



VA Center for Innovation (VACI)
Broad Agency Announcement (BAA)

VA118-17-R-2144

Posting Date: June 2, 2017

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

Table of Contents

I. INTRODUCTION	3
II. GENERAL INFORMATION	3
III. AREAS OF INTEREST	6
IV. CONCEPT PAPER AND PROPOSAL SUBMISSION INSTRUCTIONS	10
A. Submission Instructions:.....	10
i. Concept Paper Submission Instructions	10
ii. Full Proposal Preparation and Submission Instructions	11
V. CONCEPT PAPER AND PROPOSAL EVALUATION CRITERIA/BASIS FOR AWARD	16
VI. NOTIFICATION INFORMATION	17
VII. OTHER PERTINENT INFORMATION FOR FULL PROPOSAL SUBMISSION AND POTENTIAL CONTRACT AWARD	18
VIII. REFERENCES	20

I. INTRODUCTION

As an innovation engine within the Department of Veterans Affairs, the vision of the VA Center for Innovation (VACI) is a VA innovating at the forefront of science and research, service delivery, and employee empowerment. VACI leads this vision through development of organizational capability, delivery of operational breakthroughs, and by driving futures. VACI is committed to developing and employing agile mechanisms that allow VA to source incremental and transformational innovations in order to best serve Veterans and their families. This Broad Agency Announcement (BAA) opportunity seeks to source and fund early stage research, development, prototyping, and piloting with an overall goal of moving forward the state of the art.

VACI invites all potential offerors (including private sector companies, non-profits, and institutions of higher learning) to contribute ideas for innovations in Kidney Disease prevention, care coordination, and treatment that significantly increase Veteran access to services, reduce or control costs of delivering those services, enhance the performance of VA operations, and improve the quality of service that Veterans and their families receive.

NOTE: This BAA is an expression of interest only and does not commit the Government to make an award or pay concept paper or proposal preparation costs generated in response to this announcement. The cost of concept paper and proposal preparation for a response to a BAA is not considered an allowable direct charge to any resultant contract or any other contract.

All questions shall be submitted to the Contracting Officer (CO) (Carol Newcomb, 732-795-1018, Carol.Newcomb@va.gov).

II. GENERAL INFORMATION

This BAA for Kidney Disease is structured to allow for a competition cycle, which consists of submission of concept paper followed by an invitation only proposal, to select projects to be funded for an initial development phase and option period phase for subsequent field test/piloting. VA seeks solutions that can be developed, piloted, and evaluated within a 12-24 month period. This total period must include all time required for prototype testing and evaluation and for evaluation of field test results. The objectives of the Phases are as follows:

- **Development Phase (contract base period - up to 12 months):** This phase is intended to develop new and untested ideas and technologies or novel customization and application of existing technologies that have the potential to provide benefits outweighing all costs, with results that significantly exceed currently deployed solutions. Technologies, care coordination, education and treatment products submitted as Development Proposals shall achieve a working prototype or test system.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

Field Test (Piloting) Phase (contract optional period: up to 12 months): This phase is intended to field test and evaluate the solution developed in the Development Phase. Solutions shall be repeatable and ready for small-scale deployment at the VISN or facility level.

Predominantly we are seeking projects that offer a development phase plus a field testing/piloting optional phase. Offerors who do not require a development phase may choose to submit only a proposal for field test/piloting phase as the base contract period. In this case, the period of performance is limited to a 1 year base period and no option period.

A. Submission Dates:

- **Stage 1: Concept Papers**-Submissions will be accepted from **June 14, 2017- August 14, 2017**. In response to this BAA solicitation, Concept Papers must be submitted to VA's Virtual Office of Acquisition Portal at: <https://www.voa.va.gov/default.aspx?PagelD=-2> no later than 11:59 PM ET on August 14, 2017. VA will attempt to review and reply to all Concept Paper submissions as soon as is feasible with a target date of approximately sixty (60) calendar days following the Concept Paper submission close date of August 14, 2017.
- **Stage 2: Proposals** -Submission will be accepted only upon written request and notification by a VA Contracting Officer. Offerors will have 30 days to prepare a full proposal for submission.

See Section IV for concept paper and proposal submission instructions.

B. Authority: This BAA is issued under the provisions of Parts 35.016 and 6.102(d)(2) of the Federal Acquisition Regulation (FAR), which provides for the competitive selection of proposals submitted in response to this announcement. Accordingly, proposals selected for award are considered to be the result of full and open competition and fully compliant with PL 98-369, entitled "The Competition in Contracting Act of 1984."

C. Eligible Participants: All responsible sources capable of satisfying the objective of this BAA are encouraged to reply in accordance with the instructions specified herein. Private for profit and not-for-profit entities, and institutions of higher education are eligible to apply. Small businesses, small disadvantaged businesses, Veteran owned small businesses, and service-disabled Veteran owned small businesses are encouraged to submit concept papers for this solicitation. NOTE: In order to conduct business with the Government, Offerors must be registered in the System for Award Management (SAM) database.

- D. Standards of Conduct and Conflict of Interest:** Current VA employees, including staff, clinicians, and uncompensated employees, are prohibited from participating in particular matters involving conflicting financial, employment, and representational interests (see, e.g., 18 U.S.C. §§ 203, 205 & 208). Therefore, they may not legally participate in concept paper or proposal preparation. With respect to any proposals that may ultimately be submitted in response to this BAA, proposers are notified that the government will assess all submissions for the existence or appearance of any potential conflicts of interest. Notwithstanding any government assessment that shall be conducted as a result of proposal submissions, it is principally incumbent upon the party submitting any proposal to the government for funding consideration to assess all facts relevant to the existence or potential existence of a conflict of interest and disclose such information the government for appropriate consideration.
- E. Type of Contract that may be Awarded:** The Government intends to use only Firm Fixed Price (FFP) contract(s) when making awards resulting from this BAA. Multiple awards are anticipated although no commitments or promises are made in this regard.
- F. Total Funding Availability for Award(s):** Although VA plans to award multiple contracts through this BAA, no funding has been specifically reserved for this announcement at this time. The following contract funding limits have been established:
- Development Phase -maximum funding is \$250,000.00
 - Field Test/Piloting Phase-maximum funding is \$500,000.00
 - Combined Development Phase and Field Test/Piloting Phase -maximum funding is \$750,000.00
- G. Open Source Software:** For technology-based proposals, open source software solutions are encouraged and preferred. Effective deployment of Open Source Software lowers Total Cost of Ownership (TCO), produces better documented and higher quality software code, and enhances health information technology interoperability by employing open standards, open Application Programming Interfaces (APIs), and open data.
- H. Questions:** Interested parties may submit questions related to the BAA solicitation directly to **both** Carol Newcomb (Carol.Newcomb@va.gov) and Raymond Mesler (Raymond.Mesler@va.gov). Please state “BAA Question” in the subject line of the email. The deadline for submission of questions is July 31, 2017. Responses to the questions will be provided via an amendment to the BAA.

III. AREAS OF INTEREST

This section of the BAA contains statements of particular fields of interest to the subject VACI Industry Competition. All questions regarding this BAA shall be directed to the Contracting Officer.

Background: Chronic Kidney Disease (CKD) is particularly common in the Veteran population. While it impacts approximately 1 in 7 Americans, it affects 1 in 6 Veterans. In fact, CKD is the 4th most diagnosed disease within the VA. Most Veterans with CKD are cared for by a VA multidisciplinary Primary Care team, supported by nephrology specialty care consultants, aligned with the Wagner Chronic Disease Care Model.

Over 13,000 Veterans develop end stage kidney disease (ESKD) every year, disproportionately affecting non-Hispanic Whites and those of Hispanic ethnicity. Veterans may receive care for ESKD at any of 71 VA operated maintenance dialysis units, or in the community when needed. In addition, they may opt to pursue transplantation at any of 7 regional VA kidney transplant centers. The high volume of illness and the exorbitant economic and human toll that CKD exacts on the Veteran population, render CKD a healthcare crisis. Compared to cost of caring for this population (estimated at \$18 billion for VA), research is underfunded both in- and outside the VA. Due to the high volume and expenditures related to the care of Americans affected by CKD, there is a critical need for innovation to treat and prevent the disease.

The VA's four-fold mission includes delivery of excellence in health care, research, education, and support of the nation in times of crisis. The agency has a noteworthy legacy of innovation in kidney disease clinical care. The VA in fact was the first national healthcare system to adopt hemodialysis technology in the US in the early 1960's. Following the development of the arterio-venous shunt in 1960 by a VA Seattle physician (Dr Belding Scribner), and the Cimino-Brescia arteriovenous fistula (AVF) at the Bronx VA in 1966, the VA led the paradigm change in dialytic support in the US. Combining dialysis technology with durable arteriovenous access enabled the delivery of maintenance dialysis for people with end stage renal disease. The VA became the first national US health system to provide maintenance dialysis for the population it served. Since then, the VA has continued to support innovation in kidney research, contributing seminal findings related to our understanding of kidney physiology and to the optimized treatment of patients with kidney disease.

To address the need for innovation in kidney disease, VA seeks innovations across 4 primary topic areas:

- Kidney Disease Prevention and Treatment
- Data Science Advances to Improve Health Care of People with Kidney Disease
- Rehabilitation of Patients with Kidney Failure
- Education for People with or at Risk for Kidney Disease and/or their Caregivers

NOTE: When responding/inquiring on a specific area of interest, refer to the Topic Number as well as the Topic Title, as identified below.

Topic Number: 0001

Topic Title: Kidney Disease Prevention and Treatment

Topic Detail: Impaired access to care is a driver of poor health outcomes and perpetuates healthcare disparities experienced by people with kidney disease. As defined by AHRQ (<https://www.ahrq.gov/professionals/prevention-chronic-care/improve/system/index.html>) “health care/system redesign involves making systematic changes to primary care practices and health systems to improve the quality, efficiency, and effectiveness of patient care.” VA Health system redesign is needed to mitigate the system-level factors that impair Veteran access to care related to kidney disease prevention and treatment. Early detection of incipient kidney disease could potentially reduce disparities in the health of Veterans with kidney disease. In order to optimize CKD detection and prevention, there may be a need for studies of novel testing strategies for kidney injury and early dysfunction. The feasibility and validation of diagnostic efforts to identify kidney disease before CKD has become established clinically and to prevent CKD onset may have the greatest potential for reducing the overall morbidity and costs of CKD. Demonstrations of cost effective interventions that could improve the kidney health of the Veteran population are sought. VA is especially interested in innovations that target the following areas:

- a. Novel models of care, interventions, or technologies that improve nephrology and/or primary care’s ability to detect, prevent, and treat CKD and end stage kidney disease
- b. Innovations that address access issues and healthcare disparities and promote equity in healthcare
- c. Innovations in kidney disease diagnostics

References for initiatives related to VA access to kidney care initiatives:

Crowley, ST et al. “Targeting access to kidney care via telehealth: the VA experience.” *Advances in Chronic Kidney Disease* Jan 24(1):22-30, 2017.

CKD incidence among Veterans in rural areas:

http://www.ruralhealth.va.gov/docs/atlas/Chapter16_Chronic_Renal_Failure_508.pdf

Topic Number: 0002

Topic Title: Data Science Advances to Improve Health Care of People with Kidney Disease

Topic Detail: People with kidney disease typically suffer from complex comorbidity, frequent hospitalization, and experience numerous care transitions, resulting in increased opportunity for harm. The VA is unique in its national, comprehensive data sources, which if better leveraged could improve the wellbeing of Veterans with kidney disease and substantially reduce avoidable health care utilization and expenditures. In addition, with the growth of community partnerships to deliver care to Veterans with kidney disease, enhanced capture and understanding of the quality and value of non-

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

VA care is essential to VA strategic planning. The rapidly evolving field of data science offers unparalleled opportunities to enhance the wellbeing of individuals, and that of the Veteran population at risk for kidney disease. Accessible and dynamic population health surveillance tools that enable comparative analyses of Veteran care, integrated across provider settings are sought. Novel tools that facilitate data analytics and use of novel and unstructured data to improve the kidney health of individuals as well as the Veteran population in general are needed. Exploration of prognostic models that attempt to forecast outcomes of relevance (for example, hospital admissions, fistula failure, and other adverse outcomes) along with analytics to predict response to therapies and treatments are of interest to the VA. Work flow embedded tools that facilitate care coordination and communication are desired. VA is especially interested in, but not limited to, innovations that target the following areas:

- a. Big data aggregation initiatives (genomic data sets, active and passively collected health data, digitized data from wireless devices) to enable kidney population surveillance analysis and reporting
- b. Advances in analytics techniques (machine learning, artificial intelligence, natural language processing)
- c. CKD care quality/coordination/communication/ end user tool development
- d. Identification of individuals at risk for kidney disease

Topic Number: 0003

Topic Title: Rehabilitation of Patients with Kidney Failure

Topic Detail: People with kidney disease suffer impaired QOL (health related quality of life) and other poor outcomes both from the disease itself and its burdensome treatment. Transformation in the delivery of kidney replacement therapy (KRT) is required to rehabilitate Veterans with kidney failure, aligning their care with their goals and values. Emerging technologies that exploit physicochemical properties of fabricated materials and regenerative properties of progenitor kidney cells offer promise of novel bionic therapy. Health system changes that promote rehabilitation through more effective care plan development, starting with the values of the person with kidney disease, are needed. And tools and health system requirements to be able to understand the limits and opportunities for both personalized dialysis therapy and preemptive kidney transplantation to advance the rehabilitation of Veterans with kidney failure are required. VA is especially interested in innovations that target the following areas:

- a. Clinical implementation of regenerative medical technologic advances in bionics, wearables, and implantable device
- b. Innovations to understand, & advance safe deceased and living donor kidney transplantation, focusing on potentially vulnerable groups (disabled, minorities, young child bearing aged women, and others); development and testing of living donor transplantation education and outreach strategies that utilize patient advocates
- c. Development and testing of alternative paradigms of KRT such as the following examples: incremental, self-care, assisted care, home KRT, preservation of residual

kidney function, and conservative care

Topic Number: 0004

Topic Title: Education for People with or at Risk for Kidney Disease and/or their Caregivers

Topic Detail: Veterans and their caregivers experience multiple challenges that limit their awareness for the risks, behavior and the management of their kidney disease. In keeping with the VA principle of delivering patient centered care, improving Veteran health literacy that facilitates informed health decisions and developing the point of care decision aids that solicit Veteran goals and preferences would be useful. Nutrition is a key means by which kidney disease may be delayed, but there is a dearth of understandable tools that positively educate Veterans and their caregivers about medical nutrition therapy and other lifestyle interventions such as exercise, fitness, and weight control. Veterans with kidney disease often require substantial psychosocial and economic support from providers and caregivers, yet little is known about how VA can best support psychosocial health and economic support for those with kidney disease and their caregivers. Processes (e.g. system changes, implementation protocols) or tools (e.g. handouts, videos, apps, personalized decision tools, educational programs, gamification and incentive structures, and demonstrations) to improve the health literacy and autonomy of Veterans with kidney disease, and optimize caregiver support with potential to decrease long term costs to health care delivered for patients with kidney disease are sought. VA is especially interested in innovations that target the following areas:

- a. Patient awareness of kidney disease & decision aids
- b. Patient directed medical nutrition and lifestyle therapy
- c. Caregiver support and medical support communities

Examples of existing VA resources for reference include the following:

e-Kidney clinic: <https://www.va.gov/health/services/renal/>

Nutrition and Food Services: <https://www.nutrition.va.gov/Kidney.asp>

IV. CONCEPT PAPER AND PROPOSAL SUBMISSION INSTRUCTIONS

The VACI BAA will be conducted in two stages: an open concept paper stage followed by an invitation-only full proposal stage. A concept paper allows BAA respondents (hereafter referred to as Offerors) to communicate the essence of their proposals with a smaller burden of time and effort. Following a technical review of the concept papers, selected Offerors will be invited by the VA Contracting Officer to submit full proposals. Offerors will have 30 days to submit a full proposal. NOTE: Current VA employees may not be involved in the preparation of concept papers or proposals under this announcement.

A. SUBMISSION INSTRUCTIONS:

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

The Government requires electronic submittal of concept papers and proposals. All concept papers and proposals shall be submitted through VA's Virtual Office of Acquisition at <https://www.voa.va.gov/default.aspx?PagelId=-2>. The Registration link for VOA can be found in the upper left hand corner of the Home Page. From the Home Page click on the Industry VAI2 button under E-Tools to submit concept papers and proposals. The VOA Helpdesk can be reached via VA.Acquisition.Systems@va.gov

Concept papers and proposals submitted via any other mechanism will not be accepted or reviewed under this BAA. No information submitted by an interested party in response to this BAA will be returned. In addition, the cost of preparing concept papers or proposals in response to this announcement is not considered an allowable direct charge to any to any resultant contract or any other contract.

i. CONCEPT PAPER SUBMISSION INSTRUCTIONS

Offerors are required to submit a concept paper that succinctly and clearly describes the innovation. VA will evaluate the concept paper according to the evaluation criteria contained in this announcement and will determine interest in moving forward in receiving a full proposal based on this technical review. Offerors must submit a concept paper in order to be eligible to receive an invitation to submit a full proposal.

All concept paper submissions must adhere to the following general guidelines:

- Maximum of three (3) pages in length, not including the cover page
- All pages shall be printable on 8-1/2 by 11-inch paper with type not smaller than 12-point font (Arial or Times New Roman). Smaller font may be used for figures, tables and charts.
- Hyperlinks are not permitted.

The concept paper must contain the following sections:

- Part 1: Transmittal Letter (does not count against 3 page limit): Transmittal Letter (must be clearly marked "Concept Paper"): Include the Technical Point of Contact's information (name, address, phone, fax, email, lead organization and business size), the title of the proposed work, proposal type (Development, Field Test or both), the Rough Order of Magnitude (ROM) cost not to exceed stated funding limits in Section II, and the duration of the proposed work.
- Part 2: Executive Summary (White Paper): The Executive Summary should include details regarding the proposed **technical approach** (architecture, implementation, impact, benefits, and challenges of the innovation) to include **needed VA resources** (anticipated requirements for piloting in the VA – such as software hosting, access to patient data and/or VA patient), **supporting analysis** (describes how the technical approach is innovative and beyond current state of the art), and **team**

expertise (key personnel and team structure). The details needed for the Executive Summary must be framed to address the following Heilmeier questions:

- What are you trying to do?
 - How is it currently done?
 - What's new?
 - Who cares?
 - What are the risks?
 - What's your plan?
 - What's your progress?
- Part 3: BAA Topic Area Number: Clearly identify one topic area number from Section III of this BAA solicitation. Offerors ***should not*** identify more than one topic area number for the concept paper.

ii. FULL PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

Only Offerors who are invited to do so may submit full proposals. Proposals will only be accepted upon written request and notification by a VA Contracting Officer. Offerors will have 30 days from date of invitation to submit a full proposal..

NOTE: Offerors are advised that an invitation to submit a full proposal indicates interest on the part of VA in exploring the potential for contract award. However, Offerors are cautioned that an invitation to submit a full proposal does *NOT* guarantee a contract award, or otherwise commit the VA in any way.

All proposals submitted to VA for consideration must be in the format specified below. Nonconforming proposals may be rejected without further consideration or review.

All proposals shall consist of two separate volumes (Volume I and Volume II, as indicated below) and shall address the mandatory policy and other submission requirements as specified herein.

Proposals must be written in English and formatted such that, when printed, all pages will be printed on 8 ½ X 11 inch paper with 1 inch margins and font type not smaller than 12 point (Arial or Times New Roman). Charts, figures, tables, and graphs may utilize smaller font size (not smaller than 8 point). Charts, diagrams, and similar representations will count towards the page count limitations. Hyperlinks are not permitted. All pages minus the cover page must be numbered. All technical information shall be provided in Volume I, which shall not exceed 30 pages. The cover page and table of contents do not count towards the page limit.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

Price/cost shall be submitted as Volume II. There is no page limit for Volume II. Volumes I and II must be provided for the proposal to be considered for review. The information requirements for Volumes I and II are provided below:

A. Volume 1 – Technical Proposal (Not to exceed 30 pages)

1. Transmittal Letter (not included in the 30 page limit): The Transmittal Letter shall be provided on your organization's Letterhead stationary.

- Transmittal Letter to include:
 - BAA Number (BAA- VA118-17-R-2144)
 - BAA Topic Area Number
 - Technical Point of Contact, to include: Salutation, First and Last Name, Street Address, City, State, Zip Code, Telephone, Email
 - Name and title of the Principal Investigator or Project Director
 - Legal name and address of your organization, and Cage Code
 - Type of organization (large business, small business, small disadvantaged business, service disabled Veteran owned small business, Veteran owned small business, institution of higher learning, non-profit or not for profit)
 - Proposal Title
 - Project Period of Performance
 - Total proposed price, broken out by price of Development Phase (Base period) and price of Field Test/Piloting Phase (Option period), as applicable
 - Date proposal was submitted
 - Confirmation of update of Representation and Certifications in the System for Award Management (SAM)
 - Name, title and signature of an official authorized to legally bind the organization, to include: Salutation, First and Last Name, Street Address, City, State, Zip Code, Telephone, email

2. Technical Proposal: Consisting of the following sections:

- Summary of Proposal (Shall not exceed 3 pages). Including the following:
 - Description of the innovation and how it fulfills the objectives stated in the BAA
 - Description of the current state of the art and how the innovation satisfies an unmet need in kidney disease

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

- Technical rationale, technical approach, and plan for accomplishment of goals and objectives
 - Description/mapping of activities to be accomplished across the period of performance (base plus option period, if applicable) and associated deliverables
 - Innovation value statement (number of Veterans impacted, cost savings/avoidance, quality of care, and patient outcomes) and description of how value will be measured
- **Detailed Proposal Information (Shall not exceed 27 pages):** The proposal should clearly define activities, approach, feasibility, and goals for both the Development phase of the base period and the field testing/piloting phase of the option period. The Technical proposal shall include, but not be limited to:
- A detailed background, discussion and description of the proposed solution. Descriptions of the development phase shall clearly identify the new technology being developed, including a description of the current technology status and the future development to be undertaken. When describing the Field Test/piloting phase clearly indicate the current level of deployment of the solution and describe the areas where a VA deployment involves new or untested usage.
 - A clear, concise definition of the impact, benefits, and scalability of the solution to the stated area of interest.
 - Statement of Work (SOW) – In plain English, clearly define the tasks/subtasks to be performed, the duration of time associated with completion of the individual tasks/subtasks in question, and dependencies, if any, among them. The SOW should be developed so that the Development and Test/Piloting Phases are separately defined. **The SOW must not include proprietary information.** For each task/subtask, provide:
 - A general description of the objective (for each defined task/activity);
 - A detailed description of the approach to be taken to accomplish each defined task/activity;
 - Identification of the primary organization responsible for task execution (prime.sub, team member, etc.);
 - The completion criteria for each task/activity - a product, event or milestone that defines its completion; and

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

- Define all deliverables (reporting, data, reports, software, etc.) to be provided to the Government in support of the proposed tasks/activities.
- An Implementation Plan that includes the proposed schedule, milestones (Note: measurable milestones should capture key activity points and should be clearly articulated and defined in time relative to the start of the effort) and deliverables, as well as the personnel, facilities, management, and structure of the organization. The Implementation Plan shall clearly identify the major development, testing and integration activities involved in the proposed solution. The Implementation Plan shall include reporting on the program's progress.
- A discussion which details the feasibility and the methodology of the proposed approach(es) and identifies the level of effort to be employed. Risks associated with the Offerors' solutions as well as mitigation strategies shall be identified and discussed.
- A presentation of the Offeror's unique capabilities and/or specialized experience, previous accomplishments, and work in closely related areas.
- Offerors shall identify and provide brief resumes for **key personnel** (These are defined as individuals crucial to the successful performance of the orders issued and the programs being supported by those orders and are those persons identified as key personnel in accordance with solicitation requirements) and the **principal investigator** (Individual(s) designated by the Offeror to have the appropriate level of authority and responsibility to direct the project supported by the contract). Resumes will count towards Technical proposal volume page limit.

B. Volume II, Price (No page limit)

The Government intends to award only Firm Fixed Price (FFP) type contract(s) under this BAA. Additionally, funding for Phase 1 Development Proposals is limited to \$250,000 and funding for Phase 2 Field Test (Piloting) Proposals is limited to \$500,000. The total price for each phase shall be inclusive of direct and indirect costs, and profit.

The Offeror's price proposal shall be prepared in a clear and concise manner that accurately reflects the Offeror's total proposed amount for accomplishing the proposed solution. Price data shall include all costs expected during the performance of the contract. All details, broken down by cost element, shall be prepared for each major

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

task along with supporting rationale and sufficient back-up documentation to support the proposed price. All price data is subject to Government evaluation and verification. The Contracting Officer will utilize the techniques set forth at FAR 15.402 and other appropriate sections to assist in the determination of price reasonableness. The Offerors shall provide other than cost or pricing data in sufficient detail to substantiate the price proposed.

The price proposal shall include the following elements of major cost for the proposed effort:

- 1) Direct Labor: The labor category, number of hours, direct labor rate per hour for each category and totals for each category of the effort.
- 2) Materials: An itemized listing of material requirements and associated costs for the effort. Unless otherwise specified, all materials purchased for performance of the effort are to be delivered to the Government upon completion/termination of the contract. Any item that exceeds \$5,000 must be supported with back-up documentation such as a copy of catalog prices lists or quotes.
- 3) Travel: Contemplated expenditures for travel which support the effort. Provide the purpose of the trip, number of trips, number of days per trip, departure and arrival destinations, number of people, etc.
- 4) Other Direct Costs: Costs associated with laboratory usage, computer usage, reproduction, etc. with sufficient back-up documentation to support proposed costs
- 5) Costs for Consultants: The number of hours and breakdown of total costs shall be indicated as well as the nature and scope of the service furnished by any consultant. State the reason(s) why a consultant was required to complete the effort. Must provide a signed consultant agreement or other document which verified the proposed loaded daily/hourly rate, hours and any other proposed consultant costs (e.g., travel)
- 6) Cost for Subcontractors: A breakdown of the subcontract amount by cost element and profit/fee must be shown to fully evaluate the proposal. All subcontractor cost documentation must be prepared at the same level of detail as that required of the prime.
- 7) Indirect Costs: Including Fringes Benefits, Overhead and General & Administrative rates. Indirect costs shall indicate whether the rates used are fixed or provisional. Also indicate the time frames to which the rates are applicable.
- 8) Profit.

V. CONCEPT PAPER AND PROPOSAL EVALUATION CRITERIA/BASIS FOR AWARD

It is the policy of VACI to treat all concept papers and proposals as proprietary information. All concept papers and proposals will be subject to evaluation by a team of Government personnel. Should non-government evaluators be added to the evaluation team, appropriate information will be provided via an amendment to the BAA.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

Concept papers and proposals will be evaluated on their own merit, according to the criteria cited below. All evaluators will be made aware that, without written permission from the Offeror, concept papers and proposals shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate the concept paper or proposal. If a contract is awarded on the basis of a proposal submitted under this BAA, the negotiated terms of the contract control disclosure and use of the proposal.

The overall basis for selecting concept papers and then proposals for acceptance shall be technical, importance to agency programs, and fund availability. The following more specific criteria will be used :

- **Overall Innovation Merit:** The proposed innovation will be evaluated to determine if it represents a new innovative approach to the VA area of interest and advances the current state of the art. Is the innovation focused on increasing knowledge or understanding?
- **Technical Merit and Feasibility of Implementation Plan:** Is the technical approach designed to address a well-defined problem and is the project hypothesis based? The approach must be feasible to quickly demonstrate merit during both the Development and Field test/Piloting phases within the proposed timeframe. Major technical risks are clearly defined and viable mitigation efforts are presented to address any major or significant obstacles for success. For full proposals only, the SOW and implementation plan will also be included in the evaluation: Task descriptions and associated technical elements are complete, understandable, and in a logical sequence, with all proposed deliverables clearly defined such that achieving stated goals is highly likely.
- **Potential Impact/Benefit of the Innovation:** The innovation proposed must be clearly relevant to the mission of the Department of Veterans Affairs and address a demonstrated need in kidney disease – is there a current or future/emerging need for this innovation? The project description shall provide clear and convincing justification that the innovation will offer substantial benefit (in patient outcomes, cost savings, education, and others).
- **Offeror's Capabilities:** Demonstrated expertise/experience, techniques, or unique combinations of these that are integral factors for the achievement of proposal objectives. The effort must be supported by individuals with the requisite expertise and experience to meet the project objectives.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

Offerors whose concept papers lack technical merit or relevance to the areas of interest enumerated in this BAA, and/or whose content is not favorably assessed on the criteria above, and/or whose concept papers may fall in areas wherein funds are not expected to be available, will not be invited by the VA Contracting Officer to submit a full proposal. Offerors are advised that there is no guarantee that any of the concept papers submitted in response to a particular topic will result in an invitation to submit a full proposal. Further, more than one Offeror may be invited to submit a full proposal under a particular area of interest.

Concept papers and proposals will not be evaluated against other concept papers or proposals in the same area of interest, but rather on their respective merits as judged against the evaluation criteria.

VI. NOTIFICATION INFORMATION/PROJECT CO-DESIGN

Upon completion of the concept paper evaluation, the VA Contracting Officer will notify the Offeror that 1) the concept paper submission has been selected and the Offeror is invited to submit a full proposal which will be preceded by a 30-day Project Co-Design phase as described below, or 2) the concept paper submission has not been selected for submission of a full proposal. These official notifications will be sent via email to the Technical Point of Contact identified on the concept paper transmittal letter.

Project Co-Design – Offerors who receive an invitation to submit a full proposal will have approximately 30 days to communicate with the VA to gain further insight into the problem their innovation addresses, general resource requirements, the feasibility of developing the innovation, and the structure of the piloting phase of the project for the VA. If needed, VACI can help facilitate introductions. The Co-Design phase occurs after a concept paper has been peer-reviewed, scored, ranked, and selected for invitation for proposal submission. Following conclusion of the Project Co-Design period, Offerors will be allowed 30 days to prepare and submit their full technical and price proposals.

****Please note** – Following the Project Co-Design Period, VA employees will not communicate with the Offeror or their team regarding any aspect of the proposal preparation including, but not exclusive of, drafting proposal, providing advice, reviewing or editing proposal.

In all instances, the Government reserves the right to select for negotiation all, some, or none of the proposals received in response to this solicitation. The Government reserves the right to conduct discussions with an Offeror if the Government determines this to be necessary and in the Government's best interest. However, the Government need not conduct discussions with all Offerors and may hold discussions with only a few or just one Offeror. The Government may permit an Offeror to submit a proposal revision as part of discussions. This opportunity may be extended at the Government's discretion to Offeror. Additionally, the Government reserves the right to accept proposals in their entirety, or to select only portions of proposals for funding

consideration. The Government may also reshape and re-scope the proposed effort into phases or blocks, including short periods of performance with the potential for options, if appropriate, to quickly prototype or otherwise substantiate proof-of-concept, or to assess progress on a continuing or ongoing basis.

VII. OTHER PERTINENT INFORMATION FOR FULL PROPOSAL SUBMISSION AND POTENTIAL CONTRACT AWARD

- A. Responsibility Determination:** To be eligible for award of a contract, all prospective Offerors must meet certain minimum standards pertaining to financial resources, ability to comply with performance schedules, have a satisfactory performance record, integrity, organizational structure, experience, accounting and operational controls, technical skills, facilities and equipment and be otherwise qualified. For additional information concerning standards of responsibility for prospective contractors, please refer to FAR Subpart 9.1.
- B. Restrictive Marking on Proposals:** Notwithstanding VA policy, if information contained in the proposal is in the public domain or cannot be protected under law as trade secret (e.g. a patent application), VA will not accept liability for failure to safeguard it against open disclosure. If an Offeror wishes to restrict the proposal, the Offeror shall mark the title page with the following legend: "This data shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the proposal; provided that if a contract is awarded to this BAA responder as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use or disclose the data to the extent provided in the contract. This restriction does not limit the Government's right to use information contained in the proposal if it obtained from another source without restriction. The data subject to this restriction is contained on page _____."
- C. Key Personnel:** Skilled experienced professional and/or technical personnel are essential for successful contractor accomplishment of the work to be performed under this effort. These are defined as individuals crucial to the successful performance of the orders issued and the programs being supported by those orders and are those persons identified as key personnel in accordance with solicitation requirements. The Contractor agrees that the key personnel shall not be removed, diverted, or replaced from work without prior notification of the CO. Requirements that reflect the seniority and/or expertise levels of these labor categories, if any, will be specified at the order level.
- D. Substitution of Personnel:** Any personnel the contractor offers as substitutes shall have the ability and qualifications, including educations and experience, equal to or better than the key personnel whose biography was submitted with the successful proposal. Requests to substitute personnel shall be provided to the CO for review and approval. All notification of substitutions in key personnel

shall be submitted to the CO at least 15 calendar days prior to making and change in key personnel, to the maximum extent practicable. The notification shall be in writing and shall provide a detailed explanation of the circumstances necessitating the proposed substitution. The contractor shall submit a complete biography/resume for the proposed substitute, and any other information requested by the CO. The CO will evaluate such requests and promptly notify the contractor of approval or disapproval thereof in writing.

- E. System for Award Management (SAM):** Successful Offerors not already registered in the System for Award Management (SAM) will be required to register prior to award of any contract. Information on SAM registration is available at <http://www.sam.gov>.
- F. Representations and Certifications:** Each Offeror shall complete and submit Representations and Certifications via the System for Award Management at <https://www.sam.gov>. Each Offeror shall attest that, at time of the submission of its offer, its record at Representations and Certifications is current, accurate, and complete.
- G. Subcontracting Plan:** In negotiated acquisitions, each solicitation of offers to perform a contract or contract modification, that individually is expected to exceed \$700,000 and that has subcontracting possibilities, shall require the apparently successful Offeror to submit an acceptable subcontracting plan. If the apparently successful Offeror fails to negotiate a subcontracting plan acceptable to the Contracting Officer within the time limit prescribed by the contracting officer, the Offeror will be ineligible for award. However, subcontracting plans are not required from small business concerns.

VIII. REFERENCES

Note to prospective contractors: If you are proposing an IT solution all or parts of the following references, Addendum A and B may apply to the resulting contract.

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"

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

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. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <http://www.va.gov/vapubs/>
9. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs/>
10. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. 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
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
19. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
20. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” October, 28, 2015
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle,” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
25. OI&T ProPath Process Methodology (reference process maps at <http://www.va.gov/PROPATH/Maps.asp> and templates at <http://www.va.gov/PROPATH/Templates.asp>)
26. One-VA Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.asp>)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
29. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, “Transition to IPv6”, September 28, 2010
33. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

34. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
35. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
36. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
37. 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
38. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
39. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
40. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
41. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
42. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
43. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
44. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
45. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
46. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
47. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
48. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
49. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
50. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
51. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
52. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552>)
53. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
54. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
55. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
59. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
60. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
61. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
62. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
63. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
64. “Veteran Focused Integration Process (VIP) Guide 1.0”, December, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
65. “VIP Release Process Guide”, Version 1.4, May 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
“POLARIS User Guide”, Version 1.2, February 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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 PM, 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.

A3.1. 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:

<https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards> and

<http://www.section508.gov/content/learn/standards>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at <http://www.section508.va.gov/section508/Resources.asp>.

Deliverables:

- A. Final Section 508 Compliance Test Results

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 CO 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 CO 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 CO.
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:

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

- 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.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.
4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

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

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 (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.
- e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d)(1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection 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 VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). 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, *Implementation of Privacy Threshold Analysis and 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 11 configured to operate on Windows 7 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

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA 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 (c), 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.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

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, *but in no event longer than ____ days.*

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 *within ____ days.*

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 CO 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 in accordance with the TIC Reference Architecture and 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 A&A of the Contractor’s systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

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 CO 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 A&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 A&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.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

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.

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

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

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
 - a) date of occurrence;
 - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - 8) Known misuses of data containing sensitive personal information, if any;
 - 9) Assessment of the potential harm to the affected individuals;
 - 10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
 - 11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
- d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of \$37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
- 1) Notification;
 - 2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
 - 3) Data breach analysis;
 - 4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
 - 5) One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
 - 6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

- a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - 1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for

Department of Veterans Affairs Center for Innovation (VACI)
Broad Agency Announcement (BAA) for Kidney Disease 2017
VA118-17-R-2144

compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

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

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

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

(End of Broad Agency Announcement)