Agreement shall control and supersede and nullify any conflicting terms as it relates to the parties.

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

12. Review Date. The provisions of this Agreement will be reviewed by Covered Entity every two years from Effective Date to determine the applicability of the agreement based on the relationship of the parties at the time of review.

Department of Veterans Affairs
Veterans Health Administration

By :
Name :
Title:
Date :

By : _____
Name : _____
Title: _____
Date : _____

WD 05-2451 (Rev.-14) was first posted on www.wdol.gov on 06/17/2011

****

REGISTER OF WAGE DETERMINATIONS UNDER THE SERVICE CONTRACT ACT | U.S. DEPARTMENT OF LABOR
EMPLOYMENT STANDARDS ADMINISTRATION
By direction of the Secretary of Labor | WAGE AND HOUR DIVISION
| WASHINGTON D.C. 20210
|
|
|
| Wage Determination No.: 2005-2451
Diane C. Koplewski Division of | Revision No.: 14
Director Wage Determinations | Date Of Revision: 06/13/2011

States: Ohio, Pennsylvania

Area: Ohio Counties of Belmont, Harrison, Jefferson, Tuscarawas
Pennsylvania Counties of Allegheny, Armstrong, Beaver, Bedford, Blair, Butler, Cambria, Cameron, Centre, Clarion, Clearfield, Clinton, Crawford, Elk, Erie, Fayette, Forest, Fulton, Greene, Huntingdon, Indiana, Jefferson, Lawrence, McKean, Mercer, Potter, Somerset, Venango, Warren, Washington, Westmoreland

Fringe Benefits Required Follow the Occupational Listing

OCCUPATION CODE - TITLE	FOOTNOTE	RATE
01000 - Administrative Support And Clerical Occupations		
01011 - Accounting Clerk I		14.66
01012 - Accounting Clerk II		16.92
01013 - Accounting Clerk III		20.33
01020 - Administrative Assistant		21.11
01040 - Court Reporter		17.78
01051 - Data Entry Operator I		12.17
01052 - Data Entry Operator II		13.81
01060 - Dispatcher, Motor Vehicle		17.44
01070 - Document Preparation Clerk		12.44
01090 - Duplicating Machine Operator		12.44
01111 - General Clerk I		11.61
01112 - General Clerk II		14.59
01113 - General Clerk III		16.37
01120 - Housing Referral Assistant		18.54
01141 - Messenger Courier		10.42
01191 - Order Clerk I		13.17
01192 - Order Clerk II		15.74
01261 - Personnel Assistant (Employment) I		16.18
01262 - Personnel Assistant (Employment) II		18.09
01263 - Personnel Assistant (Employment) III		20.18
01270 - Production Control Clerk		20.18
01280 - Receptionist		11.91
01290 - Rental Clerk		15.53
01300 - Scheduler, Maintenance		15.48
01311 - Secretary I		15.48
01312 - Secretary II		17.32

01313 - Secretary III	19.31
01320 - Service Order Dispatcher	17.00
01410 - Supply Technician	21.43
01420 - Survey Worker	15.04
01531 - Travel Clerk I	12.61
01532 - Travel Clerk II	13.54
01533 - Travel Clerk III	14.52
01611 - Word Processor I	12.90
01612 - Word Processor II	15.53
01613 - Word Processor III	17.37
05000 - Automotive Service Occupations	
05005 - Automobile Body Repairer, Fiberglass	18.95
05010 - Automotive Electrician	17.78
05040 - Automotive Glass Installer	17.10
05070 - Automotive Worker	17.10
05110 - Mobile Equipment Servicer	15.85
05130 - Motor Equipment Metal Mechanic	18.41
05160 - Motor Equipment Metal Worker	17.10
05190 - Motor Vehicle Mechanic	18.70
05220 - Motor Vehicle Mechanic Helper	15.23
05250 - Motor Vehicle Upholstery Worker	16.47
05280 - Motor Vehicle Wrecker	17.10
05310 - Painter, Automotive	19.03
05340 - Radiator Repair Specialist	17.10
05370 - Tire Repairer	13.96
05400 - Transmission Repair Specialist	18.41
07000 - Food Preparation And Service Occupations	
07010 - Baker	12.08
07041 - Cook I	11.10
07042 - Cook II	12.33
07070 - Dishwasher	9.05
07130 - Food Service Worker	8.63
07210 - Meat Cutter	13.70
07260 - Waiter/Waitress	8.86
09000 - Furniture Maintenance And Repair Occupations	
09010 - Electrostatic Spray Painter	16.22
09040 - Furniture Handler	12.62
09080 - Furniture Refinisher	17.27
09090 - Furniture Refinisher Helper	13.89
09110 - Furniture Repairer, Minor	15.47
09130 - Upholsterer	16.22
11000 - General Services And Support Occupations	
11030 - Cleaner, Vehicles	9.28
11060 - Elevator Operator	11.02
11090 - Gardener	14.44
11122 - Housekeeping Aide	12.96
11150 - Janitor	13.61
11210 - Laborer, Grounds Maintenance	12.35
11240 - Maid or Houseman	11.50
11260 - Pruner	12.96
11270 - Tractor Operator	13.53

11330 - Trail Maintenance Worker	12.35
11360 - Window Cleaner	13.78
12000 - Health Occupations	
12010 - Ambulance Driver	14.04
12011 - Breath Alcohol Technician	17.33
12012 - Certified Occupational Therapist Assistant	20.79
12015 - Certified Physical Therapist Assistant	18.88
12020 - Dental Assistant	14.32
12025 - Dental Hygienist	23.01
12030 - EKG Technician	22.90
12035 - Electroneurodiagnostic Technologist	22.90
12040 - Emergency Medical Technician	14.04
12071 - Licensed Practical Nurse I	15.31
12072 - Licensed Practical Nurse II	17.33
12073 - Licensed Practical Nurse III	19.33
12100 - Medical Assistant	12.39
12130 - Medical Laboratory Technician	16.83
12160 - Medical Record Clerk	14.13
12190 - Medical Record Technician	16.42
12195 - Medical Transcriptionist	14.26
12210 - Nuclear Medicine Technologist	24.86
12221 - Nursing Assistant I	10.49
12222 - Nursing Assistant II	11.79
12223 - Nursing Assistant III	12.87
12224 - Nursing Assistant IV	14.44
12235 - Optical Dispenser	13.89
12236 - Optical Technician	12.53
12250 - Pharmacy Technician	12.39
12280 - Phlebotomist	14.44
12305 - Radiologic Technologist	23.00
12311 - Registered Nurse I	23.50
12312 - Registered Nurse II	28.75
12313 - Registered Nurse II, Specialist	28.75
12314 - Registered Nurse III	34.78
12315 - Registered Nurse III, Anesthetist	34.78
12316 - Registered Nurse IV	41.68
12317 - Scheduler (Drug and Alcohol Testing)	21.47
13000 - Information And Arts Occupations	
13011 - Exhibits Specialist I	21.25
13012 - Exhibits Specialist II	27.77
13013 - Exhibits Specialist III	29.81
13041 - Illustrator I	19.11
13042 - Illustrator II	24.36
13043 - Illustrator III	26.32
13047 - Librarian	24.59
13050 - Library Aide/Clerk	10.34
13054 - Library Information Technology Systems Administrator	20.34
13058 - Library Technician	16.06
13061 - Media Specialist I	16.02
13062 - Media Specialist II	17.92

13063 - Media Specialist III		19.99
13071 - Photographer I		14.36
13072 - Photographer II		18.25
13073 - Photographer III		21.51
13074 - Photographer IV		25.13
13075 - Photographer V		30.38
13110 - Video Teleconference Technician		16.58
14000 - Information Technology Occupations		
14041 - Computer Operator I		15.90
14042 - Computer Operator II		17.79
14043 - Computer Operator III		19.84
14044 - Computer Operator IV		22.05
14045 - Computer Operator V		24.41
14071 - Computer Programmer I	(see 1)	22.35
14072 - Computer Programmer II	(see 1)	27.62
14073 - Computer Programmer III	(see 1)	
14074 - Computer Programmer IV	(see 1)	
14101 - Computer Systems Analyst I	(see 1)	
14102 - Computer Systems Analyst II	(see 1)	
14103 - Computer Systems Analyst III	(see 1)	
14150 - Peripheral Equipment Operator		15.90
14160 - Personal Computer Support Technician		22.05
15000 - Instructional Occupations		
15010 - Aircrew Training Devices Instructor (Non-Rated)		26.29
15020 - Aircrew Training Devices Instructor (Rated)		31.81
15030 - Air Crew Training Devices Instructor (Pilot)		37.86
15050 - Computer Based Training Specialist / Instructor		27.62
15060 - Educational Technologist		29.84
15070 - Flight Instructor (Pilot)		37.66
15080 - Graphic Artist		20.56
15090 - Technical Instructor		19.41
15095 - Technical Instructor/Course Developer		23.74
15110 - Test Proctor		16.96
15120 - Tutor		16.96
16000 - Laundry, Dry-Cleaning, Pressing And Related Occupations		
16010 - Assembler		9.28
16030 - Counter Attendant		9.28
16040 - Dry Cleaner		11.56
16070 - Finisher, Flatwork, Machine		9.28
16090 - Presser, Hand		9.28
16110 - Presser, Machine, Drycleaning		9.28
16130 - Presser, Machine, Shirts		9.28
16160 - Presser, Machine, Wearing Apparel, Laundry		9.28
16190 - Sewing Machine Operator		12.33
16220 - Tailor		13.09
16250 - Washer, Machine		10.04
19000 - Machine Tool Operation And Repair Occupations		
19010 - Machine-Tool Operator (Tool Room)		17.05
19040 - Tool And Die Maker		22.76
21000 - Materials Handling And Packing Occupations		
21020 - Forklift Operator		16.10

21030 - Material Coordinator	19.96
21040 - Material Expediter	19.96
21050 - Material Handling Laborer	18.10
21071 - Order Filler	13.89
21080 - Production Line Worker (Food Processing)	16.10
21110 - Shipping Packer	13.72
21130 - Shipping/Receiving Clerk	13.72
21140 - Store Worker I	13.55
21150 - Stock Clerk	17.17
21210 - Tools And Parts Attendant	16.10
21410 - Warehouse Specialist	16.10
23000 - Mechanics And Maintenance And Repair Occupations	
23010 - Aerospace Structural Welder	23.47
23021 - Aircraft Mechanic I	22.54
23022 - Aircraft Mechanic II	23.47
23023 - Aircraft Mechanic III	24.59
23040 - Aircraft Mechanic Helper	17.82
23050 - Aircraft, Painter	22.09
23060 - Aircraft Servicer	19.78
23080 - Aircraft Worker	20.91
23110 - Appliance Mechanic	19.92
23120 - Bicycle Repairer	13.96
23125 - Cable Splicer	26.97
23130 - Carpenter, Maintenance	20.21
23140 - Carpet Layer	17.94
23160 - Electrician, Maintenance	24.24
23181 - Electronics Technician Maintenance I	21.91
23182 - Electronics Technician Maintenance II	23.12
23183 - Electronics Technician Maintenance III	24.60
23260 - Fabric Worker	19.30
23290 - Fire Alarm System Mechanic	21.02
23310 - Fire Extinguisher Repairer	18.17
23311 - Fuel Distribution System Mechanic	22.44
23312 - Fuel Distribution System Operator	18.49
23370 - General Maintenance Worker	17.81
23380 - Ground Support Equipment Mechanic	22.54
23381 - Ground Support Equipment Servicer	19.78
23382 - Ground Support Equipment Worker	20.91
23391 - Gunsmith I	18.17
23392 - Gunsmith II	20.42
23393 - Gunsmith III	22.54
23410 - Heating, Ventilation And Air-Conditioning Mechanic	18.95
23411 - Heating, Ventilation And Air Contditioning Mechanic (Research Facility)	19.69
23430 - Heavy Equipment Mechanic	20.39
23440 - Heavy Equipment Operator	22.45
23460 - Instrument Mechanic	23.17
23465 - Laboratory/Shelter Mechanic	21.55
23470 - Laborer	14.78
23510 - Locksmith	18.41

23530 - Machinery Maintenance Mechanic	21.00
23550 - Machinist, Maintenance	20.25
23580 - Maintenance Trades Helper	16.43
23591 - Metrology Technician I	23.17
23592 - Metrology Technician II	24.11
23593 - Metrology Technician III	25.19
23640 - Millwright	25.25
23710 - Office Appliance Repairer	19.71
23760 - Painter, Maintenance	19.35
23790 - Pipefitter, Maintenance	27.98
23810 - Plumber, Maintenance	22.95
23820 - Pneudraulic Systems Mechanic	22.54
23850 - Rigger	22.54
23870 - Scale Mechanic	20.42
23890 - Sheet-Metal Worker, Maintenance	25.78
23910 - Small Engine Mechanic	17.11
23931 - Telecommunications Mechanic I	24.45
23932 - Telecommunications Mechanic II	25.32
23950 - Telephone Lineman	23.55
23960 - Welder, Combination, Maintenance	18.79
23965 - Well Driller	20.23
23970 - Woodcraft Worker	22.54
23980 - Woodworker	15.90
24000 - Personal Needs Occupations	
24570 - Child Care Attendant	10.71
24580 - Child Care Center Clerk	12.98
24610 - Chore Aide	10.15
24620 - Family Readiness And Support Services Coordinator	12.25
24630 - Homemaker	13.49
25000 - Plant And System Operations Occupations	
25010 - Boiler Tender	24.99
25040 - Sewage Plant Operator	20.44
25070 - Stationary Engineer	24.99
25190 - Ventilation Equipment Tender	17.79
25210 - Water Treatment Plant Operator	20.44
27000 - Protective Service Occupations	
27004 - Alarm Monitor	14.65
27007 - Baggage Inspector	10.28
27008 - Corrections Officer	21.65
27010 - Court Security Officer	22.91
27030 - Detection Dog Handler	14.84
27040 - Detention Officer	21.65
27070 - Firefighter	22.94
27101 - Guard I	10.28
27102 - Guard II	14.84
27131 - Police Officer I	24.82
27132 - Police Officer II	26.93
28000 - Recreation Occupations	
28041 - Carnival Equipment Operator	10.03
28042 - Carnival Equipment Repairer	10.42

28043 - Carnival Equpment Worker 8.54
28210 - Gate Attendant/Gate Tender 13.83
28310 - Lifeguard 10.94
28350 - Park Attendant (Aide) 15.47
28510 - Recreation Aide/Health Facility Attendant 11.29
28515 - Recreation Specialist 16.79
28630 - Sports Official 12.32
28690 - Swimming Pool Operator 18.27
29000 - Stevedoring/Longshoremen Occupational Services
29010 - Blocker And Bracer 21.51
29020 - Hatch Tender 21.51
29030 - Line Handler 21.51
29041 - Stevedore I 20.33
29042 - Stevedore II 22.51
30000 - Technical Occupations
30010 - Air Traffic Control Specialist, Center (HFO) (see 2) 35.77
30011 - Air Traffic Control Specialist, Station (HFO) (see 2) 24.66
30012 - Air Traffic Control Specialist, Terminal (HFO) (see 2) 27.16
30021 - Archeological Technician I 17.95
30022 - Archeological Technician II 18.28
30023 - Archeological Technician III 24.87
30030 - Cartographic Technician 25.30
30040 - Civil Engineering Technician 21.90
30061 - Drafter/CAD Operator I 18.25
30062 - Drafter/CAD Operator II 20.41
30063 - Drafter/CAD Operator III 22.77
30064 - Drafter/CAD Operator IV 28.00
30081 - Engineering Technician I 16.06
30082 - Engineering Technician II 18.06
30083 - Engineering Technician III 20.98
30084 - Engineering Technician IV 24.78
30085 - Engineering Technician V 30.31
30086 - Engineering Technician VI 36.67
30090 - Environmental Technician 21.50
30210 - Laboratory Technician 20.26
30240 - Mathematical Technician 25.30
30361 - Paralegal/Legal Assistant I 19.93
30362 - Paralegal/Legal Assistant II 24.70
30363 - Paralegal/Legal Assistant III 30.21
30364 - Paralegal/Legal Assistant IV 33.56
30390 - Photo-Optics Technician 26.70
30461 - Technical Writer I 21.84
30462 - Technical Writer II 25.69
30463 - Technical Writer III 28.75
30491 - Unexploded Ordnance (UXO) Technician I 22.74
30492 - Unexploded Ordnance (UXO) Technician II 27.51
30493 - Unexploded Ordnance (UXO) Technician III 32.97
30494 - Unexploded (UXO) Safety Escort 22.74
30495 - Unexploded (UXO) Sweep Personnel 22.74
30620 - Weather Observer, Combined Upper Air Or Surface Programs (see 2) 22.77

30621 - Weather Observer, Senior	(see 2)	25.30
31000 - Transportation/Mobile Equipment Operation Occupations		
31020 - Bus Aide		14.71
31030 - Bus Driver		18.40
31043 - Driver Courier		13.74
31260 - Parking and Lot Attendant		10.49
31290 - Shuttle Bus Driver		14.65
31310 - Taxi Driver		10.92
31361 - Truckdriver, Light		14.65
31362 - Truckdriver, Medium		17.07
31363 - Truckdriver, Heavy		18.69
31364 - Truckdriver, Tractor-Trailer		18.69
99000 - Miscellaneous Occupations		
99030 - Cashier		8.57
99050 - Desk Clerk		10.19
99095 - Embalmer		23.36
99251 - Laboratory Animal Caretaker I		12.22
99252 - Laboratory Animal Caretaker II		13.02
99310 - Mortician		27.76
99410 - Pest Controller		17.04
99510 - Photofinishing Worker		13.23
99710 - Recycling Laborer		18.05
99711 - Recycling Specialist		20.80
99730 - Refuse Collector		16.68
99810 - Sales Clerk		12.12
99820 - School Crossing Guard		10.25
99830 - Survey Party Chief		18.85
99831 - Surveying Aide		11.23
99832 - Surveying Technician		17.13
99840 - Vending Machine Attendant		14.01
99841 - Vending Machine Repairer		16.78
99842 - Vending Machine Repairer Helper		14.01

ALL OCCUPATIONS LISTED ABOVE RECEIVE THE FOLLOWING BENEFITS:

HEALTH & WELFARE: $3.59 per hour or $143.60 per week or $622.27 per month

VACATION: 2 weeks paid vacation after 1 year of service with a contractor or successor; 3 weeks after 8 years, and 4 weeks after 15 years. Length of service includes the whole span of continuous service with the present contractor or successor, wherever employed, and with the predecessor contractors in the performance of similar work at the same Federal facility. (Reg. 29 CFR 4.173)

HOLIDAYS: A minimum of ten paid holidays per year, New Year's Day, Martin Luther King Jr's Birthday, Washington's Birthday, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans' Day, Thanksgiving Day, and Christmas Day. (A

contractor may substitute for any of the named holidays another day off with pay in accordance with a plan communicated to the employees involved.) (See 29 CFR 4174)

THE OCCUPATIONS WHICH HAVE NUMBERED FOOTNOTES IN PARENTHESES RECEIVE THE FOLLOWING:

1) COMPUTER EMPLOYEES: Under the SCA at section 8(b), this wage determination does not apply to any employee who individually qualifies as a bona fide executive, administrative, or professional employee as defined in 29 C.F.R. Part 541. Because most Computer System Analysts and Computer Programmers who are compensated at a rate not less than $27.63 (or on a salary or fee basis at a rate not less than $455 per week) an hour would likely qualify as exempt computer professionals, (29 C.F.R. 541. 400) wage rates may not be listed on this wage determination for all occupations within those job families. In addition, because this wage determination may not list a wage rate for some or all occupations within those job families if the survey data indicates that the prevailing wage rate for the occupation equals or exceeds $27.63 per hour conformances may be necessary for certain nonexempt employees. For example, if an individual employee is nonexempt but nevertheless performs duties within the scope of one of the Computer Systems Analyst or Computer Programmer occupations for which this wage determination does not specify an SCA wage rate, then the wage rate for that employee must be conformed in accordance with the conformance procedures described in the conformance note included on this wage determination.

Additionally, because job titles vary widely and change quickly in the computer industry, job titles are not determinative of the application of the computer professional exemption. Therefore, the exemption applies only to computer employees who satisfy the compensation requirements and whose primary duty consists of:

(1) The application of systems analysis techniques and procedures, including consulting with users, to determine hardware, software or system functional specifications;

(2) The design, development, documentation, analysis, creation, testing or modification of computer systems or programs, including prototypes, based on and related to user or system design specifications;

(3) The design, documentation, testing, creation or modification of computer programs related to machine operating systems; or

(4) A combination of the aforementioned duties, the performance of which requires the same level of skills. (29 C.F.R. 541.400).

2) AIR TRAFFIC CONTROLLERS AND WEATHER OBSERVERS - NIGHT PAY & SUNDAY PAY: If you work at night as part of a regular tour of duty, you will earn a night differential and receive an additional 10% of basic pay for any hours worked between 6pm and 6am.

If you are a full-time employed (40 hours a week) and Sunday is part of your regularly scheduled workweek, you are paid at your rate of basic pay plus a Sunday premium of 25% of your basic rate for each hour of Sunday work which is not overtime (i.e. occasional work on Sunday outside the normal tour of duty is considered overtime work).

HAZARDOUS PAY DIFFERENTIAL: An 8 percent differential is applicable to employees employed in a position that represents a high degree of hazard when working with or in close proximity to ordinance, explosives, and incendiary materials. This includes work such as screening, blending, dying, mixing, and pressing of sensitive ordance, explosives, and pyrotechnic compositions such as lead azide, black powder and photoflash powder. All dry-house activities involving propellants or explosives. Demilitarization, modification, renovation, demolition, and maintenance operations on sensitive ordnance, explosives and incendiary materials. All operations involving regrading and cleaning of artillery ranges.

A 4 percent differential is applicable to employees employed in a position that represents a low degree of hazard when working with, or in close proximity to ordance, (or employees possibly adjacent to) explosives and incendiary materials which involves potential injury such as laceration of hands, face, or arms of the employee engaged in the operation, irritation of the skin, minor burns and the like; minimal damage to immediate or adjacent work area or equipment being used. All operations involving, unloading, storage, and hauling of ordance, explosive, and incendiary ordnance material other than small arms ammunition. These differentials are only applicable to work that has been specifically designated by the agency for ordance, explosives, and incendiary material differential pay.

** UNIFORM ALLOWANCE **

If employees are required to wear uniforms in the performance of this contract (either by the terms of the Government contract, by the employer, by the state or local law, etc.), the cost of furnishing such uniforms and maintaining (by laundering or dry cleaning) such uniforms is an expense that may not be borne by an employee where such cost reduces the hourly rate below that required by the wage determination. The Department of Labor will accept payment in accordance with the following standards as compliance:

The contractor or subcontractor is required to furnish all employees with an adequate number of uniforms without cost or to reimburse employees for the actual cost of the uniforms. In addition, where uniform cleaning and maintenance is made the responsibility of the employee, all contractors and subcontractors subject to this wage determination shall (in the absence of a bona fide collective bargaining agreement providing for a different amount, or the furnishing of contrary affirmative proof as to the actual cost), reimburse all employees for such cleaning and maintenance at a rate of $3.35 per week (or $.67 cents per day). However, in those instances where the uniforms furnished are made of "wash and wear" materials, may be routinely washed and dried with other personal garments, and do not require any special treatment such as dry cleaning, daily washing, or commercial laundering in order to meet the cleanliness or appearance standards set by the terms of the Government contract, by the contractor, by law, or by the nature of the work, there is no requirement that employees be reimbursed for uniform maintenance costs.

The duties of employees under job titles listed are those described in the "Service Contract Act Directory of Occupations", Fifth Edition, April 2006, unless otherwise indicated. Copies of the Directory are available on the Internet. A links to the Directory may be found on the WHD home page at http://www.dol.

gov/esa/whd/ or through the Wage Determinations On-Line (WDOL) Web site at http://wdol.gov/.

REQUEST FOR AUTHORIZATION OF ADDITIONAL CLASSIFICATION AND WAGE RATE {Standard Form 1444 (SF 1444)}

Conformance Process:

The contracting officer shall require that any class of service employee which is not listed herein and which is to be employed under the contract (i.e., the work to be performed is not performed by any classification listed in the wage determination), be classified by the contractor so as to provide a reasonable relationship (i.e., appropriate level of skill comparison) between such unlisted classifications and the classifications listed in the wage determination. Such conformed classes of employees shall be paid the monetary wages and furnished the fringe benefits as are determined. Such conforming process shall be initiated by the contractor prior to the performance of contract work by such unlisted class(es) of employees. The conformed classification, wage rate, and/or fringe benefits shall be retroactive to the commencement date of the contract. {See Section 4.6 (C)(vi)} When multiple wage determinations are included in a contract, a separate SF 1444 should be prepared for each wage determination to which a class(es) is to be conformed.

The process for preparing a conformance request is as follows:

1) When preparing the bid, the contractor identifies the need for a conformed occupation(s) and computes a proposed rate(s).

2) After contract award, the contractor prepares a written report listing in order proposed classification title(s), a Federal grade equivalency (FGE) for each proposed classification(s), job description(s), and rationale for proposed wage rate(s), including information regarding the agreement or disagreement of the authorized representative of the employees involved, or where there is no authorized representative, the employees themselves. This report should be submitted to the contracting officer no later than 30 days after such unlisted class(es) of employees performs any contract work.

3) The contracting officer reviews the proposed action and promptly submits a report of the action, together with the agency's recommendations and pertinent information including the position of the contractor and the employees, to the Wage and Hour Division, Employment Standards Administration, U.S. Department of Labor, for review. (See section 4.6(b)(2) of Regulations 29 CFR Part 4).

4) Within 30 days of receipt, the Wage and Hour Division approves, modifies, or disapproves the action via transmittal to the agency contracting officer, or notifies the contracting officer that additional time will be required to process the request.

5) The contracting officer transmits the Wage and Hour decision to the contractor.

6) The contractor informs the affected employees.

Information required by the Regulations must be submitted on SF 1444 or bond paper.

When preparing a conformance request, the "Service Contract Act Directory of Occupations" (the Directory) should be used to compare job definitions to insure that duties requested are not performed by a classification already listed in the wage determination. Remember, it is not the job title, but the required tasks that determine whether a class is included in an established wage determination. Conformances may not be used to artificially split, combine, or subdivide classifications listed in the wage determination.

Contractor Security Control Assessment (CSCA)

Self-Assessment Questionnaire for Contract Service Providers

Version 1.2

May 15, 2009

Document Change Control

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

Table of Contents

Executive Summary

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

Purpose

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

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

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

Scope

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

- Extending VA security mandates and education to affiliated contractor agencies;

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

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?:

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***

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.	☐	☐	

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?	☐	☐	

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

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

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?	☐	☐	

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

Requirement 5: Conduct Risk Assessments

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

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

Question	Response: (Select One)		Comment
	YES	NO	
1. Has a System of Records been created per the Privacy Act of 1974?	☐	☐	
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:			

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

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?	☐ ☐	☐ ☐	

Physical Security

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

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

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

Access to VA Information and VA Information Systems

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

Custodial Requirements

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

Question	Response: (Select One)		Comment
	YES	NO	
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)		Comment
	YES	NO	
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)		Comment
	YES	NO	
1. Does the organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures?	☐	☐	
2. Have all contractors/subcontractors signed the VA National Rules of Behavior?	☐	☐	
3. Have all contractors/subcontractors completed the VA approved security training?	☐	☐	
4. Have all contractors/subcontractors completed the VA approved privacy training?	☐	☐	

Appendix A. References

Department of Veterans Affairs
VA Directive 6500, *Information Security Program*.
VA Handbook 6500, Information Security Program
VA Handbook 6500.1 Electronic Media Sanitization
VA Handbook 6500.3 Certification and Accreditation

Federal Information Processing Standards
FIPS 140-2, Security Requirements for Cryptographic Modules
FIPS 190, Guideline for the Use of Advanced Authentication Technology Alternatives.
FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.
FIPS 201-1, Personal Identity Verification for Federal Employees and Contractors.

National Institute of Standards and Publications
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.
NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*.
NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*.
NIST SP 800-73, *Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV Card Application Namespace, Data Model and Representation, 2- End-Point PIV Card Application Interface, 3- End-Point PIV Client Application Programming Interface, 4- The PIV Transitional Data Model and Interfaces*.
NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*.
NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.
NIST SP 800-88, *Guidelines for Media Sanitization*.

SECTION E - SOLICITATION PROVISIONS

E.1 52.216-1 TYPE OF CONTRACT (APR 1984)

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

(End of Provision)

E.2 52.216-27 SINGLE OR MULTIPLE AWARDS (OCT 1995)

The Government may elect to award a single delivery order contract or task order contract or to award multiple delivery order contracts or task order contracts for the same or similar supplies or services to two or more sources under this solicitation.

(End of Provision)

E.3 52.217-5 EVALUATION OF OPTIONS (JUL 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

(End of Provision)

E.4 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

The contracting officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee's authority. A copy of the designation shall be furnished to the contractor.

(End of Provision)

E.5 VAAR 852.273-74 AWARD WITHOUT EXCHANGES (JAN 2003)

The Government intends to evaluate proposals and award a contract without exchanges with offerors. Therefore, each initial offer should contain the offeror's best terms from a cost or price and technical standpoint. However, the Government reserves the right to conduct exchanges if later determined by the contracting officer to be necessary.

(End of Provision)