PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

VistA Application Analytics (VAA)

July 30, 2024
VA-FY-24-00054128
Task Order PWS Version: 1.2

Contents

1.0 BACKGROUND

To aid maintenance and manageability of VistA, VA has migrated all VistA systems to the VA Enterprise Cloud (VAEC), a federally certified U.S. GovCloud managed by Amazon Web Services (AWS). By leveraging the built-in traffic logging capabilities of the VAEC-based VistA systems, VHA has the first-ever opportunity to analyze the actual clinical care workflows employed in VA medical centers. Such analysis would drive improved standards of practice by health care providers. These improvements would be prompted by the actual practice of care and not speculation about how care is being provided.

VA care is currently provided through VistA's point of care clients ('VistA Applications") which communicate with the VistA servers. Taken as a whole, these communications between VistA clients and VistA servers capture the patterns of clinical care activity performed today in VA. The Vista Application Analytics task order calls for health care data experts to analyze the traffic between VistA clients and three representative VistA servers. The analysis will be provided in a series of precise reports, detailing different aspect of VA care.

Analysis will include the types and volumes of structured and unstructured information read and written by clearly identified classes of health care professional as well as the range of time spent on different tasks. On completion, VHA will possess a set of concrete, actionable recommendations, and demonstrations for improving the care provided to Veterans as well as a guide for how to perform such analysis in the future.

2.0 APPLICABLE DOCUMENTS

The Contractor shall comply with the following documents, in addition to the documents in Paragraph 2.0 in the T4NG Basic Performance Work Statement (PWS), in the performance of this effort**:**

1. 44 U.S.C. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. VA Handbook 6500.6, "Contract Security," March 12, 2010
3. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)

3.0 SCOPE OF WORK

The Contractor shall analyze the traffic exchanged between VistA clients and a representative sample of VAEC-based VistA systems. These exchanges use VA's proprietary Remote Procedure Call (RPC) protocol. The Contractor shall use the built-in facilities of VAEC to capture this traffic non-invasively (without any need to change or

reconfigure the VistA system itself or its clients). From this captured data, the Contractor shall provide detailed analysis of representative traffic, identifying point-of-care applications, user behaviors, patterns of clinical use, and areas of concern. The Contractor shall reduce the production of this analysis to a repeatable process.

3.1 APPLICABILITY

This Task Order (TO) effort PWS is within the scope of paragraphs 4.1.5 and 4.2.11 of the T4NG Basic PWS.

3.2 ORDER TYPE

The effort shall be proposed on a Firm Fixed Price (FFP) basis.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The PoP shall be 12 months from date of award with one 12-month option period. The overall Period of Performance shall not exceed 24 months.

4.2 PLACE OF PERFORMANCE

Efforts under this TO shall be performed at Contractor facilities. The Contractor shall identify the Contractor's place of performance in their Task Execution Plan submission.

4.3 TRAVEL OR SPECIAL REQUIREMENTS

The Government anticipates travel to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program related meetings for this effort is two trips with two contractors per trip. Anticipated locations include the following, estimated at 2-3 days in duration:

1. Washington, D.C

4.4 CONTRACT MANAGEMENT

All requirements of Sections 7.0 and 8.0 of the T4NG Basic PWS apply to this effort. This TO shall be addressed in the Contractor's Progress, Status and Management Report as set forth in the T4NG Basic contract.

4.5 GOVERNMENT FURNISHED PROPERTY

Not Applicable.

4.6 SECURITY AND PRIVACY

All requirements in Section 6.0 of the T4NG Basic PWS apply. Addendum B requirements have been tailored to reflect the security and privacy requirements of this specific TO.

4.6.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Security and Suitability Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of this TO effort. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the TO.

The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide a monthly progress report to the Contracting Officer (CO) and Contracting Officer's Representative (COR) via electronic mail. This report shall include: (1) a summary of all project milestones and their anticipated completion dates, (2) invoicing data, (3) an assessment of current month and future month activities, and (4) a discussion of any issues related to contract performance or administration.

The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

Deliverable:

A. Monthly Progress Report

5.1.3 TECHNICAL KICKOFF MEETING

A technical kickoff meeting shall be held within 10 days after TO award. The Contractor shall coordinate the date, time, and location (can be virtual) with the Contracting Officer (CO), as the Post-Award Conference Chairperson, the VA PM, as the Co-Chairperson, the Contract Specialist (CS), and the COR.

The Contractor shall provide a draft agenda to the CO and VA PM at least five (5) calendar days prior to the meeting. Upon Government approval of a final agenda, the Contractor shall distribute to all meeting attendees. During the kickoff-meeting, the Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort via a Microsoft PowerPoint presentation. At the conclusion of the meeting, the Contractor shall update the presentation with a final slide entitled "Summary Report" which shall include notes on any major issues, agreements, or disagreements discussed during the kickoff meeting and the following statement "As the Post-Award Conference Chairperson, I

have reviewed the entirety of this presentation and assert that it is an accurate representation and summary of the discussions held during the Technical Kickoff Meeting for the VistA Application Analytics effort." The Contractor shall compile the PowerPoint into a Microsoft Word document and submit the final Microsoft Word document to the CO for review and signature within three (3) calendar days after the meeting.

The Contractor shall also work with the CS, the Government's designated note taker, to prepare and distribute the meeting minutes of the kickoff meeting to the CO, COR and all attendees within three (3) calendar days after the meeting. The Contractor shall obtain concurrence from the CS on the content of the meeting minutes prior to distribution of the document.

5.2 VISTA CLIENT TRAFFIC CAPTURE AND ANALYSIS (Base Period)

5.2.1 CAPTURE OF VISTA CLIENT TRAFFIC

The Contractor shall coordinate the use of built-in VAEC facilities to non-invasively log the VistA client traffic (RPC traffic) of VAEC-hosted VistAs for a representative period. As a non-invasive method, it will not require any change, reconfiguration, interfaces, development, patches, or plugins in the VistA system itself or any client communicating with that VistA.

The Contractor shall coordinate the logging of all client traffic of three VAEC-based production VA VistAs ("Analyzed VistAs"). At least one of the VistAs should support a large integrated medical facility.

The Contractor shall:

a) In collaboration with the Government, identity three VistAs and obtain permission from their managers to capture their RPC traffic.
b) Coordinate the configuration of the RPC Traffic capture to log all RPC traffic for these three VistAs.
c) Monitor and ensure traffic logging of each of the three identified VistAs for at least one month and the storage of all captured data in VAEC for analysis.
d) Develop and provide a VistA Traffic Logging Standard Operating Procedure to document the processes and procedures used to log required traffic from any VistA, including permissions required from VistA owners and VAEC maintainers

Deliverables:

A. VistA Traffic Logging Standard Operating Procedure

5.2.2 ANALYSIS OF VISTA CLIENT TRAFFIC

Using the client traffic captured (deliverable 5.2.1A) , the Contractor shall provide Traffic Analysis Reports comprising the complete client traffic for each of the three analyzed VistAs. In addition, the Contractor shall provide a Cross VistA Analysis Report distinguishing cross-VistA from VistA-specific traffic patterns. All four reports (i.e. 3 Traffic Analysis Reports and 1 Cross VistA Analysis Report) shall be composed in GitHub compatible markdown with embedded graphics where appropriate. The Contractor shall store all four reports as markdown in the VA Enterprise GitHub.

Traffic Analysis Report for each VistA shall characterize:

a) User volume
b) Client types and volume of use
c) Connection volumes, frequency, and duration
d) Types of user authentication/security and relative use
e) Machine from end Users
f) RPC usage frequency and execution times
g) RPC groupings – representing transactions
h) RPCs specific to a VistA from cross-VistA RPCs

Deliverables:

A. Traffic Analysis Reports for three production VistAs
B. Cross VistA Traffic Analysis Report

5.2.3 ANALYSIS OF USE OF KEY VISTA CLIENTS

Based on the traffic and client types isolated during the VistA traffic analysis, the Contractor shall produce a detailed Client Traffic Analysis of the operation of three of the most used VistA point-of-care applications ("Clients"). CPRS shall be one of the three; the remaining two shall be chosen after project start based on client usage. All three reports shall be composed in GitHub compatible markdown with embedded graphics where appropriate. The Contractor shall store the three reports in a git in the VA Enterprise GitHub. All client analyses must be validated and verifiable in a demonstrable way, matching RPC flows to specific client screens and typical tasks. The Contractor shall document the verification and validation of the analysis and provide a Client Traffic Analysis Validation and Verification Report.

The per Client Traffic Analysis shall include:

a) User volumes and types. User types shall capture clinical care specialties and roles.
b) Connection volume and duration, tying frequency of client use to user types
c) Types of user authentication/security and relative use
d) Patient volumes

e) Enumeration of all RPCs used by a client and their relative use
f) Distinction of clinical from non-clinical RPCs
g) Distinction of RPCs that change (write) from those that read the clinical record
h) Distinction of slow running, high overhead and variable overhead RPCs
i) Clinical care task sets, represented as groups of RPCs used in tandem
j) Match task sets with the use of one or more specific client screens
k) Task sets employed by different user types
l) Isolate performance issues with patterns of use that slow care
m) Verification and validation that the analysis accurately captures care provision

Deliverables:

A. Three (3) VistA Client Use Analysis Reports
B. Client Analysis Validation and Verification Report

5.2.4 VISTA CLIENT USE IMPROVEMENT REPORT

Based solely on the Client Use Analysis Reports, the Contractor shall provide recommendations to upgrade the use of the top three RPC-using Point-of-Care VistA Clients to deliver better clinical care. These recommendations shall be documented in Client Use Improvement Reports for each Client in Microsoft Word and a supporting PowerPoint presentation.

Deliverables:

A. Client Use Improvement Reports

5.3 VISTA CLIENT TRAFFIC CAPTURE AND ANALYSIS [OPTION PERIOD 1]

This option will take the approach to non-invasive traffic analysis used in the base period, and extend its application to other types of VistA traffic and scenarios.

5.3.1 MIGRATED VISTA CLIENT TRAFFIC ANALYSIS

Post Cerner migration, the VistA of a migrated site (“Migrated VistA”) is still in production, running a subset of its previous functionality.

Client traffic for one month from a Migrated VistA shall be captured, using the same mechanism employed in the base period (5.2.1).

Migrated VistA Traffic Analysis Report shall include:

- Identify which clients are still in use and how they are used
- Identify the type and volume of users still operating in this VistA
- Identify the subset of RPCs still being used – compare to the range of RPCs used in full VistAs analyzed in year one.

Deliverables:

A. Migrated VistA Traffic Analysis Report

5.3.2 VISTA COMMUNITY CARE CLIENT TRAFFIC ANALYSIS

An increasing amount of veteran care is provided outside VA in the private sector ("Community Care").

Client traffic for one month reflecting Community Care from a production VistA shall be isolated and captured using the same mechanism employed in the base period (5.2.1).

The Vista Community Care Traffic Report shall include:

- Types, volumes, and sources of parseable text
- Types, volumes, and sources of references to images/screenshots
- Where and how this information is displayed in pre-existing and specialized VistA clients
- Recommendations how to better integrate this external information with clinical and other data within VA

Deliverable:

A. VistA Community Care Traffic Analysis Report

6.0 GENERAL REQUIREMENTS

6.1 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Provides quality services/products	Satisfactory or higher

Performance Objective	Performance Standard	Acceptable Levels of Performance
B. Project Milestones and Schedule	1. Products completed, reviewed, delivered in accordance with the established schedule 2. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Level of expertise and staffing appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the TO to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.2 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

Not Applicable

6.3 SHIPMENT OF HARDWARE OR EQUIPMENT

Not Applicable.

6.4 ENTERPRISE AND IT FRAMEWORK

Not Applicable

6.5 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

Not Applicable

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, 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 are 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.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. 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 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).

2. 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 information is returned to 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.

3. 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 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 CO within 30 days of termination of the contract.

4. 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 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.

5. 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.

6. 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.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Directive 1605.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. 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.

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

10. 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 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 CO for response.

11. 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 CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (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 COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not Applicable.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

Not Applicable.

B6. 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 COR 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.

B7. 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. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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 Breaches Involving Sensitive Personal Information*, 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 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.

B8. 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-days' 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.

B9. 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 VA Information Security Rules of Behavior, relating to access to VA information and information systems;

2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS 2.0 # VA 10176) and complete this required privacy and information security training annually;

3) 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 CO 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 CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically 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.