Business Requirements Session

Department of Veterans Affairs
Office of Information Security (OIS)

November 16 – 20, 2015

Working Draft, Pre-Decisional, Deliberative Document

U.S. Department of Veterans Affairs

What Does Our Program Do?

- Office of Information Security (OIS)
- Manages the VA-wide information security and privacy programs that protect the information security and privacy infrastructure of VA
- “Devoted to supporting all stages of Veteran care by protecting the personal information of Veterans and the employees who serve them”
- OIS protects the personally identifiable information (PII) of 23 million Veterans, 45 million beneficiaries, and over 300,000 VA employees

Working Draft, Pre-Decisional, Deliberative Document

OIS Offices

- Office of Cyber Security (OCS)
- Office of Privacy and Records Management (OPRM)
- Network Security Operations Center (VA-NSOC)

Working Draft, Pre-Decisional, Deliberative Document

Office of Cyber Security (OCS)

- Establishes policy and oversees the implementation and operation of IT security programs across the Department

- Manages and directs all activities for audit resolution and readiness, the Certification Program Service, security architecture and software assurance, the Emergency Response team, and identity access management

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-OCS

Name of Investment	Description
Big Data	Analyze VA Cyber Security data and develop an approach for establishing a VA Cyber Security big data program.
Cyber Security Transformation	Address the oversight, execution, budgeting, programming, promotion, management and monitoring cyber security activities across VA regions and facilities. VA's cyber security program is a comprehensive department-wide initiative supporting VA's multiple administrations and staff offices in cooperation with Federal Departments and Agencies, i.e., DHS, HHS, DoD.
End Point Manager (Big Fix) Maintenance	FO remediation, ISCM, EMF-FDR, etc 24x7 premium support with dedicated resources and additional product licenses are required due to increased utilization of the BigFix and Cognos platforms integrating into multiple efforts including
Policy Support	The contractor shall provide assistance to the OCS, Security Technical Management Service (STMS) in revising, reviewing, and interpreting the operational, technical, and management controls required by VA's information security program. The contractor shall provide support to translate and customize specific Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), E-government Act, Freedom of Information Act (FOIA), Privacy Act, and other requirements for the VA environment.

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-OCS

Name of Investment	Description
Cloud Security Support	The contractor to provide cloud computing security expertise to help VA plan, design, and develop security for cloud computing operations, and develop security practices for application development. The contractor will actively demonstrate, through proof-of-concept, ways the cloud can provide security by showing how to move sensitive information and systems to secure cloud-based servers.
Cognos Additional Licenses	The purpose of this acquisition is to increase the number of IBM Cognos Business Intelligence license units from the 140 units included in the VA owned IBM Tivoli Endpoint Manager (TEM a.k.a. BigFix) bundle. IBM included 140 Processor Value Units equivalent in the platform bundle (Contract GS-35F-4153D) to meet the contract requirement for the Executive Dashboard.
Cyber Security Hosted Services Platform Support (CSHS)	This investment will provide operations and infrastructure support, on a continual basis, for the IBM Endpoint Manager (IEM) (Formerly TEM), and the Risk Vision, Governance Risk and Compliance (GRC) Tool. The hosted services capability will reside in the NSOC TIC gateway cages in Chicago, IL and Sterling, VA.
Cyber Security Program Services	The contractor shall support VA's Assessment and Authorization (A&A) process by providing necessary technical services to include, the Independent Verification and Validation (IVV) of individual systems, the review of PIV Card Issuing (PCI) Stations operational compliance, and to inventory, develop and verify VA's Security Control Assessment (SCA) test cases.

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-OCS

Name of Investment	Description
Identity and Access Management Support (IAMS)	The Contractor shall provide services, analysis, and training support to the IAM BPMO. The Contractor shall perform strategic planning support to include IAM Roadmap and Two Year Plan updates, managing and tracking program risks, assessing Office of Management and Budget (OMB) and other agency mandates, and analyzing the IAM Framework, assessment of IAM policy alignment with Federal mandates, and conducting Electronic Authentication Assurance Assessments.
Accreditation Support	The purpose of this requirement is to ensure effective compliance with Assessment & Authorization (A&A) activities to support risk reviews for all Department systems and major applications, to included observations related to accreditation documentation related deficiencies and will support a rapid, intensive effort to correct SSPs, RAs, CMPs, and Network Diagrams to ensure they are up-to-date, comprehensive, integrated and provide an accurate depiction of the accredited system. In addition, this effort will support FSS perform wireless scanning at each of the OIG sites, prior to the OIG's arrival, while simultaneously assisting FSS develop an approach to wireless scanning that is consistent with policy and current resource requirements.

Working Draft, Pre-Decisional, Deliberative Document

Office Of Privacy and Records Management (OPRM)

Works across OIS to integrate privacy considerations and requests for information, manage official records, and ensure that the confidentiality, integrity, and availability of VA sensitive information and information systems are protected

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-OPRM

Name of Investment	Description
Privacy Security Events Tracking	Privacy and Security Event Tracking System (PSETS) is used to record all privacy-related complaints and privacy/security incidents across the VA. Privacy and Security event tracking is a component of the Department of Veterans Affairs (VA) Privacy Program, mandated in VA Directive 6502, VA Enterprise Privacy Program, and administered by the VA Office of Privacy and Records Management, Privacy Service.
Data Validation	This project will allow for the creation of a database from all submitted Privacy Impact Assessments (PIAs) and allow for the current manual process of compliance and review to become fully automated. The automation will include the creation, submission, review, approval, digital signature and publication of all VA PIAs.
Control Unclassified Information	Executive Order 13556 establishes a program for managing Controlled Unclassified Information that emphasizes the openness and uniformity of Government-wide practice. DVA shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination and decontrol procedures.
SSN Reduction	The Department of Veteran's Affairs (VA) Social Security Number (SSN) Reduction Initiative, which is overseen by the Office of Privacy and Records Management, Privacy Service, is an initiative that requires contractor support to assist the VA Privacy Service's efforts to track Administration and Staff Office SSN reduction plans and activities and conduct SSN Privacy Reviews.

Working Draft, Pre-Decisional, Deliberative Document

Network Security Operations Center (NSOC)

The VA Network and Security Operations Center (NSOC), defends, manages, and monitors the network operating status and cyber security posture of the Department by providing the day to day management, operation and configuration of the enterprise network infrastructure, internet gateways, the delivery of enterprise security systems and services, the monitoring and reporting of security incidents, the conduct of threat and vulnerability analysis, the validation of adequate security controls within the enterprise and the full range of functions across the spectrum of activities relating to incident management, incident response and enterprise network management.

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-NSOC

Name of Investment	Description
Software Licensing and Maintenance	The VA Network and Security Operations Center (VA-NSOC) requires support and maintenance / upgrade licenses for various solutions.
SolarWinds MDPP SW / HW	The MDPP Leadership Working Group and the Medical Device Isolation Architecture (MDIA) Working Group have chosen the SolarWinds network management solution to provide enterprise-wide MDIA Virtual Local Area Network (VLAN) visibility and data gathering capabilities for networked medical device inventory discovery. These capabilities are required to support the development and maintenance of an enterprise-wide inventory of networked medical devices while incurring the least risk to medical device operation and healthcare service delivery to Veterans. This procurement is for software to augment the NSOC instances of SolarWinds to provide this functionality.
Tenable Security Center	Supports The Enterprise scanning solution and Visibility to the Desktop, identifies all vulnerabilities and reports the findings to the appropriate system administrators for corrective action and up to management.
TIC Gateway Refresh	Perform a technical refresh of hardware / software solution s that make up the VA TIC Gateway.
Gateway Hosted Services Hardware Maintenance	This is a Networx contract requirement. The implementation of this project ensures that the Department of Veterans Affairs maintains full compliance with the mandatory requirements of the Trusted Internet Connections initiative and ensures that the Department's Information Technology Infrastructure and Information Systems resources and information are protected by maintaining separation of hosted and non-hosted environments and ensures unimpeded access to non-hosted equipment by those responsible for maintaining the equipment whereas access to the hosted areas requires a member of the Network Security Operations Center at all times.

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-NSOC

Name of Investment	Description
Network Engineering, Design, Implementation and Infrastructure Support (NEDIIS)	The NEDIIS service contract will include the operations, maintenance, management, and engineering support of the VA Wide Area Network (WAN), Trusted Internet Connection (TIC) Gateway services, and other support services for the Department of Veterans Affairs (VA).
Technology Refresh of TIC Global Support Infrastructure (TIC-GSI)	**Compute/Network Refresh:** refresh would be upgrading existing infrastructure to faster newer 14 core processors, and a minimum of 768G of memory per blade. While maintaining the current footprint. **Storage Refresh:** Increasing our performance and scales with our current in place storage disk shelves and augmenting it with additional storage and solid state drives.. **Software:** Upgrading the Virtual Suite as well as adding in security software for the audit logging and compliance part of the infrastructure.

Working Draft, Pre-Decisional, Deliberative Document

Upcoming FY16 Contract Opportunities-NSOC

Name of Investment	Description
NexGen App Firewall procurement	**Chassis based solution:** a chassis-based architecture where the chassis backplane capacity exceeds the throughput of the current chassis modules – avoiding the limitations encountered by a standalone single appliance solution. The vendor must have formalized committed plans to produce upgraded modules that will be backwards compatible with the chassis and with current modules. The upgraded modules are to provide enhanced capabilities and greater throughput as compared to an existing, standalone appliance based solution. **Interface flexibility:** Refresh would be upgrading the existing infrastructure to hardware that supports 1Gbps, 10Gbps, and 40Gbps interface modules, with formalized committed plans to support 100Gbps modules in the future on future line cards in order to stay well ahead of the ever increasing throughput requirements at each TIC Gateway. **SSL decryption:** The new hardware / solution will support forward SSL decryption based on URL category, whereby an administrator can determine which URL categories are subject to decryption and which are not. URL category determination must require no third-party integration or licensing, and must utilize the same categorization engine as the URL filtering feature. Hardware will support the current VA traffic load through the TIC Gateways as well as allow room for future growth. This will allow for the application of thread prevention features and capabilities to decrypted SSL traffic.

Working Draft, Pre-Decisional, Deliberative Document

Additional Information

- For more information about the Office of Information Security, contact: OISBusinessOffice@va.gov

- For information on doing business with VA, visit: http://www.va.gov/oal.business/dbwva.asp

Questions?

Working Draft, Pre-Decisional, Deliberative Document