PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Informatics and Analytics (OIA)
Standards & Interoperability (S&I)

Security Software Architecture (Project No. HI 16-9)

Date: 8/12/2016

PWS Version Number: 2.2

Contents

1.0 BACKGROUND

The Department of Veterans Affairs (VA) engages in effective use of state-of-the-art Information Technology (IT) activities both inside and outside of the enterprise boundaries that depend upon healthcare standards and standards development. The integrity of VA health information systems require common processes, terms and information attributes to support clinical use, as well as common mechanisms to ensure security, privacy and patient safety. Health information standards development organizations meet these needs by providing the common information attributes upon which VA IT systems depends. Because of the importance of standards in VA healthcare operations, VA participates actively in multiple Standards Development Organizations (SDO) and Standards Related Organizations (SRO).

In addition, the VA must integrate standards into its business processes and health information systems. In particular, standards affect the way that information is stored and used, and the protocols that must be observed to achieve interoperability between systems and business partners. Accordingly, healthcare standards must be integrated into line of business requirements, health informatics and system design and engineering.

Standards cover a diverse range of information and specifications and can be as simple as defining how the state field in an address is exchanged (e.g. abbreviated state code vs. spelled out) or as complex as a collection of standards necessary to support the security framework essential to protect health information entrusted to our care.

Work Group Requirements

The order requirements are subdivided into four (4) Work Groups (WG), each with corresponding objectives and discrete tasks and deliverables. For all deliverables under this order, the Contractor shall create and maintain a shareable repository organized by Work Group task of relevant engineering artifacts (engineering folders) consistent with best practices of the Carnegie Mellon Software Engineering Institute. The repository shall be maintained in Microsoft Office SharePoint Workspace and contain the final Government approved deliverable as well as plans, drafts, graphics, references, and working papers used in its development.

Work Group 1 – VHA Healthcare Security and Privacy Informatics Standards Development and Application

The purpose of Work Group 1 is to maintain interoperable healthcare security and privacy information models meeting VHA's healthcare line of business security and privacy informatics needs and which represent healthcare business context.

Standards-based interoperable domain analysis models are created and integrated within VA/VHA security, privacy, and healthcare systems to enforce Veteran privacy preferences and organizational policy. Models conform to Health Level 7 (HL7) Service-Award Interoperability Framework (SAIF) Conceptual Specification requirements based on Reference Model of Open Distributed Processing (RM-ODP) including vocabulary reflecting VHA business definitions.

SDO activities include: creating; balloting and reconciling modeling and information standards; participating in terminology related working groups; writing and presenting papers/presentations; and reviewing and making recommendations on papers produced by external organizations as well as meeting preparation and attendance. Objectives include: creating, balloting, reconciling within SDO's, and informing, integrating supporting standards adoption within VA. To accomplish these goals and activities, the Contractor participates in Standards Development Organizations (SDO's) to create and maintain interoperable security and privacy informatics standards that can be used by VHA and its healthcare partners nationwide. Principal support is directed towards VistA Evolution (VE) and its respective programs [Joint Legacy Viewer (JLV), Electronic Health Management Platform (eHMP), Veteran Authorization Preferences (VAP), VistA]. VE efforts are also activities related to and benefit the exchange of patient protected healthcare information supporting legacy eHealth Exchange, and Direct.

Work Group 1 – Overarching Objectives

The Contractor shall conduct SDO/SRO activities producing interoperable U.S. domain analysis models including metadata supporting VA activities for Identity Management, Identity and Access Management (IAM), Authentication and Authorization, Security Labeling, Release of Information, Patient Consent, and other services supporting Veteran security and privacy as applied to VA/VHA healthcare information systems.

The Contractor shall: Provide maintenance and update to the HL7 and associated artifacts/models, and maintain ISO Standards Tracking Worksheet of ISO TC215 WG4 and SC27 security and privacy standards development for healthcare informatics review/ballot tracking purposes.

Work Group 1 – Technical Objectives

The Contractor shall participate (as committee member or co-chair) in the development of informatics standards through standards development organizations and standards related organizations identified in the VHA healthcare Security and Privacy Informatics Development category. Projects in these groups vary, however, participation is intended to ensure VHA has the opportunity to review and participate in work activities and vote on proposed ballots (actual voting will be done by the Project Manager (PM) or designated VHA representatives). Principal focus is Tier 1 SDO's such as HL7 and Organizations for the Advancement of Structured Information Standards (OASIS) – see technical objective II below. Tier 2 SDO's includes the American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS), the International Organization for Standards (ISO), and the National Institute for Standards Technology (NIST). The Contractor shall participate in VHA led SDO/SRO healthcare security and privacy projects attending Security and Privacy Working Group meetings, providing meeting materials (presentations, Working Group technical input/reviews, ballot/ballot reconciliation materials, and meeting minutes).

> **Technical Objective I:** The Contractor shall participate in Tier 1 SDO's such as HL7 and OASIS. Activities in Tier 1 SDO's include attending technical committee (including physical) meetings, ballot technical input/reviews, and harmonization. Tier 1 activities principally involve an active participatory role, creating new standards, updating existing standards, vocabulary harmonization directly applicable to VHA programs and projects.

Technical Objective II: The Contractor shall participate in Tier 2 SDO's such as American Society for Testing and Materials (ASTM), IHE, and ANSI-INCITS. Activities in Tier 2 SDO's include attending technical committee (virtual) meetings, ballot technical input/reviews and harmonization with Tier 1 standards where appropriate. Tier 2 activities principally involve a monitoring role as VHA currently does not lead any active security and privacy initiatives there.

Technical Objective III: The Contractor shall provide HL7 standard security and privacy information model input to the Department of Health and Human Services (DHHS) with the goal of establishing a standards-based U.S. security and privacy information model. The Contractor shall provide a VHA specific version of theHL7 information model in support of the VA unified security architecture and project teams.

Technical Objective IV: The Contractor shall provide a tracking report of ISO TC215 WG4 and SC27 new work items, drafts and ballots so that VA can plan and consolidate inputs and responses to VHA work items responding to ANSI INCITS CS1 and the US TAG to ISO TC215 committee actions.

Technical Objective V: The Contractor shall provide quality assurance (QA) and control, consistent document formatting, and administrative procedures and reporting. QA functions as a central clearing house for document reviews for clarity, proper technical writing, adherence to established style standards (available upon contract award) and content for this and three (3) other contracts. Reviews will consist of corrections and inline comments for areas requiring clarification working with the author. Documents include internal reports, presentations, and external material presented to DHHS, or other Federal Departments including all standards drafts and final copies submitted for ballot or reconciliation. Document corrections need to be tracked in a consolidated listing by version and final, type, and other attributes. QA functions include management of three (3) SharePoint sites containing several hundred security documents, a Wiki, and quality review of VHA Security Groove spaces. QA also provides central status reporting of security activities and consolidation of reports support three (3) other VHA security and privacy supporting contracts.

Work Group 2 – Security Requirements Steering Committee (SRSC) Support

The Contractor shall summarize VHA healthcare line of business interests in healthcare privacy and security standards requirements that may be deemed by the VA Security Requirements Steering Committee as supportive of VHA business requirements. The VA SRSC exercises oversight authority in regard to the development and approval of enterprise cross-cutting security and privacy requirements for use within VA. The SRSC maintains ultimate responsibility for gathering and validating of all security requirements, submission of the security requirements to the VA Enterprise Requirements Repository, negotiation of those requirements through Peer Review, tracking those requirements through the approval and base-lining process, ensuring requirements are allocated and traceable to the project level, and tracking the requirements through the VA change management processes. Activities shall be conducted in accordance with the SRSC Charter and operational procedures and guidelines (available upon contract award).

Work Group 2 – Overarching Objectives

The Contractor shall perform tasks and provide deliverables related to developing, balloting and managing VA and VA administration line of business security requirements, coordinating with Office of Information and Technology (OI&T), VA, and Administration stakeholders and VA projects. In performing these duties the overarching objective is to produce an enterprise-wide authoritative view of security and privacy that include VHA healthcare-specific needs and which can be used by VA leadership, developers, operational staff, policy/administrative authorities, line of business requirements developers, and system architects. To achieve these overarching objectives, SRSC activities must support a number of technical activities including:

- A single authoritative view of cross-cutting security requirements across the VA enterprise
- Compliance with NIST, and other VA adopted Standards
- Compliance with VA, Administration and Federal security policies and requirements governance
- Consistency with Administration line of business security and privacy requirements
- Review of requirements for security relevance and assignment of the "Security Control" attribute based on the NIST Special Publication (SP) 800-53 Security Controls standards
- Preparation and coordination of SRSC meetings
- Ongoing review of requirements for omissions and follow-up actions to correct errors, interpretations for clarity
- Requirements management such that no requirement can be assigned to more than one service without breaking the parent into child requirements so that that each child is assigned to one and only one service
- Presentation of Specialized views of security and privacy requirements supporting developmental, operational and VA line of business users
- Preparation of SRSC Ballots, including parsing of source materials, conduct of ballot activities, and resolution of comments
- Allocation and maintenance of SRSC balloted requirements within the VA Enterprise Requirements Repository
- Creation of security specific Requirements Management (RM) processes, as necessary, to facilitate operation of the SRSC

Work Group 2 – Technical Objectives

Provide all activities required for the conducting of SRSC ballots (consistent with the overarching objectives and SRSC established procedure), with results collated, reconciled, and reported to affected stakeholders. Included are SRSC administrative processes for the conduct of SRSC activities, periodic SRSC meetings to ensure the smooth operation of the SRSC, it's interaction with OI&T and VA line of business stakeholders, including the management of the activities of the SRSC Technical Advisory Group (TAG) and maintenance of the SRSC database of proposed and approved security and privacy requirements and their disposition.

Work Group 3 – Role and Business Rule Engineering and Support

The purpose of role attribute and business rule support is to create and manage healthcare line of business role and security attributes in order to provide a single authoritative repository of VHA access control information for enforcement by VA's Identity and Access Management (IAM) security services.

Work Group 3 – Overarching Objectives

The overarching objective is to support the VHA healthcare line of business in collaboration with the OI&T by providing VHA security and privacy business role, attribute and rule definitions needed to provision VA's enterprise identity and access management (IAM) systems. It supports the VHA by defining standardized permissions for role-and attribute-based access control (RBAC/ABAC) and the definition of security and privacy business rules through analysis and modeling of line of business workflow, tasks and business processes. In addition, activities include reviews of Veteran privacy rules. The objective provides for inclusion into the overall policy sets needed to determine access to VA operational systems containing personally identifiable information. The following activities define the substance of the overarching objectives:

- Participation in role, attribute governance activities with OI&T and Identity and Access Management, such as IAM's Enterprise Access Control Board (EACB)
- Coordination of VHA role engineering activities with Kaiser Permanente, Department of Defense (DoD) and Indian Health Service (IHS)
- Coordination with VHA healthcare line of business elements and subject matter experts to define and catalog security and privacy related roles and rules
- Maintenance of VA role engineering information according to the specifications of the VA Role Engineering process
- Act as the repository of VHA business models, use cases coordinating the collection, maintenance and harmonization of HIPAA security and privacy
- Support for activities providing updates to HL7's healthcare role and attribute engineering permissions vocabulary standard
- Support to specialized line of business services (e.g., clinical definition of healthcare constraints and obligations vocabularies)
- Maintain the authoritative store of VHA Basic and Functional Role permission and attribute/clearance definitions
- Provide guidance and support for mapping to VA standard roles for VHA project information system internal and proprietary roles

Work Group 3 – Technical Objectives

Technical Objective I: Through activities of healthcare policy governance, define and publish authoritative catalogues of VHA cross-cutting permissions and corresponding roles and other information (aligned to specific lines of business) needed to provision access control decision

information repositories and to make and enforce security and privacy decisions for access to VHA protected information.

Technical Objective II: Manage and maintain VHA administrative processes for the conduct and communication of all activities to stakeholders and management. Conduct/participate in meetings as needed to ensure the smooth interaction with OI&T and VA stakeholders. Other activities include the maintenance of the VHA RBAC Task Force (TF) database of permissions, constraints, structural and functional roles and attributes via a VHA RBAC SharePoint.

Work Group 4 – VA Enterprise Access Control Board (EACB) Support

The Department of Veterans Affairs (VA) Enterprise Access Control Board (EACB) acts as the authoritative source for technical VA-wide security and privacy terminology, identifiers, and recommends standard interoperable terminology (attributes) which provides the basis for common access to EACB subscribing applications. VHA participates in the EACB and will actively collaborate on defining and maintaining jointly agreed upon Information Technology (IT) vocabulary needed to support security and privacy authorizations in shared DoD and VA VistA Evolution applications.

Work Group 4 – Overarching Objectives

The contractor shall perform tasks and provide deliverables related to the EACB in support to establish, manage, and provide authoritative access control attributes (known as clearances) required to implement VHA security and privacy within VistA Evolution and related and supporting projects/programs. In performing these duties the overarching objective is to define and maintain jointly agreed on IT vocabulary needed to support healthcare security and privacy authorizations in DoD and VA VistA Evolutions related applications. To achieve these overarching objectives, VHA activities must support number of technical activities including:

- Maintains and publishes a catalog of standard interoperable VHA user roles, clearances and associated constraints
- Maintains and publishes a catalog of standard interoperable access attributes for use by VHA subscribing applications
- Maintains an information model mapping DoD/VA formally approved information classes to standard attributes
- Coordinates with HHS Federal Health Information Modeling and Standards (FHIMS) regarding alignment of VHA and Federal models
- Evaluates policies regarding the protection of electronic health information shared among federal health care organizations
- Provide a common reference for access control that can be used for governance purposes
- Provides support for planning and interoperability testing for VHA subscribing applications
- Acts as an authority to review potentiality proprietary and department unique access terminology making recommendations to the health architecture review board making exceptions and waivers
- Serve as an advisory source of expertise for development of access control use cases

Work Group 4 – Technical Objectives

Technical Objective I: The contractor shall participate (as committee member) in activities of the VA EACB, establish, manage, and provide authoritative access control attributes required to implement DoD/VA security and privacy within VistA Evolution subscribing applications. Projects supported may vary, however, participation is intended to ensure VHA has the opportunity to manage, review, and participate in relevant work activities.

Technical Objective II: The contractor shall provide updates on EACB administrative processes as needed for the conduct and communication of all activities to VHA stakeholders and management. Conduct periodic meetings and guides support for the analysis, development, collaboration of EACB artifacts, and recommendations. Other activities include maintain electronic collaboration space and document manager, support productive DoD/VA EACB Subgroup engagements, and conduct requirements and business process analysis for functional domains under review by the VA EACB.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," May 18, 2007
9. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
10. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
11. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
12. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004

16. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
17. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
18. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
19. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
20. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of Va Information Systems,” February 3, 2014
21. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010
23. Project Management Accountability System (PMAS) portal (reference PWS References - Technical Library at https://www.voa.va.gov/)
24. OI&T ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
25. Technical Reference Model (TRM) (reference at https://www.voa.va.gov/)
26. National Institute Standards and Technology (NIST) Special Publications (SP)
27. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
28. VA Directive 6300, Records and Information Management, February 26, 2009
29. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
30. OMB Memorandum, “Transition to IPv6”, September 28, 2010
31. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
32. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
33. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
34. OMB Memorandum 05-24, Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
35. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
36. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
37. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
38. NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems, November 20, 2008
39. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
40. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013

41. Draft NIST Special Publication 800-157, Guidelines for Derived Personal Identity 523 Verification (PIV) Credentials, March 2014
42. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in 525 Mobile Devices (Draft), October 2012
43. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
44. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference Enterprise Architecture Section, PIV / IAM https://www.voa.va.gov/)
45. VA Memorandum, VAIQ # 7100145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM https://www.voa.va.gov/)
46. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM https://www.voa.va.gov/)

3.0 SCOPE OF WORK

Activities within scope include participation in or providing support to a wide range of security and privacy standard generally to related activities both external and internal to the Department of Veterans Affairs (VA).

More specifically, Software Security Architecture is focused on activities specific to VHA's legal responsibilities as VHA's designated Health Insurance Portability and Accountability (HIPAA) provider for healthcare, healthcare security informatics, healthcare security and privacy business workflow including healthcare security and privacy information models requirements and requirements management. Application analysts support the development of healthcare domain security and privacy vocabulary and standards within Health Level 7 (HL7) crucial to the analysis of security and privacy requirements supporting VHA clinical systems and programs. Software Security Architecture provides:

- Healthcare standards support related to creating, balloting and maintaining information, information models, vocabularies and code sets defining security and privacy healthcare domain concepts and attributes.
- Support for managing healthcare business security and privacy requirements including those that are cross-cutting requirements across the Department.
- Monitors VHA relevant external security and privacy standards.

Core activities include support to VA's engagement with healthcare security standards and standards influencing organizations such as:

- American National Standards Institute (ANSI)
- ANSI International Committee for Information Technology Standards (INCITS)
- Health Level Seven (HL7)
- Internet Engineering Task Force (IETF)
- Integrating the Healthcare Enterprise (IHE)
- International Standards Organization (ISO)
- KANTARA

- National Institute of Standards and Technology (NIST)
- Organization for the Advancement of Structured Information Systems (OASIS)
- Object Management Group (OMG)
- World Wide Web Consortium (W3C)

In addition, the VHA must integrate healthcare security and privacy standards into its business processes and health information systems. In particular, standards affect the way that information is stored and used, and the protocols that must be observed to achieve interoperability between/among systems and business partners. Accordingly, healthcare standards must be integrated into all aspects of line of business requirements and health informatics affecting health information system design and engineering.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be twelve (12) months from date of award plus four (4) twelve (12) month option periods.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed primarily at the Contractor's facility. Additional work may be required at the travel locations indicated in the "Travel" section.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort throughout the period of performance. The Government will reimburse the cost of travel required. This includes travel, subsistence, and associated labor charges for travel time. Reimbursement for travel is limited to that required in the performance of the contract. Specific Government direction to attend meetings or gather information shall be reimbursed on a cost-reimbursable basis only. All travel shall be in accordance with the Federal Travel Regulations (FTR). Local travel, within a 50-mile radius from the Contractor's facility or the relocation of contractor personnel from other geographic areas for the purpose of staffing a contract is considered the cost of doing business and is not subject to reimbursement. The Government will not pay travel charges for travel to and from the Contractor employee's home and Government Office or to and from one company building to another (either within a company or to and from a price to a sub company. Travel, subsistence, and associated labor charges for travel time for travel beyond a 50-mile radius of the Contractor's facility are authorized for reimbursement on a case-by-case basis and must be pre-approved by the Contracting Officer's Representative (COR). Travel costs subject to reimbursement are limited to travel occurring at the direction of the Government, performed in conjunction with a specific requirement for a trip authorized in the contract. Any administrative/clerical support travel costs shall be considered and approved by the Contracting Officer (CO) on a case-by-case basis. Travel shall be reflected on the contract as a separate, reimbursable line item with a not-to exceed (NTE) total expenditure. Travel will be requested, approved and reimbursed in accordance with the contract.

Registration fees associated with travel shall be priced separately from travel. The Government will reimburse the Contractor for actual costs associated with the fees. The Contractor shall submit an invoice with registration fee receipt to be reimbursed. No profit, overhead, or other costs associated with registration fees will be paid by the Government.

The contractor must obtain written approval from the Veterans Affairs (VA) CO (or the designated back-up when the VA Contracting Officer is out of the office) **BEFORE** any travel begins, utilizing the Travel Authorization Request (see Attachment A). Travel and per diem expenses will be reimbursed on an actual expenditures basis in accordance with Federal Travel Regulations and FAR 31.205-46. Travel that occurs without written pre-approval will **NOT** be reimbursed. The contractor **MUST** use attachment - Travel Authorization Request for travel pre-approval. Other documents or e-mails will **NOT** be accepted as pre-approval.

In order to be reimbursed for travel, the contractor shall submit supporting documentation as required by Federal Travel Regulations with invoices. Federal Travel Regulations require for any temporary travel destination you must provide a receipt to substantiate your claimed travel expenses for lodging and a receipt for any authorized expenses costing over $75. (FTR 301-11.25). Expenses for subsistence and lodging will be reimbursed to the contractor only to the extent where an overnight stay is necessary and authorized by Federal Travel Regulations in effect at the time of the stay for the specific location.

Approval for rental vehicles is discouraged and will be approved on an individual basis. Additional information can be found at: http://www.gsa.gov/ftr .

The Government estimates the following travel:

The Government anticipates three (3) trips for HL7 working group meetings (3 trips). Locations are to be determined (TBD) and will be published by HL7.

TRAVEL			
Estimated Locations	**Approximate Number Of Trips Per Contract Year**	**Approximate Number Of Contractor Personnel Required Per Trip**	**Approximate Number Of Days Per Trip**
HL7 TBD	1	2	5
HL7 TBD	1	2	5
HL7 TBD	1	2	5

The Government anticipates one (1) trip for VHA Standards Coordination Purposes.

TRAVEL			
Estimated Locations	**Approximate Number Of Trips Per Contract Year**	**Approximate Number Of Contractor Personnel Required Per Trip**	**Approximate Number Of Days Per Trip**
Washington, DC	1	2	5

4.4 TYPE OF ORDER

Firm-Fixed-Price (FFP)

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 STANDARDS DEVELOPMENT ORGANIZATION (SDO) ACTIVITIES

The Contractor shall participate in Standards Development Organization (SDO) and Standards Related Organizations (SRO). Participation includes attending meetings, writing and presenting papers, ballot materials, project scope statements, and reviewing papers produced by external organizations. Coordinate the ongoing development of the committee standards. Tasking includes meeting preparation and attendance, standards maintenance and enhancement, and coordination with internal members.

5.1.1. Tier 1 SDO HL7 Working Group Support:

The Contractor shall attend meetings and participate in Tier 1 SDO activities of HL7 Working groups including Security, Privacy, Service Oriented Architecture and Electronic Health Records. Present three (3) four (4)-month summaries of Tier 1 activity (PowerPoint format) reviewing current and proposed activities with HL7 ballot material including Project Scope Statements, Notices of Intent to Ballot, Administrative Ballot Submissions, Ballot Content, and perform Ballot reconciliation activities in accordance with the HL7 Governance and Operations Manual. Activity areas include:

- HL7 RBAC/ABAC vocabulary supporting authorization to and Security Labeling of healthcare clinical content
- SOA Pass Access Control Conceptual Model vocabulary
- CBCC Security and Privacy Information Model
- CBCC Vocabulary Harmonization
- EHR Vocabulary
- Security and Privacy Ontology
- HCS Vocabulary, HCS Business Requirements
- Data Segmentation for Privacy (General)
- FHIM Vocabulary coordination, vocabulary harmonization
- CBCC Fast Healthcare Interoperability Resource (FHIR)
- EHR, Security, CBCC Vocabulary Joint Projects
- Natural Language Processing (NLP) vocabulary development

DELIVERABLE 5.1.1 – Prepare HL7 Activity Report Summary including: HL7 Service Oriented Architecture Audit; HL7 CBCC (Privacy) Joint Security and Privacy Information Model; HL7 CBCC (Privacy) Data Segmentation for Privacy Implementation Guide; HL7 CBCC (Privacy) FHIR Questionnaire; and HL7 CBCC (Privacy) FHIR Electronic Health Repository (EHR) Security, Privacy, and Provenance vocabulary alignment.

5.1.2. HL7 Role and Attributed-Based Security and Privacy Vocabulary and Informatics Standards:

The Contractor shall produce, maintain, and update HL7's role and attributes-based security and privacy vocabulary and informatics standards in support of VHA's VistA Evolution program, and VA's planned Enterprise Access Control Board.

DELIVERABLE 5.1.2. – Provide security, service-oriented architecture, and privacy oriented business vocabulary additions, validation, and updates for role and attributes-based access control.

5.1.3. HL7 Security Working Group Meeting Agendas and Minutes Support

The Contractor shall provide support for HL7 Security Working Group Meetings by preparing HL7 Security Working Group Meeting Agendas and Minutes (prepare proposed agenda beforehand), usually one to two days in advanced, delivered in a meeting announcement, however, agendas may be modified during the meeting upon the request of participants and minutes covering the meeting proceedings afterwards. The Contractor shall enter Agendas and Minutes into the official HL7 Wiki and GForge site maintained by the Working Group for active projects.

DELIVERABLE 5.1.3. – Prepare HL7 Security Working Group Meeting Agendas and Minutes.

5.1.4. Tier 2 SDO Technical Committee Progress Support

The Contractor shall attend meetings and monitor Technical Committee Progress for Tier 2 SDO. The Contractor shall present three (3) four (4)-month summaries of Tier 2 activity (PowerPoint format) of current and proposed activities with ANSIINCITS, ASTM, and OASIS security and privacy oriented technical committees.

DELIVERABLE 5.1.4. – Produce Tier 2 SDO Activity Summary Reports including ASTM, ANSI-INCITS, ISO, and OASIS.

5.1.5. Trip Reports

The Contractor shall prepare trip reports (format as specified by Standards Office). This is a report of any trip or meeting attended as part of this contract. Trip/meeting report formats will be provided upon contract award.

DELIVERABLE 5.1.5. – Prepare trip reports one (1) week following the trip.

5.1.6. Quality Assurance (QA) Tracking History Report Update

The Contractor shall document Quality Assurance (QA) Tracking History report and maintain review tracking history of QA activity. VA PM will provide the documents. QA functions consist of document reviews for clarity, proper technical writing, adherence to established style standards (available on contract award) and content. Reviews consist of corrections and in-line comments for areas requiring clarification. The Contractor shall track document corrections by version and final. Reviews for approximately 162 documents in twelve (12) months can be expected [average three (3) documents per weekly report].

DELIVERABLE 5.1.6. – Weekly Quality Assurance (QA) Tracking History Report Updates.

5.2 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) STANDARDS ACTIVITIES

5.2.1. ISO Standards Activities Support

In support of the US Technical Advisory Group (TAG) to ISO Technical Committee (TC) 215, the Contractor shall provide technical review of standards and standards related documents including ISO TC 215 Working Group 4 assignments for drafting ISO Standards. Reviews shall include analysis of the technical competency of the proposed document and identifying gaps and lack of completeness. Furthermore, the review shall assess the sufficiency of the proposed standard to meet its express goals, and the relevancy to VHA healthcare security and privacy.

The Contractor shall maintain the ISO standards management spreadsheet (list of standards, identifier, work item, functional area, current status, last milestone, next action regarding this item and due date, linked to location in VA standards repository, and provide comments appropriate to the current committee status and likelihood of ballot). Standards, related artifacts, and current working versions provided under this task shall be located in the Standards SharePoint Workspace (link provided upon award). Standards shall be retained unmodified in the format in which they are received.

Tasking includes submission of designated standards (from all Tier 1/Tier 2) SDO's into VA's Technical Reference Model.

DELIVERABLE 5.2.1. – Prepare Quarterly ISO Standards Management Spreadsheet.

5.3 NEW STANDARDS

5.3.1. Identify New Standards

The Contractor shall write a focused white paper on proposed new standards describing approach, priority, standards assignment, coordination, collaboration, and requirements. The white paper shall be prioritized based upon VHA's Blueprint for Excellence. The principal source of requirements shall be emerging and balloted healthcare line of business security and privacy requirements or identified gaps of the Security Requirements Steering Committee.

DELIVERABLE 5.3.1. – Prepare a white paper three (3) times a year corresponding to HL7 Working Group Meetings.

5.4 REPORTING AND ENGINNERING

5.4.1. Progress Reporting

The Contractor shall provide weekly reports of progress on all tasking in a format provided by the Government upon award. The reporting will list all tasks, due dates, and account for weekly progress as well as overall progress suitable for more senior management on an "as required" basis.

DELIVERABLE 5.4.1 – Prepare weekly progress report to PM

5.4.2. Engineering Folders Management and Maintenance

The Contractor shall manage and maintain engineering folders for all tasks. The engineering folders will include all drafts, research materials, references, and other sources critical to reconstructing and establishing the history of work accomplished. The engineering folder is continuously maintained as an artifact of each task item.

DELIVERABLE 5.4.2. – Manage and maintain engineering folders weekly.

5.5 SECURITY STANDARDS APPLICABILITY (TRACKING AND AWARENESS)

Once a new security or privacy relevant base standard, implementation guide, or interoperability specifications approved by ballot process is available within a standards setting organization (e.g. SDO/SRO), and upon notification by the PM, the Contractor shall determine the applicability of a standard to VHA near-term, long-term, or no applicability. For standards that are relevant to VHA, the subsequent analysis shall address ways the standard impacts the VHA's VE application design and development/purchase process. The Contractor shall make a presentation on selected standards (as determined by the PM) to the Standards Office summarizing the analysis and applicability of the standards. VHA expects to track approximately six (6) such standards annually. These are the new security or privacy relevant base standard, implementation guide, or interoperability specifications which will be available following approval by ballot process within a standards setting organization.

Standards include all Tier 1/Tier 2 SDO's and the National Standards Institute of Science and Technology standards and technical reports.

5.5.1. Healthcare Security and Privacy Standards Applicability Analysis

The Contractor shall provide a Healthcare Security and Privacy Standards Applicability Analysis Report. The report shall be written documents in Microsoft Word format using a style guide specified by the Government (style guides provided upon contract award). Presentation shall be in Microsoft Office PowerPoint format. The report shall cover the material specified in the Task 5.6 description.

DELIVERABLE 5.5.1. – Prepare a Healthcare Security and Privacy Standards Applicability Analysis Report every six (6) months.

5.6 STANDARDS ACTIVITIES (GENERAL)

The Contractor shall participate in VHA healthcare line of business project activities to promote and develop standards in working groups and teams supporting VHA's VE and healthcare line of business.

The Contractor shall support these activities including but not limited to: areas of security and privacy technology; healthcare application requirements-driven process; healthcare informatics; health information technology and tools; vocabulary; requirements; and terminology.

5.6.1. Healthcare Informatics Security and Privacy Engagement Summary

The Contractor shall engage in a "discovery" process for the purpose of documenting findings of a targeted analysis effort. Specific activities include:

- Participate in VA working groups and VE teams to identify issues and gaps regarding security and privacy standards.
- Review national, administration, region and project architectures, designs, requirements and other documentation for security relevance to VE.
- Participate in national level committees and working groups as well as other organizations (e.g. Kaiser Permanente, Department of Defense, Healthcare Information and Management Systems Society, American Medical Informatics Association, Health Information Standards and Policy Committees, HHS security and privacy working groups external to VA) in support of VHA healthcare line of business security and privacy standards goals.
- Coordinate with VA and VHA business stakeholders on matters relevant to security and privacy standards and processes.

DELIVERABLE 5.6.1. – Prepare Healthcare Informatics Security and Privacy Engagement Summary every four (4) months.

5.7 STANDARDS ADOPTION-SECURITY REQUIREMENTS STEERING COMMITTEE (SRSC)

The VA SRSC exercises oversight authority in regard to the development and approval of security requirements for use within the VA. The VA SRSC maintains ultimate responsibility for gathering and validation of all security requirements, submission of the security requirements for update, negotiation

of requirements through Peer Review, tracking requirements for the approval in base-lining process, ensuring requirements are allocated and traceable to the project level, and tracking the requirements through VA Office of Information and Technology specified processes.

The Contractor shall lead and coordinate security requirements activities to identify, ballot, and maintain crosscutting security and privacy requirements as part of the activities of the VA's Security Requirements Steering Committee (SRSC) as specified below:

- Review of Requirements for Consistency with Standards Development organization security requirements, the Integrating the Healthcare Enterprise (IHE) profiles, VHA, the VA and federal security policies, and VA-level security requirements
- Parse SRSC specify documents for requirements [approximately six (6) requirement documents] as directed for incorporation into SRSC ballots.
- Review requirements for security relevance and assigned the "Security Control" attribute based on the NIST SP 800-53 Security Controls standards.
- Review requirements for understanding, clarity and omissions, making additions and corrections as needed.
- Provide Requirements Traceability by Assigning Parent-Child Relationships (approximately 400 requirements with 50 to 200 added annually for which traceability may need to be determined).
- Resolve VA issues by Proposing a Solution and Incorporating SRSC Member Comments regarding Requirement Interpretation, Allocation, Service Assignment in Conflict with Operational, other security requirements, and VA policy. To meet this requirement, the Contractor may consult with other Health Data Informatics Security and Privacy personnel and members of the SRSC Technical Advisory Group.
- Support the SRSC in the coordination and managing of security requirements, their allocation to projects and in resolving issues with Office of Cyber and Information Security (OCIS) for security requirements maintained within the VA Enterprise.
- Conduct ballots and ballots reconciliation activities to achieve consensus among the members of the ballot pool per the existing SRSC ballot processes (provided upon contract award).
- Provide completed ballots to VA Office of Information and Technology (OI&T) and facilitate collection of additional requirements attributes requested.
- Maintain the SRSC Microsoft SharePoint Workspace.
- Support the SRSC in working with VA OI&T representatives to facilitate resolution of any questions, concerns, or issues regarding security specific requirements.

5.7.1. Parse Identified Standards

The Contractor shall parse identified standards, policy and guidelines for security and privacy requirements applicable to VE and VHA's healthcare line of business quarterly (approximately 8 per year).

DELIVERABLE 5.7.1. – Parse standards quarterly

5.7.2. Security Requirements Ballots

The Contractor shall prepare and announce Security Requirements Ballots (specified by SRSC Policy and Procedures – to be provided upon contractor award).

DELIVERABLE 5.7.2. – SRSC Ballots quarterly.

5.7.3. SRSC Requirements Database

The Contractor shall manage and update the SRSC Requirements Database (an existing Requisite Pro Requirements Database currently exists within VA Product Development) with SRSC proposed, approved and balloted requirements, including all working documents and ballot related materials as part of the existing Microsoft SharePoint Workspace. The SRSC SharePoint Workspace is the project repository provided by VA for maintaining all SRSC activities and artifacts and will contain all SRSC ballots and all requirements, working materials, background documents, and parse documents used to generate requirements. The SRSC ShrePoint Workspace shall serve as a single authoritative engineering folder for all SRSC actions, minutes Requirements work and administrative activities.

The Contractor shall provide individual licenses as part of the contract. VA will provide access to the SRSC SharePoint Workspace upon contract award.

DELIVERABLE 5.7.3. – Manage and update SRSC Requirements Database monthly. This is a continuous draft with monthly updates to the Configuration Managed Archive.

5.7.4. SRSC Meeting Agendas and Minutes

The Contractor shall provide SRSC Meeting Agendas and Minutes. Agendas are to be published no sooner than the day before the meeting and no later than the day before the meeting in advance of meetings, however, agendas may be modified during the meeting upon request of participants. Minutes are to be taken of the meeting proceeding and published after the meeting and not before the meeting, noting discussions, actions and assignments, due dates, and next meeting days. In order to take minutes, the Contractor shall attend the meetings. Meetings shall be conducted via teleconference.

DELIVERABLE 5.7.4. – Prepare monthly SRSC Meeting Agendas and Minutes.

5.7.5. Requirements Reviews per SRSC Procedures

The Contractor shall conduct Requirements Reviews per SRSC procedures. One-fourth of all SRSC requirements (approximately 400 total) are to be reviewed each quarter as part of the annual review. SRSC procedures are available in the SRSC Microsoft SharePoint Workspace. The Contractor shall be provided access to the space upon contract award. For estimation purposes, principal review activities involve verifying that the requirement attributes such as source document, NIST SP 800-53 allocation, guideline text/sources, and responsible stakeholder are current and correct.

DELIVERABLE 5.7.5. – Prepare quarterly Requirements Reviews per SRSC Procedures.

5.8 VA ENTERPRISE ACCESS CONTROL BOARD ACTIVITIES

The Department of Veterans Affairs (VA) Enterprise Access Control Board (EACB) acts as the authoritative A source for technical VE security and privacy terminology. The board identifies and recommends standard interoperable terminology (attributes) which provides the basis for common

access to i.e. VE associated applications. VHA participates in the EACB and will actively collaborate on defining and maintaining jointly agreed upon Information Technology (IT) vocabulary needed to support security and privacy authorizations and DoD/VA subscribing applications.

The Contractor shall perform tasks and provide deliverables related to the EACB in support to establish, manage, and profile authoritative access control attributes required to implement security and privacy within VE. In performing these duties, the overarching objectives is to define and maintain jointly agreed upon IT vocabulary needed to support security and privacy authorizations and DoD and VA VE subscribing applications. To achieve these overarching objectives, EACB activities must support a number of technical activities including:

- Support for activities of the EACB Charter.
- Maintains and publishes a catalog of standards-based interoperable user roles and associated constraints.
- Maintains and publishes a catalog of standards interoperable access attributes for use by VE subscribing applications.
- Maintains an information model mapping DoD/VA formally approved information classes to standard attributes.
- Coordinates with HHS Federal Health Information Modeling and Standards (F HIMSS) regarding alignment of VE and Federal models.
- Evaluates policies regarding the protection of electronic health information shared among Federal healthcare organizations.
- Provide a common reference for access control that can be used for governance purposes.
- Provide support for planning and interoperability testing for VE subscribing applications.
- Acts as an authority to review potentially proprietary and department unique access terminology making recommendations to the Enterprise Architecture Review Board making exceptions and waivers.
- Serve as an advisory source of expertise for development of access control use cases.
- Maintain the DoD/VA HACB charter.
- Conduct VHA security and privacy requirements and healthcare business process analysis for functional/project domains under review by the EACB.

5.8.1. Catalog of VHA User Roles/Attributes

The Contractor shall maintain a catalog of standard interoperable EACB user roles and associated constraints, access attributes for use by VE subscribing applications monthly.

DELIVERABLE 5.8.1. – Maintain catalog of VHA user roles/attributes monthly.

5.8.2. Information Model Map

The Contractor shall maintain information model mapping VE formally approved information classes to HL7 standard code/value sets.

DELIVERABLE 5.8.2. – Quarterly information model mapping

5.8.3. Semi-Annual Review of Software Test Plans

The Contractor shall provide semi-annual review of software test plans of VE Core Projects.

DELIVERABLE 5.8.3. – Semi-annual review of software test plans of VE Core Projects.

5.8.4. VE Security Functional Requirements Analysis Report

The Contractor shall provide a semi-annual VE Security Functional Requirements Analysis Report.

DELIVERABLE 5.8.4. – VE Security Functional Requirements Analysis Report semi-annually.

5.8.5. Permissions Catalog Update

The Contractor shall provide semi-annual permissions catalog updates.

DELIVERABLE 5.8.5. – Permissions Catalog Updates semi-annually.

5.8.6. RBAC Repository Report

The Contractor shall provide a monthly RBAC Repository Report.

DELIVERABLE 5.8.6. – RBAC Repository Report monthly.

5.8.7. Security and Privacy Constraints Catalog

The Contractor shall provide semi-annual Security and Privacy Constraints Catalogs.

DELIVERABLE 5.8.7. – Security and Privacy Constraints Catalog semi-annually.

5.8.8. Standards Security Wiki Content

The Contractor shall provide weekly Standards Security Wiki Content.

DELIVERABLE 5.8.8. – Standards Security Wiki Content weekly.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf)

and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 http://www-x.antd.nist.gov/usgv6/index.html), the Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Information concerning IPv6 transition in addition to OMB/VA Memoranda can be found at https://www.voa.va.gov/.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstation shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provide certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate	**Moderate Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

	Position Sensitivity and Background Investigation Requirements		
Task Number	**Low/NACI**	**Moderate/MBI**	**High/BI**
Task 5.1 – Standards Development Organization Activities	☒	☐	☐
Task 5.2 – International Organization for	☒	☐	☐

Standardization Standards Activities			
Task 5.3 – New Standards	☒	☐	☐
Task 5.4 – Progress Reporting and Engineering	☒	☐	☐
Task 5.5 – Security Standards Applicability (Tracking and Awareness)	☒	☐	☐
Task 5.6 – Standards Activities (General)	☒	☐	☐
Task 5.7 – Standards Adoption Security Requirements Steering Committee	☒	☐	☐
Task 5.8 – VA Enterprise Access Control Board Activities	☒	☐	☐

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.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).
d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations

Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).

g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Performance Levels
A. Technical Needs	1. Shows understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and	Satisfactory or higher

	mission requirements 4. Offers quality services/products	
B. Project Milestones and Schedule	1. Quick response capability 2. Products completed, reviewed, delivered in timely manner 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	1. Provided valuable service to Government 2. Services/products delivered were of desired quality	Satisfactory or higher

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion.

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service, and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of

products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

6.6 GOVERNMENT FURNISHED PROPERTY

Government Furnished Property (GFP) will not be provided.

6.7 GOVERNMENT FURNISHED MATERIALS/EQUIPMENT

The Contractor shall ensure adequate Local Area Network (LAN)/Internet data information and system security in accordance with VA standard operating procedures and standards, laws and regulations. The Contractor's firewall and web server shall meet or exceed the Government minimum requirements for security. All government data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA project manager and VA ISO as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

All Contractor employees under this contract are required to complete the VA's online Cyber Security and Privacy Awareness Training course(s) annually. Contractors must provide signed certification of completion to the CO during each year of the contract exercised options periods. This requirement is in addition to any other training that may be imposed on the Contractor, the CO, or other VA organizations.

All persons requiring access to VA information systems shall sign a System Rules of Behavior Notice for those systems before being given access, and annually thereafter. A completed VA form 9957 must be submitted for each employee requiring access to a VA system.

All computer systems residing on VA premises or under VA control will be administered by VA System Administration staff. Contractor personnel shall be granted only the least access required to accomplish activities associated with this contract.

All employees of the Contractor must sign a non-disclosure agreement regarding release of data and information pertaining to the contract and publication of data and information of material related to the project.

The Government will provide the Contractor the following:

1. Access rights to the VA Network,
2. Access to VA Email,
3. Access to SharePoint
4. VPN access to VA Network

5. Access rights to any applications and data stores requisite in performing the analyses outlined above.

In the instance that specific government required software cannot be sufficiently accessed via the VA Citrix Gateway, the government will provide GFE to ensure work can be accomplished and delivered in accordance with contractual requirements.

6.8 GOVERNMENT FURNISHED INFORMATION

VA will retain all rights and privileges, including those of patent and copy, to all Government furnished data. The Contractor shall neither retain nor reproduce for private or commercial use any data or other materials furnished under this contract. The Contractor agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such data. These rights are not exclusive and are in addition to any other rights and remedies to which the Government is otherwise entitled elsewhere in this contract.

Government Furnished Information (GFI) will be provided. This would include items such as project specific documents and other information, equipment or materials as determined necessary by the Government.

7.0 ACRONYMS/DEFINITIONS

Acronym	Definition
ABAC	Attribute Based Access Control
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
CBCC	Community Based Collaborative Care
DHHS/HHS	Department of Health and Human Services
DoD	Department of Defense
EACB	Enterprise Access Control Board
eHMP	Electronic Health Management Platform
EHR	Electronic Health Record
FHIMS	Federal Health Information Modeling and Standards
FHIR	Fast Healthcare Interoperability Resource
HCS	Healthcare Classification System
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information Standards
HL7	Health Level 7
IAM	Identity and Access Management
IETF	Internet Engineering Task Force

IHE	Integrating the Healthcare Enterprise
IHS	Indian Health Service
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standards
IT	Information Technology
JLV	Joint Legacy Viewer
NIST	National Institute for Standards and Technology
NLP	Natural Language Processing
OASIS	Organizations for the Advancement of Structured Information Standards
OCIS	Office of Cyber and Information Security
OI&T	Office of Information and Technology
OMG	Object Management Group
PM	Project Manager
QA	Quality Assurance
RBAC	Role Based Access Control
RM	Requirements Management
RM-ODP	Reference Model of Open Distributed Processing
SAIF	Service-Award Interoperability Framework
SDO	Standards Development Organizations
SOA	Service Oriented Architecture
SP	Special Publication
SRO	Standards Related Organizations
SRSC	Security Requirements Steering Committee
TAG	Technical Advisory Group
TBD	To Be Determined
TC	Technical Committee
TF	Task Force
VA	Veterans Affairs
VAP	Veteran Authorization Preferences
VE	VistA Evolution
VHA	Veterans Health Administration
WG	Work Group
W3C	World Wide Web Consortium

8.0 REPORTING REQUIREMENTS

9.0 FORMAL ACCEPTANCE OR REJECTION OF DELIVERABLES

The Government will have ten (10) business days to review each deliverable and provide feedback/comments. The contractor shall have five (5) business days to incorporate feedback/comments and make appropriate revisions. The contractor shall provide the revised version of each deliverable to the COR and VA PM. The COR will review and determine final acceptance by the Government. The COR will notify the contractor of final acceptance within five (5) business days.

The contractor shall be responsible for adhering to all pertinent VA standards including, but not limited to, ensuring that all documentation and deliverables are stored on appropriate VA servers within one (1) week of their completion. The contractor shall use the VA Nationwide Teleconferencing System (VANTS) for all pertinent conference calls and the VA Exchange server for all pertinent email. Upon assignment of VA email accounts, use of external email accounts for the purpose of VA communications and business will be prohibited. The contractor shall be responsible for adhering to all pertinent VA IT policies and procedures that will be made available at the contractor's request upon award.

10.0 KEY PERSONNEL

Certain skilled experienced professional and/or technical personnel are essential for accomplishing the work to be performed. These individuals are defined as "Key Personnel," and are those persons whose resumes are submitted and marked by the contractor as "Key Personnel." Substitutions shall only be accepted if in compliance with "Substitution of Key Personnel," provision identified below.

The CO may notify the contractor and request immediate removal of any personnel assigned to any task by the contractor that are deemed to have a conflict of interest with the Government or if the performance is deemed to be unsatisfactory. The reason for removal shall be documented and replacement personnel shall be identified within three (3) business days of the notification. Employment and staffing difficulties shall not be justification for failure to meet established schedules.

10.1 SUBSTITUTION OF KEY PERSONNEL

All contractor requests for approval of substitutions hereunder shall be submitted in writing to the COR and CO (using Personnel Change Form) at least 30 calendar days in advance of the effective date, whenever possible, and shall provide a detailed explanation of the circumstances necessitating the proposed substitution, a complete resume for the proposed substitute, and any other information requested by the CO necessary to approve or disapprove of the proposed substitution. New personnel shall not commence work until all necessary security requirements have been fulfilled and resumes provided and accepted. The COR and CO will evaluate such requests and promptly notify the contractor of approval or disapproval in writing.

11.0 ADMINISTRATIVE REQUIREMENTS

The contractor shall hold a Project Kick-Off Meeting with a project advisory group composed of key stakeholders and subject matter experts (SMEs) to be identified by the VA PM. The contractor shall schedule the Kick-Off Meeting to be held no later than (NLT) five (5) business days after contract award

or as agreed upon between the VA PM and contractor. At the Kick-Off Meeting, the contractor shall review the details of their intended approach, work plan, and project schedule.

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet

Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_x_ § 1194.25 Self contained, closed products
_x_ § 1194.26 Desktop and portable computers
_x_ § 1194.31 Functional Performance Criteria
_x_ § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the

information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.

4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor

personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

ADDENDUM B

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

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, 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 Contracting Officer 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 Contracting Officer 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 Contracting Officer 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 Handbook 1600.01, *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 contracting officer 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 contracting officer for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service 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

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the

development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

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

c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the

convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

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

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be reviewed and approved by VA prior to implementation.

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

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

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.

ATTACHMENT A – TRAVEL AUTHORIZATION REQUEST

Requestor Name:

Organization:

Position Title:

Travel Dates:

Traveling from:

Traveling to:

Purpose of trip:

Associated Task, Subtask and/or Deliverable:

Duration of Trip (excluding travel days):

Approximate Costs:

- Transportation:
- Lodging:
- Per Diem:
- Other:
- TOTAL:

Approving Official Name:

Approved: o Yes oNo

Approving Official Signature:

Comments: