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

1. REQUISITION NUMBER	PAGE OF
	1 2

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
70RTAC19A00000009	09/01/2019		70RTAC18Q00000022	09/06/2018

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	(b)(6)	(b)(6)	ES

9. ISSUED BY CODE DHS/OPO/ITAC

U.S. Dept. of Homeland Security
Office of Procurement Operations
Information Tech. Acquisition Ctr.
245 Murray Lane, SW, #0115
Washington DC 20528-0115

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS: 541511
SIZE STANDARD: $27.5

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE	12. DISCOUNT TERMS	☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
	As Indicated On Each Call		☒ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE

As Indicated On Each Call

16. ADMINISTERED BY CODE DHS/OPO/ITAC

U.S. Dept. of Homeland Security
Office of Procurement Operations
Information Tech. Acquisition Ctr.
245 Murray Lane, SW, #0115
Washington DC 20528-0115

17a. CONTRACTOR/ OFFEROR CODE 1120747570000 FACILITY CODE

BLACKSTONE TECHNOLOGY GROUP
150 CALIFORNIA ST FL 9
SAN FRANCISCO CA 941114560

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE

As Indicated On Each Call

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

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	GSA Contract #: 47QTCA18D00EP DUNS Number: 112074757+0000 The Department of Homeland Security (DHS) awards this Blanket Purchase Agreement (BPA) with Firm-Fixed-Price, Time-and-Materials or Labor Hour Contract Line Item Numbers (CLINs) to Blackstone Technology Group. The purpose of this BPA is to procure Architecture, Development, and Platform Technical Support Services (ADaPTS) for the Office of the Chief Information Officer (OCIO) to assist in executing and accomplishing *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
As Indicated On Each Call

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$0.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

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

30a. SIGNATURE OF OFFEROR/CONTRACTOR
(b)(6)

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
(b)(6)

(b)(6)

30c. DATE SIGNED 8/15/19

31b. NAME OF CONTRACTING OFFICER *(Type or print)*
(b)(6)

31c. DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	the OCIO mission objectives. The period of performance of this BPA is as follows: (b)(4) ATTACHMENTS: (b)(4)				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY		

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

U.S. Department of Homeland Security

Office of the Chief Information Officer

Blanket Purchase Agreement (BPA)
for
Architecture, Development, and Platform Technical Services (ADaPTS)

(September 1, 2019)

DEPARTMENT OF HOMELAND SECURITY
BLANKET PURCHASE AGREEMENT
TERMS AND CONDITIONS

Pursuant to GSA Schedule Contract Number 47QTCA18D00EP and Federal Acquisition Regulation (FAR) 8.405-3, Blanket Purchase Agreement (BPA), the Contractor agrees to the following terms and conditions of a BPA EXCLUSIVELY WITH the Department of Homeland Security (DHS).

(1) All services/labor categories currently listed on your GSA Schedule, to include new services/labor categories added during the performance of this BPA can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the GSA Schedule contract, except as noted below:

ITEM (Model/Part Number or Type of Service) BPA Labor Categories	SPECIAL BPA DISCOUNT/PRICE BPA Discounted Labor Rates
Delivery: DESTINATION Per Each BPA Order	DELIVERY SCHEDULE/DATES Each BPA Order

(2) The Government estimates, but does not guarantee, that the volume of purchases utilizing this BPA will be (b)(4) for the BPA orders placed under this BPA. The BPA holder(s) will be notified when the BPA's estimated total value is reached. .

(3) This BPA does not obligate any funds. The Government is obligated only to the extent of authorized orders actually made against this BPA.

(4) The period of performance for this BPA will have a five (5) year ordering period from the date of award. This BPA expires at the end of the current Contractors' GSA Schedule or each subsequent contract period for which GSA extends the GSA Schedule contract by modification.

(5) The warranted Contracting Officers within the following office is hereby authorized to place orders under this BPA.

OFFICE	POINT OF CONTACT
(b)(6)	(b)(6)

(6) Only written orders will be placed against this BPA.

(7) Unless otherwise agreed to, all BPA orders shall reference the relevant sections of the BPA Statement of Work (SOW). The following ordering procedures apply to all BPA orders:

- Services/Supplies will be ordered by issuance of written BPA orders in accordance with FAR 8.405-3(c) (2).
- BPA Orders are subject to the terms and conditions of this BPA and the Contractor's GSA FSS contract number, as may be amended.
- No work will be performed and no payment will be made except as authorized by a written BPA order.
- A BPA order will be considered issued when the Government transmits the order to the Contractor.
- Individual BPA orders must include the following information at a minimum:
    - Name of Contractor
    - GSA Contract, BPA and order numbers
    - Date of BPA order
    - Description of the services to be performed and/or SOW
    - Schedule B – CLIN number, labor category, quantity, unit price and extended total amount
    - Delivery schedule or period of performance
    - Place of delivery or performance
    - Contract type
    - Accounting and Appropriation Data
    - Deliverables and reporting requirements
    - Applicable clauses
    - Invoicing and payment instructions when a progress payment is allowed.

(8) If the Contractor's current GSA Schedule is replaced with a subsequent schedule, the applicable terms and conditions of the subsequent schedule shall be incorporated into this agreement upon bilateral modification of the contract and the terms of such subsequent schedule shall apply. However, a follow-on GSA Schedule will not affect the maximum term of the BPA and its BPA orders. Furthermore, the BPA's pricing will only be changed as a result of a bilateral modification to the BPA.

It is the responsibility of the Contractor to notify the BPA Contracting Officer of GSA Schedule contract and/or price changes affecting services under this BPA. The discount rate applied this BPA shall remain the same throughout the term of the BPA.

1.0 Introduction

This is a multiple-award Blanket Purchase Agreement (BPA) under the GSA Schedule 70 contract, SIN 132-51 *Information Technology Professional Services* to perform the Office of the Chief Information Officer (OCIO) requirements of Architecture, Development, and Platform Technical Support services as specified in the Statement of Work (SOW). The Contractor shall provide all management, supervision, labor, facilities, and materials necessary to perform on a BPA order basis.

1.1 Competition

BPA Establishment: The OCIO Architecture, Development, and Platform Technical Services (ADaPTS) BPA Request for Quote (RFQ) is issued and competed under the GSA Federal Supply Schedule 70. Multiple BPAs will be awarded as a result of the solicitation.

BPA Order Level: For new requirements, each multiple-award BPA holder will be provided a fair opportunity to be considered for each BPA Order exceeding the micro-purchase threshold, unless an exception at FAR 8.405-6(a)(1)(i) applies. (See FAR 8.405-3(c)(2) and 8.405-6(a))

2.0 Order Type

Orders placed against this BPA may use one or a combination of the following contract types:

- Firm-Fixed-Price (FFP)
- Time-and-Materials (T&M)
- Labor-Hour (LH)

FFP is the preferred pricing structure. T&M or LH contracts will be used only if the Contracting Officer (CO) executes a Determination and Findings (D&F) at the BPA order level that no other contract type is suitable to acquire the service in accordance with FAR 8.404(h) and FAR 12.207(b)(1)(ii).

3.0 BPA Pricing - Labor Hourly Rate and Discount Terms

BPA Labor Categories/Price List provides this BPA's negotiated and fixed hourly labor rates (on-site and off-site) and negotiated discount rate which will remain in effect until the BPA's expiration. The BPA hourly labor rates are fully burdened to include wage, overhead, general and administrative expenses, profit, and the GSA Industrial Funding Fee (IFF). These fixed hourly labor rates are ceiling rates, the Contractor may elect to propose lower hourly rates on a BPA order basis.

3.1 Incremental Funding

The BPA orders will be fully funded at the time of award. HSAM 3032.702(e) restricts the use of incremental funding for fixed-price, labor hour or time and materials orders; however, when the Government is operating under a Continuing Resolution (CR) DHS is authorized to use incremental funding; therefore, some orders may be incrementally funded under this BPA.

4.0 Statement of Work

4.1 Background

The Department of Homeland Security (DHS), Office of the Chief Information Officer (OCIO) is responsible for leading the engineering of DHS' Digital Transformation by providing knowledgeable and innovative insights into technology products or services across all Information Technology (IT) portfolios, strengthening cybersecurity, IT acquisition, IT security, executive oversight, and promoting the use and deployment of best of breed technologies using a unified framework for collectively managing IT investments.

The OCIO provides enterprise technical architectural planning and delivery of enterprise IT services. In addition, OCIO is the DHS lead for Cloud based computing, in the private, hybrid and public Clouds. OCIO manages multiple, unrelated IT projects in the design, development, testing and staging phases. OCIO seeks to provide innovative business solutions, lower costs through shared services, and reduce the time spent marketing for new capabilities. As the foundation for customer-centric service delivery, OCIO establishes a secure utility computing environment where innovation, re-use, and quality are core principles. OCIO promotes the adoption of standardized solutions and services across the department.

DHS has identified several requirements for new business applications that will support improved integration and overall efficiency of headquarters business units.

Additionally, DHS needs to modernize several of its existing business applications to migrate off unsupported platforms and improve the efficiency of OCIO's application delivery functions. OCIO's intent is to build these applications based on a suite of reusable services.

4.2 Objective

The objective of this procurement is to obtain highly specialized technical contractor support services to assist the OCIO in executing and accomplishing its mission objectives. The key mission objectives are listed below:

- Implement and manage Cloud based commodity computing services
- Perform end-to-end technical requirements management for enterprise IT services
- Maintain and track application service level agreements and performance measurements
- Support Government-Off-The-Shelf (GOTS) / Commercial-Off-The-Shelf (COTS) application integration and interoperability for customer developed components
- Perform application and service compliance and performance monitoring (e.g. FedRAMP, DHS Directive 4300A, NIST Guidance, Federal Information Security Management Act of 2002 (FISMA), Privacy, Rehabilitation Act of 1973 (a.k.a. Section 508)).
- Plan, develop and manage enterprise application development and delivery

- Provide an integrated approach to enterprise application capabilities (e.g. user interface, application logic, access to data and security, etc.)
- Perform application delivery and quality assurance including configuration management
- Provide Strategy, Policy and Governance Support
- Provide Architecture and Planning Support
- Provide Development and Implementation Support
- Provide Strategic Communications Support
- Provide Operations and Maintenance Support
- Provide Operations/Database Support
- Identify and recommend products (preferably open source) to streamline processes and add efficiencies

4.3 Scope

The scope of this effort includes the contractor support services necessary to provide a full range of IT and program support services. All services and products that will be provided under this BPA must comply with Government security, Section 508, and architecture requirements. The scope of the services and products to support these services required includes, but is not limited to:

- Program and project management
- Agile Software Development Processes
- Engagement and facilitation of key stakeholders
- Business Analysis and Requirement management
- Application, service and cloud architecture support
- Application and Service Design, Development, Implementation and Migration
- Unit, System, User Acceptance and Automated Testing
- User Interface / User Experience Design
- Business Intelligence, dashboard and analytics support
- Business process re-engineering and change management
- Integration with databases and applications
- Analytics and reporting
- Release management
- Training support
- Data Standardization, Quality, and Analytic Support Services
- Platform Support and Disaster Recovery (DR)
- User guides and system documentation
- Systems Engineering Lifecycle (SELC) Support
- Manage Cloud based commodity computing services and Shared Services
- Knowledge management, communications, and graphics support
- Security Support Services
- Security Engineering Services
- Configuration Management Support
- Support for new and evolving technologies

4.4 Specific Task Requirements

In order to support the agency mission, projects and system requirements, the Government requires highly specialized information technology systems support services in the following task areas. Specific task requirements will be specified in each individual BPA order.

4.4.1 TASK ONE. Program and Project Management

Effective program and project management are essential components of OCIO's mission. OCIO has the responsibility of developing and implementing a comprehensive program and project management capability for overseeing and controlling program and project activities.

The Contractor shall employ a comprehensive project management approach following the Project Management Body of Knowledge (PMBOK), which will include development and oversight of project schedules and key management plans for Government review and approval. The Contractor shall facilitate Government project teams and key stakeholders to gain consensus on key project parameters, including scope, resource requirements, project plans, and schedule dependencies. The Contractor shall ensure that scope, performance expectations, and resource requirements are clear, well-defined and thoroughly documented.

The Contractor shall employ Agile project management methodology to enrich traditional project management methodologies. Agile uses iterative, incremental development, which allows requirements and solutions to evolve through collaboration in an integrated project team environment. The Contractor shall promote adaptive planning, evolutionary development and delivery, in a time-boxed iterative approach, and encourage rapid and flexible response to change using the Agile methodology.

4.4.2 TASK TWO. Business Analysis and Requirements Management

The Contractor shall develop for Government review, a standard requirements management process for implementation that provides traceability across the full lifecycle of service and application development. This process shall provide and align with DHS Enterprise Architecture (EA) processes to ensure potential services are appropriately vetted prior to committing resources for implementation.

The Contractor shall support a fully automated suite of software (currently Atlassian) with the following capabilities:

Figure 1 - Requirements Software Capabilities

Software Capabilities	Key Characteristics	Phase of System Lifecycle

Requirements Management	• Automated Bi-directional Traceability across tiers of requirements (Higher level business requirements down through to detailed technical requirements). • Automated Bi-directional Traceability across life cycle elements (Requirements to design elements to code/module to test script). • Tracking of requirements by attributes (i.e., functional area, source, date, iteration). • Easy reporting and measurement tracking.	Requirements/ Design/ Development/ Testing

The Contractor shall use the aforementioned capabilities and processes to manage requirements through their lifecycle.

4.4.3 TASK THREE. Application, Service, and Cloud Architecture Support

The Contractor shall provide support for the definition of application and service architectures, as well as the evaluation and definition of standards. Specifically, the Contractor shall assess leading edge and emerging technologies, and conduct analyses of their applicability and viability for DHS applications and services. In addition, the Contractor shall assist the Government with leadership and management of service planning, enablement, directory services and services analyses.

The Contractor shall support the OCIO in the on-going development of the Cloud Architecture to include:

- Provide an integrated approach to enterprise application capabilities (e.g. user interface, application logic, access to data and security, etc.)
- Establish target/reference architectures for implementing hybrid cloud based applications and services, while ensuring that the following critical functions are incorporated: Log Management, Artifact Repository, Vulnerability Scanning, Secrets Management, Discovery, Intrusion Detection, Source Code Management, Identity and Access Management, Lightweight Directory Access Protocol, Domain Name System, Forward Proxy, Reverse Proxy, Automation Orchestration, Configuration Management, Container Orchestration, Cloud Security, Data Protection, Data Segregation, Mobility and Data Tracking.
- Assist OCIO in driving reusable services and capabilities to reduce the number of interfaces, services, and service buses.

The Contractor shall interface with and support the Office of the Chief Information Officer (OCIO). In this role, the Contractor shall propose application development standards for Government review, and foster the use of Agile development to ensure enterprise services provide scalable, reusable components to meet future customer requirements.

In addition, the Contractor shall work across OCIO to assist with the design, development,

testing, staging, and production environments for HQ and enterprise applications and services. The Contractor shall develop a proposed to-be infrastructure for Government approval to leverage virtualization and cloud computing.

4.4.4 TASK FOUR. Application and Service Design, Implementation and Migration

The Contractor shall support the OCIO by providing database and development services on multiple, simultaneous projects and services. In addition, the Contractor shall support the migration of applications, data, and services to newly developed platforms and services.

The Contractor shall provide the following:

- The Contractor shall design and develop applications and platform services for use by DHS. The design and development activities shall leverage prior efforts where directed by Federal program manager and/or the COR. All efforts shall use the Agile methodology unless approved by the functional federal lead to do otherwise. The design and development shall include the creation of frameworks and tools for deployment and support of the application and service.
- The Contractor shall perform trade off analyses to include analysis of alternatives, cost benefit analysis, total cost of ownership and usage, and technical tradeoffs.
- The Contractor shall plan and support capacity and performance management of the Cloud or Virtual Service environments.
- The Contractor shall create and refine prototypes for Government approval in a rapid development environment.
- The Contractor shall implement applications and services to include, but not limited to, obtaining approvals; setting up and configuring infrastructure; integrating to other applications, services and data stores; migrating code, frameworks and data; supporting reviews and testing; and creating documentation.
- The Contractor shall update and maintain applications and services whether in the DHS Enterprise Data Centers, the DHS Private or Public Clouds, or through a third party provider.
- The Contractor shall support Digital Identity Management and Digital Rights Management, information management and e-discovery capabilities.
- The Contractor shall support Digital Asset Management capabilities to organize, store and disseminate digital imagery to include photos, videos, audios, and documents.
- The Contractor shall support direct mail capability for the DHS enterprise.
- The Contractor shall design, develop, test and deploy applications and services in a highly virtualized environment using select applications and Integrated Development environments. Technologies that will be supported include, but are not limited to:

Microsoft technologies: The Contractor shall provide support to, and proven expertise in, developing, maintaining and administrating Microsoft applications to include, but not limited to, troubleshooting issues, on-boarding and off-boarding new customers, and implementing product enhancements. The Contractor shall also tune and manage the health of the databases. The Contractor shall provide development and platform support using the following technologies:

- Microsoft Azure Infrastructure as a Service and Platform as a Service Products
- Office 365 Services
- SharePoint
- Forefront Identity Manager (FIM)
- Active Directory (AD)
- SQL Server Database Services
- SQL Server Analysis Services (SSAS)
- SQL Server Integration Services (SSIS)
- SQL Server Reporting Services (SSRS)
- Microsoft .NET Framework & C#
- Dynamics Customer Relationship Management (CRM)

VMware: VMware is the basis for the DHS private development, test pre-production and production Cloud servers. There are hundreds of these servers in use by OCIO today. The contractor shall create, manage, support and troubleshoot these servers using the following technologies (at a minimum):

- vCloud Director
- vCenter
- ESXi
- View

Oracle: The Contractor shall provide support to, and expertise in, developing, maintaining and administrating the Oracle Platform and applications using the Oracle Platform to include, but not limited to, troubleshooting issues, on-boarding and off-boarding new customers, and implementing Oracle product enhancements. The Contractor shall also tune and manage the health of the databases. The Contractor shall provide development and platform support using the following Oracle technologies.

- Oracle Business Intelligence Enterprise Edition (OBIEE)
- Oracle Visual Analyzer
- Oracle Database
- Management Pack
- Oracle Enterprise Manager
- Hyperion
- Master Data Management

Tableau: The Contractor shall provide support to, and expertise in, developing, maintaining and administrating the Tableau Server Platform and applications using the Platform to include, but not limited to, troubleshooting issues, on-boarding and off-boarding new customers and implementing product enhancements.

Applications, Open Source Tools, and Languages: Where possible, the OCIO is using Applications, Open Source Tools, and Languages in developing, maintaining and supporting applications and services. The Contractor shall provide support and be capable of creating, managing, supporting and troubleshooting using the following applications, tools and technologies:

- Apache
- Atlassian JIRA
- DROOLS
- Drupal
- Eclipse
- Fisheye
- GRADLE
- Grails
- HADOOP
- JAVA
- MOODLE
- MySQL
- PHP
- Red Hat Linux
- Red Hat Ansible
- Spring
- Tungsten
- Zenoss
- AngularJS
- Bootstrap
- JQuery
- Terraforms

Direct Mail Solution: The Contractor shall provide support to use this solution to help headquarters and components deliver email and newsletters to the public. Currently the solution in use is GovDelivery.

JAZZ: The Contractor shall provide support to use this solution in managing the application lifecycle, especially while using Agile methodologies.

MQ Series: Used as a message oriented middleware and is part of many mainframe applications. The Contractor shall provide support to understand how to input data to and obtain data from MQ Series ques.

Web Sphere: This suite of products will be a major part of the support that is provided to some enterprise services. The Contractor shall create JAVA based applications using these technologies, as well as the Web Sphere bus.

BMC Software Applications

- Blade Logic: The Contractor shall be able to provide support and configure this solution.
- Remedy: The Contractor shall provide support by resolving tickets input into the system.

Cloud Computing: OCIO is the DHS lead for Cloud computing and currently has ten (10) Cloud services. The Contractor shall support OCIO Cloud Services that are provided to the Department to include:

- Application Lifecycle Management as a Service
- Authentication as a Service
- Business Intelligence as a Service
- Customer Relationship Management as a Service
- Email as a Service
- Enterprise Content Delivery as a Service
- Identity Proofing as a Service
- Platform as a Service (PaaS includes Infrastructure as a Service and Dev/Test as a Service)
- SharePoint as a Service
- Workplace as a Service
- Web Content Management as a Service

The Contractor shall comply with FISMA and Section 508 guidance.

4.4.5 TASK FIVE. Unit, System, User Acceptance and Automated Testing

The Contractor shall provide a full range of application and service testing. Specifically, the Contractor shall support the development and implementation of repeatable testing frameworks that encompass functional, unit, system, integration, stress, and load testing procedures.

The Contractor shall support the Agile process by providing continuous integration and builds (i.e. Ansible, Bamboo, and Bitbucket), as well as unit, functional and integration test execution, with incremental automated deployment of an application or service.

The Contractor shall provide services and software that support the following capabilities:

Figure 2 – Testing Capability Requirements

Software Capabilities	Key Characteristics	Phase of System Lifecycle
Automated/ Manual Function Testing	• Allows automated traceability of test scripts to requirements. • Automates testing using stored inputs and outputs. • Provides scripting engine/harnesses to automate tests. • Provides reporting and measurement tracking on the failure rate of test scripts against approved requirements.	Testing
Automated Load Testing / Performance Modeling	• Provides load testing tools that may increase and decrease the performance load on various parts of the infrastructure, application, services, and data stores. • Enables the software team to find out exactly how much stress (i.e. maximum number of users) each infrastructure, application, service, and data store can handle to validate that it performs at specified or higher than expected production values	Testing

4.4.6 TASK SIX. Business Process Reengineering and Change Management

The Contractor shall provide business analysis support to document key business processes, analyze them for service-enablement, identify and describe candidate services for implementation, develop recommendations for process improvement, and create service orchestration specifications for use in application development efforts. The Contractor shall provide recommendations to help DHS optimize the flexibility and impact of its service offerings.

The Contractor shall support the OCIO Change Management processes by:

- Developing and executing communication plans for stakeholders (serving as the formal method to communicate and advise stakeholders of the changes being made, timeframes, responsibilities, resulting impacts, and expectations).
- Providing organizational change management (OCM) support which includes training to institutionalize the recommended changes and educate the business users and staff about the communication plans.

4.4.7 TASK SEVEN. Release Management

The Contractor shall define, for Government review and implementation, standard

mechanisms for building and releasing software across development, testing, staging, and production environments. Release management shall be organized by platform, system, service or environment, depending on the specific objectives of the release cycle.

The Contractor shall support the Agile process by providing continuous integration and builds, as well as unit, functional and integration test execution, with incremental automated deployment of an application or service.

The Contractor shall provide services and software that support the following capabilities:

Figure 3 – Release Management Capabilities

Software Capabilities	Key Characteristics	Phase of System Lifecycle
Deployment/ Migration Tool	• Provides processes, procedures and automation for consistent, reliable builds and migrations. • Allows rapid deployment of software environments based on definable policies and controls. • Creates "snapshots" of systems manually and in an automated process. • Provides for Continuous Data Protection (CDP) when used to replicate a system. • Uses various techniques, such as ghosting/imaging and virtualization to allow a development team to rapidly create virtualized servers with the exact same image as their production boxes for development purposes. • Provides processes, procedures and tools to "sanitize" data. • Helps automate and manage a solution over its lifecycle. • Manages patch deployment. • Facilitates capacity planning and efficient resource use.	Development/ Testing / Operations & Management (O&M)
Configuration Management	• Provides continuous configuration management of the environment or service. • Provides continuous monitoring and reporting of the environment or service.	Throughout the SELC

4.4.8 TASK EIGHT. Training Support

The Contractor shall provide training on all applications developed under each individual task

order. The training will be conducted for three (3) separate target audiences:

- Business users of the application or service
- Staff that will support the application or service
- Staff that will continue working on the application or service

The business users training shall result in business users understanding and correctly using the application or service.

The support staff training shall include the content from the business users' training in addition to a walkthrough of the application's functionality and documentation. It shall prepare support staff to address questions on the application or service and determine the point at which the support efforts should be rolled over to the next level of support.

The developer training shall include the content from the business user and support staff training, as well as a walkthrough of each functional module of code. The developer walkthrough and training shall be structured so that the developer is able to understand the manner in which the application or service was developed and leave with a complete knowledge of all aspects of the application or service's functionality and support requirements.

4.4.9 TASK NINE. Data Standardization, Quality, and Analytic Support

The Contractor shall assess the type, quantity, and quality of data in order to verify that the data is suitable for its intended purpose. The Contractor shall assess the source of data and its refresh rates in order to determine where the source systems are for the data and how frequently the data is updated.

The Contractor shall provide the ability to perform Extract Load and Transformation that includes the ability to output data in the format that is required for the system, data store, service or application.

4.4.10 TASK TEN. Platform Support and Disaster Recovery (DR)

For each application or service supported, the contractor shall provide support for advanced application or service issues that the customers cannot address (as defined in their Operations & Maintenance Handbooks and their Memorandum of Agreements), both during the daily work hours and after hours, via an on-call service. The Contractor shall provide this service using staff that participates in the application or service development where possible.

The Contractor shall provide services and software that support the following capabilities:

Figure 4 – Support Capabilities

Software Capabilities	Key Characteristics	Phase of System Lifecycle

Help Desk (Level 1-3 support of deployed applications)	• Provides ability for development staff to enter, obtain, update and close tickets. • Provides ability to define issues seen. • Provides ability to enter actions taken on issues.	O&M
Level 2-3 platform support	• Production Deployments • Monthly Patching	O&M
Backup / Restore / Disaster Recovery	• Allows an organization to make backups of code bases and application configurations and then restore them quickly should any fault happen to the system. • Creates "snapshots" of systems manually and in an automated process. • Provides for Continuous Data Protection (CDP) when used to replicate a system. • Provides geographic site failover for production.	O&M

4.4.11 TASK ELEVEN. Manage Cloud Based Commodity Computing Services, Shared Services and "X" as a Service (XaaS)

The Contractor shall support the OCIO in the implementation and management of Cloud based commodity computing services and Shared Services. This includes:

- Obtaining and documenting business, functional and technical requirements
- Evaluating and making recommendations on technology and design trade offs
- Providing processes, procedures and documentation to support on-boarding and off-boarding customers
- Integrating applications and services (Infrastructure as a Service, Platform as a Service & Software as a Service) into current architecture, including all back-office systems
- Migrating applications and data from the current DHS datacenters to approved cloud solution offerings
- Providing technical assistance in maintaining and tracking application service level agreements and performance measurements to include:
    - Resource and workload utilization rates
    - Measurements of usage
    - Availability
    - Serviceability
    - Creating and evaluating root cause analyses for incidents
- Recommending enhancements to the services
- Providing Operations and Maintenance Support for the service

The Contractor shall support the OCIO application and service compliance activities, as well as provide performance monitoring in support of FedRAMP, DHS Directive 4300A, NIST Guidance, Federal Information Technology Reform Act (FITARA), Federal Information Security Modernization Act of 2014 (FISMA), Privacy, Rehabilitation Act of 1973 (a.k.a. Section 508) and other applicable legislation. The Contractor shall manage and track the system and service security posture.

4.4.12 TASK TWELVE. User Guides and System Documentation

The Contractor shall develop all documentation and deliverables required using industry best practices such as PMI Project Management Body of Knowledge (PMBOK), Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMI), and Institute of Electrical and Electronics Engineers (IEEE).

The Contractor shall develop all documentation and deliverables in accordance with Acquisition Directive 102-01, Acquisition Management Instruction/Guidebook 102-01, Appendix B: Software Engineering Life Cycle (SELC).

4.4.13 TASK THIRTEEN. Security Support Services

The Contractor shall develop system security plans and support security related activities consistent with the Information Systems Security Officer (ISSO) functions for the certification, accreditation, and continuous monitoring and compliance of the DHS enterprise.

The Contractor shall provide Information Security support to the OCIO with sufficient Application & Engineering Security expertise to maintain the security baselines of all IT systems in accordance with the DHS 4300A Sensitive Systems Policy. This includes but is not limited to the following:

- The Contractor shall comply with the ISSO Roles and Responsibilities as laid out in DHS 4300 A/B.
- The Contractor shall be designated as an ISSO for individual systems by a formal appointment letter from the OCIO Risk Management Division (RMD).
- The Contractor shall maintain the Security Authorization or Certification and Accreditation of their assigned system.
- The Contractor shall track the Security Authorization of their assigned system.
- The Contractor shall deliver all required documentation using the current DHS approved templates, forms, regulations, and methods.
- The Contractor shall continuously update all Security Authorization documentation as required by the ISSO Standard Operating Procedure (SOP) and the Cloud Support documentation.
- The Contractor shall provide advisement to stakeholders to assign resources and establish timelines to ensure the successful Security Authorization of a system.
- The Contractor shall maintain all required documentation to maintain their assigned system's Authority to Operate or system go live dates on the tracking site.
- The Contractor shall document all relevant NIST 800-53 (continuously current version) and 4300A (continuously current version) Security Controls and/or applicable departmental policies for each IT system the Software Security Support is responsible for.

- The Contractor shall draft a Security Package and perform any modifications throughout the lifecycle of the IT system.
- The Contractor shall draft a Control Implementation Summary (CIS) and perform any modifications throughout the lifecycle of the IT system.
- The Contractor shall work closely with the System Owner to identify any additional controls that are applicable to the system to maintain a favorable security posture.

4.4.14 TASK FOURTEEN. Security Engineering Services

The Contractor shall engineer, architect, implement, deploy, maintain, and administer commercial and open-source products. The Contractor shall provide personnel that are "hands-on", highly technical, expert security engineers with the ability to engineer, implement, and support security applications, as well as, generate supporting technical documentation. The Contractor shall maintain existing tools and systems as well as support the security activities associated with the evaluation and introduction of new security technologies into the CIO environment. This includes but is not limited to the following:

- The Contractor shall provide support on all information security activities at the program level including policy development, compliance inspections, audits, reviews and communications security.
- The Contractor shall provide support and work on the development phases of information security systems development lifecycle.
- The Contractor shall oversee, evaluate, and support the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements and ensures compliance from internal and external perspectives.
- The Contractor shall conduct assessments of threats and vulnerabilities, determine deviations from acceptable configurations, enterprise or local policy, assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations.
- The Contractor shall document incident correlation requirements, select incident correlation engines and recommend configuration guidelines. The Contractor shall perform analysis to determine the optimum configuration of network and host sensors. This analysis includes traffic load analysis, performance impacts of monitoring, determination of potential attack characteristics based on mission and infrastructure, and determination of site-specific data collection requirements.
- The Contractor shall analyze and recommend resolution of information security problems based on knowledge of the major information security products and services, an understanding of their limitations, and a working knowledge of the disciplines of information security.

4.4.15 TASK FIFTEEN. Configuration Management Support

The Contractor shall provide Configuration Management (CM) support activities to the OCIO. These include but are not limited to the following:

- The Contractor shall support CM Boards and Project Teams through activities and deliverables such as project status reports, design documents, design validation, migration planning, service delivery guidance, and implementation support documents.
- The Contractor shall develop, maintain, update, and implement CM plans and procedures, control configuration baselines, conduct functional and physical configuration audits, and formal qualification reviews.
- The Contractor shall submit proposed changes to DHS systems or to project baselines to the Change Control Board (CCB) and the Technical Working Group (TWG), maintain a record of all submitted and approved changes, and maintain a schedule of deliverables showing both the scheduled and actual delivery dates.
- The Contractor shall develop, maintain, update, and implement a Configuration Management Data Base (CMDB), an engineering release system, a configuration item development record (including the configuration index and change status listing), configuration status accounting, and support the CCB.

4.4.16 TASK SIXTEEN. Support for New and Evolving Technologies

The dynamic nature of the OCIO mission results in rapidly changing requirements. There may be work surges to support changing priorities due to new and updated initiatives and additional resources may be needed to assist with these efforts. As such, the technologies that the Contractor shall support will change to accommodate these changes during the ordering period of the BPA. The Contractor shall assist the Government with support for these evolving technologies as they are introduced to DHS.

4.4.17 TASK SEVENTEEN. Engagement and Facilitation of Key Stakeholders

The Contractor shall provide engagement and facilitation support activities to the OCIO including project kickoffs, weekly meetings, monthly touchpoints and other facilitation projects as needed by the OCIO.

4.4.18 TASK EIGHTEEN. User Interface / User Experience Design

The Contractor shall provide support activities to improve usability, user experience, and driving user adoption and engagement. This includes conducting user research, analysis & synthesis, persona development, interaction design, and usability testing to create products in support of the OCIO customers.

4.4.19 TASK NINETEEN. Integration with database and applications

The Contractor shall provide an integration and database application service to ensure that various applications and data store across the enterprise work together seamlessly. The Contractor shall assist with systems administration, database and system design, including the design and implementation of the next-generation database and multi-tier solutions for both new and existing data bases and client-server applications.

The Contractor shall provide enterprise application integration to enable data propagation and business process execution across various applications to support complex operational business functions such as fulfilling a customer mission.

4.4.20 TASK TWENTY. Analytics and Reporting

The Contractor shall provide analytics and reporting support activities to the OCIO. These include but are not limited to the following:

- Review existing analytic metrics for effectiveness and make recommendations for the metrics
- Review existing reports for effectiveness and make recommendations for reporting content
- Provide expertise for project reporting as well as portfolio reporting for the divisions.

4.4.21 TASK TWENTY-ONE. Knowledge management, communications, and graphics support

The Contractor shall provide knowledge management, communications, and graphics support activities to the OCIO. These include but are not limited to the following:

- Development of communication artifacts such as emails, newsletters, surveys to increase knowledge and engagement of stakeholders as well as identify potential new clients.
- Create information packets, presentations, and informational one page "slick sheets" to increase awareness of OCIO programs to increase adoption.
- Create graphics for web and print media.
- Update existing repositories of information to encourage sharing, re-use and adoption of specific OCIO initiatives.

4.4.22 TASK TWENTY-TWO. Business Intelligence, dashboard and analytics support

The Contractor shall improve system integration and reporting capabilities by:

- Providing the tools necessary to illustrate data for information sharing and reporting.
- Integrating priority dashboards and reporting capabilities to ensure better information sharing in addition to comprehensive assessments of management health.
- Promoting sound decision making and improving the efficiency and effectiveness of the Department by providing data visualizations to program managers and senior leaders.
- Tools currently used for dashboards and analytics are Tableau, Oracle Business Intelligence Enterprise Edition, Oracle Data Visualizer, Oracle Visual Analyzer, R Studio, Erwin and Informatica but the government is looking for innovative solutions to improve this area.

4.4.23 TASK TWENTY-THREE. Transition In and Transition Out

4.4.23.1 The Contractor shall provide transition in support. The Contractor shall support the knowledge transfer from outgoing Contractors and undertake support of all prior or ongoing tasks. The Contractor shall make staff available for hands on facilitation so that the Government may receive continuous services. All documentation produced for the Government in the possession of the Contractor that supports prior or ongoing tasks shall be made available and provided to the incoming Contractor.

4.4.23.2 The Contractor shall provide transition out support. The Contractor shall support the knowledge transfer to incoming Contractors which will undertake support of all prior or ongoing tasks. The Contractor shall make staff available for the knowledge transfer and hands on facilitation so that the Government may receive continuous services from the incoming Contractor. All documentation produced for the Government in the possession of the Contractor that supports prior or ongoing tasks shall be made available and provided to the incoming Contractor.

5.0 Quality Control/Quality Assurance

Quality Control and Quality Assurance will be integrated into the service and project implementations. Each project and service stand up will be defined and implemented using the PMBOK best practices. In addition, the projects will use the approved DHS application lifecycle management software for end to end management of the Quality Control and Quality Assurance processes. The Quality Control Plan and Quality Assurance activities will be defined at the individual order level.

6.0 Deliverables

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	12.4	Post Award Conference	Ten (10) calendar days after the BPA Order award	BPA Order COR and Contracting Officer
2	13.1	Small Business Subcontracting Plan	To be submitted as part of the quote submission at the BPA Order level	BPA Order Contracting Officer
3	13.1	Individual Subcontracting Reports (ISR)	Semiannually due by April 30 and October 30	BPA Order COR and Contracting Officer
4	13.1	Summary Subcontracting Reports (SSR)	Annually due by October 30	BPA Order COR and Contracting Officer
5	If required at the BPA Order level	IT Security Plan	Ten (10) calendar days after the BPA Order award	BPA Order COR and Contracting Officer

7.0 Period of Performance

This multiple-award BPA will have a five (5) year ordering period from the date of award.

7.1 BPA Order Period of Performance

The period of performance for each order placed under this BPA shall be specified in the

individual order. Under no circumstances may an order be placed under this BPA if the BPA has expired, or has been terminated or cancelled by the Government.

BPA orders issued in the final year of the BPA shall not extend beyond twelve (12) months after the period of performance of the final ordering period. Each BPA order's terms shall be consistent with the BPA terms and conditions and comply with the appropriation law.

7.2 Facility Security Clearance Requirements.

The Contractor shall possess and maintain a "Top Secret" facility clearance granted from the Defense Security Service at the BPA level.

8.0 Place of Performance

Work will be performed on-site at Government facilities within the Washington D.C. Metropolitan Area, the Contractor's site, and teleworking site(s) as directed and approved by the COR on each BPA order.

9.0 Telework for Contractor Personnel

Should the Contractor utilize telework for its employees in the performance of work at the order level, the Contractor shall provide copies of all applicable telework agreements to the BPA Order COR for approval within ten (10) business days after BPA order award. The BPA Order COR must approve a telework request in writing.

10.0 Hours of Operation

Contractor employees shall generally perform all work between the normal business hours of 7:00 AM - 6:00 PM, Eastern Time (ET), Monday through Friday (except Federal holidays). However, there may be occasions when contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill the requirements of each individual order. Any work that is to be performed outside of normal business hours, on weekends, or on Federal holidays (including overtime), must be approved in writing in advance by the BPA order COR prior to any work being performed.

Federal holidays include the following:

New Year's Day
Martin Luther King's Birthday
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day

Any day specifically declared by the President of the United States of America as a national holiday.

If a holiday falls on Sunday, the following Monday will be observed as the legal holiday. When a holiday falls on a Saturday, the preceding Friday is observed as a legal holiday by U.S. Government agencies.

No work shall be performed by Contractor personnel on Government facilities or offsite via telework on Federal holidays, other non-work days, or in the case of a pandemic or other emergency/unforeseen situation, such as an epidemic, natural disaster, early closing or delayed opening of the Government, as well as a Government shutdown without prior written approval of the BPA Order CO. In the event that work is approved given one of the aforementioned situations, costs incurred shall be in accordance with the rates agreed to in the approved business continuity plan, if applicable to the individual order.

11.0 Annual Review of BPA

In accordance with FAR Subpart 8.405-3(e), and as applicable, the BPA will be reviewed annually to determine in writing whether or not:

(i) The schedule contract, upon which the BPA was established, is still in effect;
(ii) The BPA still represents the best value (see FAR 8.404(d)); and
(iii) Estimated quantities/amounts have been exceeded and additional price reductions can be obtained.

12.0 Contract Administration

12.1 General:

This section provides contract administration requirements for the BPA and where applicable, for each order placed under the BPA. Costs associated with these administration requirements shall not be billed as a direct cost to the Government.

Additional contract administration requirements, not related to the basic BPA, will be specified in each order. Costs associated with these administration requirements shall be billed in accordance with terms of the individual order.

12.2 Points of Contact:

The following describe the roles and responsibility of individuals who will be the primary points of contact for the Government on matters regarding contract administration as well as other administrative information. The Government reserves the right to unilaterally change any of these individual assignments at any time.

Contracting Officer for the BPA is:

(b)(6)
Department of Homeland Security, Office of Procurement Operations

Information Technology Acquisition Center MGMT/OPO/Mailstop 0115
245 Murray Lane, SW Building 410
Washington, DC 20528-0115
Tel: (b)(6)
E-mail: (b)(6)

Contracting Specialist for the BPA is:

(b)(6)
Department of Homeland Security, Office of Procurement Operations
Information Technology Acquisition Center MGMT/OPO/Mailstop 0115
245 Murray Lane, SW Building 410
Washington, DC 20528-0115
Tel: (b)(6)
E-mail: (b)(6)

Contracting Officer's Representative for the BPA is:

(b)(6)
Tel: (b)(6)
E-mail: (b)(6)

Individual COR appointments will be designated at the BPA order level and the roles and responsibilities will be identified in the official COR appointment letter.

12.3 Unauthorized Work

The Contractor is not authorized at any time to commence with BPA order performance prior to issuance of a signed BPA order or other written approval provided by the BPA Order CO to begin work.

12.4 Post Award Conference

The Contractor shall attend a Post Award Conference with the BPA order Contracting Officer and the BPA order COR no later than ten (10) calendar days after the date of order award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss the technical and contracting objectives of the order. The Post Award Conference is at no additional cost to the Government. The Contractor is responsible for and shall prepare the meeting minutes from the Post Award Conference and shall provide the meeting minutes to the CO and the COR within 7 calendar days of the Post Award Conference. The Post Award Conference will be held at the Government's facility and/or on conference line.

12.5 Order of Precedence

The order of precedence shall be in accordance with FAR 52.212-4(s). In the event of any inconsistencies between the provisions of the BPA and the GSA Schedule, the provisions of the latter will take precedence. The Contractor shall not change, condition, or deviate from the BPA's pricing terms, or cause such to occur by virtue of not strictly complying with the terms and conditions of the RFQ and the resulting BPA.

12.6 Materials on T&M Orders

Materials are defined in the paragraph (i)(1)(ii) of the clause at FAR 52.212-4, *Contract Terms and Conditions—Commercial Items - Alternate I.* For each proposed order involving materials, the Contractor's quote shall identify the elements of other direct costs for the proposed order (see para. (i)(1)(ii)(D)(1)) and a fixed amount for indirect costs and payment schedule (see para. (i)(1)(ii)(D)(2)). In addition, *Materials* are defined in the clause at 52.232-7, *Payments under Time-and-Materials and Labor-Hour Contracts*.

All materials required for performance under the BPA orders issued pursuant to this BPA that are not Government-furnished, shall be furnished by the Contractor.

The Contractor may expect to incur other direct costs (ODC) for the BPA orders. When materials/ODC expenses should become necessary, the Contractor must first contact the COR in writing prior to the planning or commencement of any Contractor procurements. The Contractor shall seek the COR's approval in advance of incurring any cost associated with ODC's. All ODC's shall be approved by the order level COR and CO.

The Contractor shall provide estimated costs; including at least three (3) price quotes with approval request. After approval from the BPA Order CO, allowable and reasonable costs incurred by the Contractor for ODCs will be reimbursed. All ODC's must be on the Contractor's GSA schedule or teaming partners. However, for administrative convenience, the BPA Order CO may add items not on the Contractor's Federal Supply Schedule (also referred to as open market items) only if -

(1) All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed;

(2) The contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;

(3) The items are clearly labeled on the order as items not on the Federal Supply Schedule and they conform to the rules for numbering line items at subpart 4.10; and

(4) All clauses applicable to items not on the Federal Supply Schedule are included in the order

All materials purchased by the Contractor (if authorized) for the use or on behalf of the Government shall become the property of the Government. The transfer of materials shall be documented by the Contractor; in addition to an accounting of all materials consumed during the performance of individual tasks of the contract. The Contractor

shall furnish the Government a copy of such documents with the Monthly Progress Reports as directed in the individual BPA order. The Contractor shall not charge the Government any associated fees or profit over actual cost incurred for ODCs. Material handling fee is allowed. Receipts shall be provided for each ODC incurred. Once the Government approves the proposed costs, the Contractor shall not exceed the funded amount. The Contractor shall not exceed this amount without prior authorization of the Contracting Officer.

12.7 Travel Cost

Contractor travel may be required to support BPA order requirements. All Government directed travel outside the local commuting area(s) will be handled as a "direct reimbursable". All reimbursement for allowable travel cost shall be made in accordance with the Federal Travel Regulation (FTR).

Profit shall not be applied to travel costs. Contractors may apply indirect costs to travel in accordance with the Contractor's usual accounting practices consistent with FAR 31.2. An order authorizing Contractor travel will include a separate not-to-exceed CLIN for travel.

The Contractor shall be responsible for obtaining the BPA Order COR's written approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event. The locations and durations of this travel will be determined as needed by the Government. The Government will not reimburse the contractor for local commuting to work or other travel related to the Contractor's conduct of its business. All reimbursements for travel related expenses including but not limited to airfare, lodging, meals, rental cars, and incidental expenses incurred by the contractor to perform specific tasks required shall be made in accordance with the FTR and FAR 31.205-46.

The Contractor shall provide a Trip Report for each trip associated with a travel approval. The Contractor shall maintain a summary of all approved travel, to include at a minimum, the name of the traveler, location of travel, duration of trip, reason for travel, and the total cost of the trip.

12.8 Invoicing and Payment

The requirements of a proper invoice are as specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the order transmission issued against this BPA. In addition to the GSA Schedule Contract Invoicing and Payment Provisions, additional invoicing and payment instructions for Labor Hour (LH) or Time and Material (T&M) orders may be specified in the individual orders issued under this BPA.

The terms and conditions included in this BPA apply to all orders made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor's invoice, the provisions of this BPA will take precedence.

12.9 Contractor Performance Assessment Reporting System (CPARS)

In accordance with FAR 42.15, "Contractor Performance Information," past performance

evaluations shall be prepared for each BPA order that exceeds (b)(4) for services and (b)(4) for products per DHS FAR Class Deviation 11-03.

CPARS is a web-enabled application that collects and manages the library of automated CPARs reports. CPARS is for UNCLASSIFIED use only. Classified information is not to be entered into this system. The CPARS allows contractors to review and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS, it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

The designated Contractor Representative (CR) is required to register in CPARS, so the CR will be allowed to access and review the past performance reports submitted.

Contractors must register at the following websites:

CPARS: (b)(6) : (b)(6)

12.10 Government Furnished Equipment

The Government will provide the workspace, equipment, and supplies necessary to perform the on-site portion of Contractor services required in each BPA order. Specific information regarding Government Furnished Information (GFI) and Government Furnished Equipment (GFE) will be provided at the BPA order level.

13.0 Special Contract Requirements

13.1 Goals for Small Business Subcontracting

DHS is committed to ensuring that small business (SB), HUB Zone small business, small disadvantaged business (SDB), women-owned small business (WOSB), veteran-owned small business, and service-disabled veteran owned small business (SDVOSB) concerns are provided maximum practicable opportunity to participate as subcontractors in the performance of the BPA. The Contractor shall use the below small business subcontracting goals for individual orders placed under the BPA.

2018 Small Business Subcontracting Goal	
Category	**Percentage**
SB Subcontracts	(b)(4)
SDB Subcontracts	
WOSB Subcontracts	
HUBZone Subcontracts	
SDVOSB Subcontracts	

13.2 Contractor Personnel

13.2.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all of the requirements specified in this SOW. See Appendix B for labor category descriptions.

13.2.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support is maintained at all times. The Contractor shall ensure that all BPA support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to the employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

13.2.3 Key Personnel

13.2.3.1 Contractor Key personnel shall not be assigned by the Contractor to more than one key position at any time during the period of performance of any awarded order.

13.2.3.2 Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer (CO) no less than fifteen (15) calendar days in advance, submit written justification for the replacement, and provide a resume with the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace Key Contractor personnel without prior written approval from the Contracting Officer.

The following positions are designated as Key at the BPA level.

- BPA Program Manager
- Senior Architect/Solution Architect

13.3.4 BPA Program Manager

The Contractor shall provide a BPA Program Manager for the BPA who shall be responsible for all Contractor work performed under each BPA order. The BPA Program Manager shall be a single point of contact for the BPA Contracting Officer and the COR. During any absence of the BPA Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under any order. The BPA Program Manager and all designated alternates shall be able to clearly and concisely read, write, speak and understand English. Additionally, the Contractor shall not replace the BPA Program Manager without prior written approval from the BPA Contracting Officer. The BPA Program Manager is a non-billable position at the BPA level.

13.3.4.1 In the event there is any issues on the BPA Order, the BPA Program Manager shall be available to the BPA COR via telephone. The BPA Program Manager shall respond to a request for discussion or resolution of systemic problems at the BPA and BPA order level.

13.4 Training of Contractor Employees

The Contractor shall provide employees with the required core skills to meet the requirements of the associated orders. Training to build or maintain expertise of contractor employees assigned to each BPA order shall be provided by the contractor at its own expense, except when the Government has given prior approval for training to meet special requirements that are peculiar to a particular task. Contractor employees may attend seminars, symposiums, or user group conferences only if the Government certifies that attendance is mandatory for the performance of the task requirements and the COR approves such training in advance.

Reimbursement for training shall not be authorized for replacement contractor employees, for the purpose of keeping contractor employees abreast of advances in the state of the art technologies used, nor for training contractor employees on equipment, computer languages, or computer operating systems that are available on the commercial market. The Contractor shall have full responsibility for keeping contractor employees trained and abreast of advances in the standard commercial and network technologies as implemented in the IT industry.

13.5 Employee Identification

13.5.1 Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

13.5.2 Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

13.6 Employee Conduct

Contractor employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The BPA Program Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

13.7 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer), request the

Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the order. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

13.8 Branding

The Contractor shall comply with the requirements of any DHS branding and marking policies. Federal criminal statutes prohibit unauthorized use of the DHS seal. DHS policy prohibits granting authorization for certain commercial uses of the seal. It is permissible to reference DHS in materials if the reference is limited to true, factual statements. The words DHS and/or Homeland Security should appear in the same color, font, and size as the rest of the text in the document. Moreover, such references shall not imply in any way that it is an endorsement of a product, company, or technology.

Requests to use the DHS seal shall be submitted using the DHS Official Seal Usage Approval Form, available from the COR. The comments section shall be used to describe why use of the seal is being requested, and how it will be used. Completed forms shall be sent via e-mail to branding@hq.dhs.gov, and to the CO, with a copy to the COR.

13.9 Advertisements, Publicizing Awards and News Release

DHS will not issue any press release regarding this BPA without coordination with the Contractor. All press releases or announcements about agency programs, projects, and order awards shall be submitted by the Contractor for approval by the BPA CO. Under no circumstances shall the contractor, or anyone acting on behalf of the contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this BPA in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the BPA CO.

In accordance with the HSAR 3052-205-70, the Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

This section is applicable to the BPA and all BPA orders.

13.10 Accessibility Requirements (Section 508 Compliance)

13.10.1 Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

13.10.2 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

13.10.3 Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

13.10.4 Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are

available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

13.11 DHS Enterprise Architecture Compliance

All solutions and services provided by the Contractor shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards shall comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts shall be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

13.12 Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in each individual order are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of each individual order. The Contractor shall contact

the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

13.13 Interconnection Security Agreement (ISA)

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

13.14 Encrypted Data

All encryption of data shall be FIPS 140-2 and FIPS 197 Advanced Encryption Standard (AES) 256 encryption compliant. The following methods are acceptable for encrypting sensitive information:

a. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

13.15 Non-Disclosure Requirements

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the BPA orders issued or who are required to act on behalf of the BPA, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a DHS Non-Disclosure Agreement (DHS Form 11000-6) to the COR. This is required prior to the commencement of any work on a specific order and whenever replacement personnel are proposed under an existing order. Any information obtained or provided in the performance of the order is only to be used in the performance of the order.

13.16 Protection of Information

Contractor access to proprietary information may be required under individual BPA orders. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

13.17 Occupational Safety and Health Act Requirements

This BPA requires that Occupational Safety and Health Act (OSHA) requirements be met when applicable. The BPA and orders issued under this BPA may contain mandatory

clauses relating to Environment, Safety, and Occupational Health (ESOH) considerations.

13.18 Security Requirements

Contractor access to unclassified but Security Sensitive Information may be required under individual BPA orders. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination. Contractor access to classified information is not currently required under this BPA. However, the Government at a later date may require all Contractor personnel to have at a minimum, a Secret security clearance. Accordingly, all Contractor employees provided for individual BPA orders must be eligible for a "Top Secret/SCI", "Top Secret" or "Secret" Clearance. Specific level of clearance will be specified at the BPA order level.

13.19 Suitability Determination

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision will allow the contractor employees to commence work temporarily prior to the completion of a fitness/risk assessment. The granting of a favorable EOD decision shall not be considered as assurance that a full employment fitness determination will follow. A favorable EOD decision or a full employment suitability/fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the order. No employee of the Contractor shall be allowed unescorted access to a DHS Government facility without a favorable EOD decision or fitness determination by the Office of Security, Personnel Security Division.

Contractor employees waiting for an EOD decision may begin work on the order provided they do not access sensitive Government information. Limited access to Government buildings is allowed prior to the EOD decision if the Contractor is escorted by a Government employee ONLY. This limited access is to allow Contractors to attend briefings and non-recurring meetings to begin work.

13.20 Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribes policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all BPA orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the BPA order.

13.21 Compliance with DHS Security Policy

All services provided under each individual BPA order must be compliant with DHS Information Security Policy, identified in MD 4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook.

13.22 Post-Award Instructions Regarding Security Requirements for Contracts/BPA Orders

1. The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process background investigations and suitability determinations, as required, in a timely and efficient manner.

2. Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is mandatory.

a. Contractor employees (to include applicants, temporaries, part-time and replacement employees) under each individual order, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the order. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security Office/PSD. Prospective Contractor employees shall submit the following completed forms to the DHS Office of Security Office/PSD. The Standard Form (SF) 85P will be completed electronically through the Office of Personnel Management's e-QIP System. The below completed forms must be given to the DHS Office of Security Office/PSD no less than thirty (30) days before the start date of the order or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1) Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
2) FD Form 258, "Fingerprint Card" (2 copies)
3) DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
4) DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

b. Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon award of each individual order.

c. DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the order. No employee of the Contractor shall be allowed

unescorted access to a Government facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

Contractor employees waiting for an EOD decision may begin work on the order provided they do not access sensitive Government information. Limited access to Government buildings is allowed prior to the EOD decision if the Contractor is escorted by a Government employee ONLY. This limited access is to allow Contractors to attend briefings and non-recurring meetings to begin work.

d. The DHS Office of Security/PSD shall be notified of all terminations/resignations within five (5) calendar days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

e. Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process, which are not caused by the Government, do not relieve a contractor from performing under the terms of the order.

f. Your POC at the Security Office is:

(b)(6)

(b)(6)

APPENDIX A

The following clauses apply in addition to those already in the Contractor's GSA Schedule 70 contract.

A.1 FAR Clauses Incorporated By Reference (FAR 52.252-2) (FEB 1998)

This BPA incorporates one or more clauses by reference, with the same force and effect as if they were given full text. Upon request, the CO will make their full text available. Also, the full text of a clause may be accessed electronically at the following addresses:

http://www.acquisition.gov/far/farqueryframe.html, or for DHS specific clauses at http://farsite.hill.af.mil/VFHSAR1.htm

The following clauses are incorporated by reference:

FAR Clauses/ Provisions	Title	Date
52.202-1	Definitions	Nov 2013
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	Apr 2014
52.204-2	Security Requirement	Aug 1996
52.204-9	Personal Identity Verification of Contract Personnel	Jan 2011
52.209-2	Prohibition On Contracting With Inverted Domestic Corporations--Representation	Nov 2015
52.209-10	Prohibition on Contracting With Inverted Domestic Corporations	Nov 2015
52.212-4	Contract Terms and Conditions – Commercial Items & Alternate I	Jan 2017
52.217-4	Evaluation of Options Exercised at Time of Contract Award	Jul 1988
52.217-5	Evaluation of Options	Jul 1990
52.227-1	Authorization and Consent	Dec 2007
52.227-14	Rights in Data—General	May 2014
52.232-7	Payment under Time-and-Materials and Labor-Hour Contracts	Aug 2012
52.232-22	Limitation of Funds	Apr 1984
52.237-3	Continuity of Services	Jan 1991
52.242-15	Stop-Work Order	Aug 1989
52.245-1	Government Property	Jan 2017
52.246-4	Inspection of Services – Fixed Price	Aug 1996
52.246-6	Inspection – Time-and-Materials and Labor-Hour	May 2001

52.217-8 -- Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

(End of clause)

A.2 HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLAUSES

The following Homeland Security Acquisition Regulation (HSAR) clauses are included in full text form. All HSAR clauses shall flow down to all subcontractors on the BPA and BPA orders as applicable:

DHS Clauses/ Provisions	Title	Date
3052.203-70	Instructions for Contractor Disclosure of Violations	Sep 2012
3052.205-70	Advertisements, Publicizing Awards, and Release Alt I	Sep 2012
3052-215-70	Key Personnel or Facilities	Dec 2003
3052.222-70	Strikes or picketing affecting timely completion of the contract work	Dec 2003
3052.222-71	Strikes or picketing affecting access to a DHS facility	Dec 2003

HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources. (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within ten (10) calendar days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the quoter's quotation. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted;and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within six (6) months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditationdocumentation.

(End of clause)

HSAR 3052.204-71 Contractor Employee Access. (SEP 2012)

(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/herdesignee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the

Assistant Secretary for the Transportation Security Administration or his/herdesignee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as maybe necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continuedemployment contrary to the public interest for any reason, including, but not limited to, carelessness, in subordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

HSAR 3052.209-72 Organizational Conflicts of Interest (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the

limitation on future contracting is that provider(s) of ADaPTS support may not be eligible to compete for system development or integration services for DHS Acquisition programs (for both DHS headquarters and components), as they will have access to procurement-sensitive information on Government cost estimates, pre-solicitation information on requirements, funding information and acquisition strategies.

DHS cannot forecast at this time which specific future acquisitions could give rise to a conflict.

DHS anticipates that the following types of conflict may arise:
(1) Potential offerors may have had access to non-public Government information that would provide an unfair competitive advantage under the present RFP,
(2) Potential offerors may have an unfair competitive advantage because they developed or established the ground rules for the present RFP, or
(3) Potential offerors may have unfair competitive advantage because they have been in a position to evaluate other potential competitors or they had access to the non-public information of other potential competitors under this RFP.

(b) Conflicts of interest will be evaluated case-by-case for each BPA call. If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the Offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the Offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the Offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the Offeror may be found ineligible for award.

(c) Disclosure: The Offeror hereby represents, to the best of its knowledge that:
___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or
___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an Offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the Offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. Offerors are cautioned that a ground rules conflict typically cannot be mitigated.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the Offeror. The Contracting Officer will use all information submitted by the Offeror, and any other relevant information known to DHS, to determine whether an award to the Offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful Offeror shall inform the Contracting Officer within

thirty calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

HSAR 3052.209-73 Limitations of Future Contracting (JUN 2006)

The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5 - Organizational Conflicts of Interest.

(a) The nature of this conflict is that provider(s) of ADaPTS support may not be eligible to compete for future system development or integration services for DHS Acquisition programs (for both DHS headquarters and components), as they will have access to procurement-sensitive information on Government cost estimates, pre-solicitation information on requirements, funding information and acquisition strategies.

(b) Conflicts of interest will be evaluated case-by-case for each BPA call. If a conflict cannot be mitigated, the restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

Contractors shall be responsible and accountable for ensuring compliance with all Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The contractor security procedures shall be the same or greater than those that are provided by DHS Enterprise Data Center(s).

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system. At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' 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 shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture to the best of its ability and to the satisfaction of the DHS COR. Areas of consideration could include:

1) Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2) Compliance to DHS Identity Credential Access Management (ICAM)
3) Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response

4) Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5) Performance of activities per continuous monitoring requirements
6) Use of The Open Group Architecture Framework (TOGAF) and OMB Federal Enterprise Architecture (FEA) artifacts.
7)

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan. Any cost associated to standing up a SOC will be determined at the order level.

Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall

notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration. Any cost associated to standing up a CIRT will be determined at the order level.

Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security and determined at the BPA order. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and

comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The Contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for one-hundred eighty (180) calendar days and offline for three (3) years.

Personal Identification Verification (PIV) Credential Compliance
Authorities:

- HSPD-12 —Policies for a Common Identification Standard for Federal Employees and Contractors
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 —Acquisition of Products and Services for Implementation of HSPD-12
- NIST FIPS 201 —Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-63 —Electronic Authentication Guideline
- OMB M-10-15 —FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV

credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

APPENDIX B

BPA LABOR CATEGORY DESCRIPTIONS

General work experience may be substituted for education. The requirement for education levels can be substituted at the rate of 1.5 years of experience for every year of education. An associate's degree is 2 years of education, a Bachelor's degree is 4 years of education, and a Master degree is 6 years of education. The work experience to be substituted for education must be in a relevant field such as Information Technology, Information Security, or a MBA. The years of specific experience used for satisfying an education requirement cannot also be used as filling the work experience requirement.

Labor Category: IT Program Manager
Minimum Experience/Requirements: Minimum of seven (7) years' experience
Functional Responsibility:

- Manages long-term IT projects, performs design evaluations and works to complete projects within budget and scheduling restraints.
- Develops and implements long-term IT roadmaps and strategy, and monitors alignment of tactical activities.
- Provides higher-level view of activities occurring within the enterprise and the impacts on information sharing initiatives.
- Performs risk management, including identifying, prioritizing, and mitigating risks, and communicating and escalating risks and issues
- Provide the ability to manage projects that may vary by project type (i.e., a new project, an existing project, a project being transitioned from another delivery provider, etc.), size, complexity, project life cycle phases, development methods (e.g. SCRUM, spiral, etc.).
- Support the development of briefings, agendas, and other general documentation support as directed, including training material and demonstration sessions for new and existing technologies to various DHS stakeholders.
- Support a continuous improvement process by providing recommendations on improving products, services, and processes.
- Develop Communication Plans
- Develop and manage project schedules, including integrated project schedules, and plans using the tools as defined by the Government (i.e., Microsoft Project, JIRA).
- Support Management of projects within schedule and budget and defined by the Government.
- Ensure the team delivers Agile development artifacts, which will include Project Sprint/Product/Release Backlogs, Burn-downs/ups, Team Velocity, RTM, etc.

Minimum Education: A Bachelor's Degree.

Labor Category: Project Manager

Minimum/General Experience: Minimum of five (5) years' experience and PMP Certification, most of which must have been in information systems development, project management from inception to deployment; demonstrated ability to manage a team.
Functional Responsibility:

- Management and technical direction of projects
- Project performance including cost, schedule, deliverables, and contractual compliance, and is accountable for the quality and timely delivery of all project deliverable items
- Overall project/task performance
- Enforcing work standards, task schedules, reviewing work discrepancies, supervising technical personnel, recommending project hires and terminations, and communicating policies, purposes, and goals of the organization to subordinate personnel
- Assisting in the budgeting of required resources for successful project implementation and completion.

Minimum Education: A Bachelor's Degree with 24 credit hours in business related courses.

Labor Category: Subject Matter Expert III
Minimum/General Experience: Minimum of eleven (11) years progressive technical or functional experience in a selected technical area or specialty skill.
Functional Responsibility:

- Leads strategic planning initiatives in a select technical or functional area
- Meets with management and the team members frequently to propose initiatives, help foster adoption of technologies and establish priorities.

Minimum Education: A Bachelor's Degree.

Labor Category: Analyst
Minimum/General Experience: Minimum of three (3) years' experience in systems analysis and design of large information systems programs.
Functional Responsibility:

- Understanding business requirements so that they may be accurately translated in system requirements
- Understanding the design of simple information systems so that functional issues may be understood and business requirements can be properly defined for software development
- Conducting trade-off analysis on business and technical requirements
- Assisting in the development of procedures, manuals and other documentation for complex information systems

Minimum Education: A Bachelor's Degree in an IT discipline.

Labor Category: Senior Analyst
Minimum/General Experience: Minimum of seven (7) years' experience in systems analysis and design of information systems programs
Functional Responsibility:

- Understanding business requirements so that they may be accurately translated in system requirements
- Understanding the design of moderately complex information systems so that functional issues may be understood and business requirements can be properly defined for software development.

- Helping to define how information systems may be upgraded or replaced
- Conducting trade-off analyses on business and technical requirements
- The ability to quickly develop a working understanding of the applicable programming languages, operating systems and databases that will be used on the projects and programs
- Developing procedures, manuals and other documentation for information systems
- Overseeing work of Analysts on specific tasks

Minimum Education: A Bachelor's Degree

Labor Category: Financial Analyst
Minimum/General Experience: Minimum of seven (7) years' experience in systems analysis and design of information systems programs, and at least five (5) years' experience in information technology focusing on financial management.
Functional Responsibility:

- Provide expertise in Financial Management, and share knowledge of Financial Management industry standards and best practices, while being able to adjust and tailor accordingly based on the Government's methodology and requirements.
- Perform financial reporting
- Prepare Memorandum of Agreements to include cost analysis
- Manage financial burn on various activities such as Data Center, MOAs, and IAAs etc.
- Ensure funds are received, utilized, and allocated per Government requirements
- Utilize tools as specified by the Government (i.e., reporting, management tools, etc.)
- Deliver defined reports per the agreed to schedule and, where applicable, ad-hoc reports.
- Provide ad hoc financial management support, as needed

Minimum Education: A Bachelor's Degree

Labor Category: Senior Architect/Solution Architect
Minimum/General Experience: Minimum of seven (7) years' experience in design, analysis, and implementation of information systems architecture.
Functional Responsibility:

- Responsible for driving multiple customer solution design projects in parallel
- Conduct business and technical discovery with customers
- Problem solve novel solutions, architectures and use cases to help customers meet their objectives
- Provide robust recommendations for engagements while also identifying critical dependencies & gaps
- Present proposals to senior government officials in a clear and compelling way
- Continuously improve the team's knowledge, methodologies and inventory of solution design blueprints for key customer segments and classes of use cases.
- Experience working in a top-tier technical consulting or software development
- Strong drive to solve customer problems and drive projects end to end from ideation to deployment

- Balance of business and technology acumen, including ability to articulate high-level technical solutions to business problems and to tie your solutions to program success criteria
- Capable of independently applying a wide set of engineering disciplines for planning, design, analysis, coding, testing, roll-out and support of information systems architectures.
- Responsible for, or assists in, the designing of interface standards, quality assurance standards, performance standards, and cost-benefit analysis of modem state-of-the art information systems.
- Analyzes available technologies and makes recommendations of technologies to use and how best to use them.
- Outstanding problem solving and analytical skills, including ability to create clear observations, analysis and conclusions based on customer interviews and data
- Outstanding communications skills both oral and written (e.g., PowerPoint)
- Team player who can collaborate with multiple stakeholders to arrive at the best solution
- High degree of intellectual curiosity and ability to learn and apply new concepts and technologies in a wide variety of marketing disciplines

Minimum Education: Minimum of 7 years overall software development experience; BS or MS in Computer Science, Engineering or comparable experience.

Labor Category: Developer
Minimum/General Experience: Minimum of three (3) years' experience in selected programming language or environment
Functional Responsibility:

- Applying expertise in software development to solving business issues
- With minimal supervision and assistance, designing and developing documents and tests, as well as maintaining applications in a selected programming language or environments
- Working with analysts and customers to derive requirements for use cases/scenarios, determining the feasibility of design within time and cost constraints, and consulting with hardware engineers and other engineering staff to evaluate the interface between hardware and software
- Planning, designing and programming functionality to interface and use SQL Server or Oracle in coordination with the Database Administrator
- Planning, designing and programming user interfaces
- Facilitating meetings to determine the validity and priority of issues found within products both internally as well as those reproduced that are logged through Technical Support
- Investigating, identifying and resolving code issues logged internally by our QA team and externally by our Clients through Technical Support
- Staying current with associated technology advances in the marketplace and growing skills
- Troubleshooting and resolving application issues

Minimum Education: A Bachelor's Degree

Labor Category: Senior Developer
Minimum/General Experience: Minimum of seven (7) years' experience in computer programming and analysis of complex information systems, application, or operating system software. Minimum of five (5) years' experience in select programming language or environment
Functional Responsibility:

- Appling expertise in software development to solving business issues
- Ability to clearly communicate technical concepts to both technical and non-technical users
- Possessing good client-facing interpersonal skills (i.e., comfortable and effective acting as liaison between multiple technology groups and representing groups in large scale meetings)
- Having experience in all phases of the systems engineering life cycle (SELC) including initial design/analysis through deployment.
- Designing and developing documents and tests and maintaining applications in a selected programming language or environment
- Working with analysts and customers to derive requirements for use cases/scenarios
- Determining the feasibility of design within time and cost constraints, and consulting with engineering staff to evaluate the interface between hardware and software.
- Planning, assigning work when acting in a lead role, determining designs, collecting metrics on all associated development tasks, coding, debugging, creating documentation, conducting tests and building applications on a predefined schedule.
- Producing and implementing design specifications, documenting design modifications and unit testing results
- Identifying and working with strategic and technology partners to discover new product solutions
- Planning, designing and programming functionality to interface and use SQL Server or Oracle in coordination with the Database Administrator
- Planning, designing and developing user interfaces
- Designing, developing and maintaining automated deployment processes and best practices for SharePoint solution deployments to multiple environments (features, WSPs, etc.)
- Maintaining current industry knowledge of development concepts, best practices and procedures as the technology base evolves
- Facilitating meetings to determine the validity and priority of issues found within products, both internally as well as reproduced issues logged through Technical Support
- Investigating, identifying and resolving complex code issues logged internally by the QA team and externally by our clients through Technical Support
- Staying current with associated technology advances in the marketplace and growing skills
- Troubleshooting and resolving application issues
- May have to supervise subordinate software programmers and assist in their creation of a quality product.

Minimum Education: A Bachelor's Degree in an IT discipline

Labor Category: Database Administrator (DBA) (Oracle and SQL Server)
Minimum/General Experience: Minimum of five (5) years' experience in Oracle or SQL Server Relational Database Management System (RDBMS).
Functional Responsibility:

- Providing technical expertise to create detailed database designs and documenting the results, including data models and flow diagrams
- Evaluating, configuring and optimizing databases to meet user requirements
- Determining data organization, indexing methods, and security designs for databases
- Planning and coordinating the conversion or migration of existing (orlegacy) databases to state of the art RDBMS
- Defining and creating databases for applications
- Managing development and operational databases, as well as performing maintenance actions and patches to sustain their health.

Minimum Education: A Bachelor's Degree.

Labor Category: Tester
Minimum/General Experience: Minimum of three (3) years' experience in developing or testing systems.
Functional Responsibility:
Without direct supervision, responsibility includes:

- Work with business and technical teams to understand the system to be tested
- Participate in application planning meetings.
- Develop and document application test plans based on software requirements and technical specifications.
- Develop test cases and prioritize testing activities
- Execute all test cases and report defects, define severity and priority for each defect Record and document results and compare to expected results.
- Detect software failures so that defects may be discovered and corrected.
- Generate historical analysis of test results.
- Document anomalies and issues.
- Maintain database or list of software defects.
- Examine code and execution of code in various environments.
- Verify specific action or function of code.
- Operate and maintain test networks.
- Create meaningful error handling procedures for application code.
- Carry out regression testing every time changes are made to the code to fix defects.
- Ensure data integrity standards.
- Perform reviews, walkthroughs, or inspections

Minimum Education: N/A

Labor Category: Configuration Manager
Minimum/General Experience: Minimum of four (4) years' experience in managing the configuration of software code and systems.
Functional Responsibility:
Without direct supervision, responsible for managing the configuration of:

- physical client and server hardware products and versions
- operating system software products and versions
- application development software products and versions
- technical architecture product sets and versions as they are defined and introduced
- live documentation
- networking products and versions
- live application products and versions
- definitions of packages of software releases
- definitions of hardware base configurations
- configuration item standards and definitions

The Configuration Manager shall help minimize the impact of changes; provide accurate information on CIs; improve security by controlling the versions of Configuration Items (CIs) in use; and project and program planning.
Minimum Education: A Bachelor's Degree.

Labor Category: Technical Writer
Minimum/General Experience: Minimum of four (4) years' experience in writing and editing technical documentation for technical systems in accordance with established writing standards.
Functional Responsibility:

Without direct supervision, responsibility includes:

- Collecting, analyzing, composing, and translating technical information into clear, readable documents to be used by both technical and non- technical personnel
- Obtaining data from technical staff by directly interacting with them and assisting in the creation of the technical documentation when needed
- Creating processes and procedures, user manuals, training materials, installation guides, and reports
- Editing requirements functional descriptions, system specifications, user manuals, special reports, or any other customer deliverables and documents

Minimum Education: A Bachelor's Degree.

Labor Category: Application Security Analyst
Minimum/General Experience: Minimum of five (5) years' experience in application information security support.
Functional Responsibility:

Without direct supervision, responsibility includes:

- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.

- Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.

Minimum Education: A Bachelor's Degree.

Labor Category: Security Engineer
Minimum/General Experience: Minimum of five (5) years' experience in application security engineering support.
Functional Responsibility:
Experience with working in a highly technical environment, be well versed in the current state of Information Security, and be able to interpret security requirements of relevant governing bodies (NIST, OMB, DHS, etc.) The SE will interface with federal employees and contractors to perform required support activities.

Without direct supervision, responsibility includes:

- Understanding of the DHS security engineering experience.
- Certifications and direct applicable experience in CEH, Amazon, Microsoft, Linux and Cloud.
- Direct DHS experience engineering and integrating secure solutions in cloud, data centers, networks, applications using Linux, windows, identity solutions, databases, firewalls, and networks appliances.
- Experience with Information Assurance Compliance tools (XACT, TAF, etc.)
- Knowledge of Federal Government Authorization processes (NIST 800-53, DHS 4300A, DIACAP).

Minimum Education: A Bachelor's Degree.

Labor Category: Interaction Designer / User Researcher / Usability Tester
Minimum/General Experience: Minimum of three (3) years' experience in Interaction design, user research, and usability testing.
Functional Responsibility:
The Interaction Designer / User Researcher / Usability Tester is part of a highly collaborative, multi-disciplinary team focused on improving usability, user experience, and driving user adoption and engagement. They are responsible for conducting user research, analysis & synthesis, persona development, interaction design, and usability testing to create products that delight our customers.
Primarily responsible for:

- Conduct stakeholder interviews, user requirements analysis, task analysis, conceptual modeling, information architecture, interaction design, and usability testing
- Design and specify user interfaces and information architecture
- Lead participatory and iterative design activities, including observational studies, customer interviews, usability testing, and other forms of requirements discovery
- Produce user requirements specifications & experience goals, personas, storyboards, scenarios, flowcharts, design prototypes, and design specifications
- Effectively communicate research findings, conceptual ideas, detailed design, and design rationale and goals both verbally and visually
- Plan and facilitate collaborative critiques and analysis & synthesis working sessions
- Work closely with visual designers and development teams to ensure that customer goals are met and design specifications are delivered upon
- Designs and develops primarily internet/web pages and applications
- Develops proof-of-concepts and prototypes of easy-to-navigate user interfaces (UIs) that consists of web pages with graphics, icons, and color schemes that are visually appealing
- Researches user needs as well as potential system enhancements
- Has familiarity to, or may actually: code, test, debug documents, and implement web applications using a variety of platforms
- Planning, recruiting, and facilitating the usability testing of a system
- Analyzing and synthesizing the results of usability testing in order to provide recommendations for change to a system
- May create such artifacts as Usability Testing Plan, Testing Scripts, and Usability Testing Report

Minimum Education: A Bachelor's Degree.

Labor Category: DevOps Engineer
Minimum/General Experience: Minimum of five (5) years' experience in DevOps experience.
Functional Responsibility:
The DevOps Engineer has experience serving as the engineer of complex technology implementations in a product-centric environment. They are comfortable with bridging the gap between legacy development or operations teams and working toward a shared culture and vision. They work tirelessly to arm developers with the best tools and ensuring system uptime and performance.
Primarily responsible for:

- Deploying and configuring services using infrastructure as a service providers (e.g., Amazon Web Services, Microsoft Azure, Google Compute Engine, RackSpace/OpenStack)
- Configuring and managing Linux-based servers to serve a dynamic website
- Debugging cluster-based computing architectures
- Using scripting or basic programming skills to solve problems
- Installation and management of open source monitoring tools
- Configuration management tools (e.g., Puppet, Chef, Ansible, Salt)
- Architecture for continuous integration and deployment, and continuous monitoring
- Containerization technologies (e.g., LXC, Docker, Rocket)

- Perform the Operations Support and Maintenance on applications of various sizes and complexity.

Minimum Education: A Bachelor's Degree