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

1. REQUISITION NUMBER	PAGE	OF
	1	297

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
NRC-HQ-10-17-A-0008	06/06/2017		NRC-HQ-10-16-R-0005	09/21/2016

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	DOMONIQUE MALONE	301-415-8164	ET

9. ISSUED BY — CODE NRCHQ

US NRC - HQ
ACQUISITION MANAGEMENT DIVISION
MAIL STOP TWFN-5E03
WASHINGTON DC 20555-0001

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: 541519
SIZE STANDARD: 150

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

15. DELIVER TO — CODE

As Indicated On Each Call

16. ADMINISTERED BY — CODE NRCHQ

US NRC - HQ
ACQUISITION MANAGEMENT DIVISION
MAIL STOP TWFN-5E03
WASHINGTON DC 20555-0001

17a. CONTRACTOR/ OFFEROR — CODE 827860300 — FACILITY CODE

SYNAPTEK CORPORATION
ATTN KAMRAN JINNAH
1818 LIBRARY STREET
SUITE 500
RESTON VA 20190

TELEPHONE NO. 7036274677

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

18a. PAYMENT WILL BE MADE BY — CODE

As Indicated On Each Call

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 #: GS-35F-0018Y Procurement Title: GLobal INfrastructure and Development Acquisition (GLINDA) NRC RFQ Number: NRC-HQ-10-16-R-0005 GSA e-Buy Number: RFQ1078832 Period of Performance: 06/06/2017 to 09/29/2019 *(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: REF. _____ 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	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
	[redacted]

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		JOSEPH L. WIDDUP	06/06/2017

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

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

United States
Nuclear Regulatory Commission

GLobal INfrastructure and Development Acquisition (GLINDA) Blanket Purchase Agreement (BPA)

Contents

SECTION B: SERVICES AND PRICING

B.1 Services

The Contractor shall provide business services to the NRC in accordance with the scope of work provided in Section C.

The Contractor shall provide all management, supervision, and labor, and shall plan, schedule, coordinate, and assure effective performance, for all requirements as outlined in Section C.

B.2 Order Type

This procurement will be a multiple award Blanket Purchase Agreement (BPA) under the General Services Administration's (GSA) Multiple Award Schedule (MAS) 70. The NRC intends to award at least two (2) BPAs including at least one award to a small business.

The BPA will enable NRC programs to compete discrete requirements in the form of BPA Calls, amongst the BPA award holders. BPA Calls may be competed on a Time-and-Materials (T&M), Labor-Hour (L-H), or Firm-Fixed-Price (FFP) basis, or a hybrid of these contract types. Specific details will be further provided at the BPA Call level, which may include such variations as including timesheets with invoicing for T&M packages.

B.3 Price Schedule

B.3.1 Labor Rates

The Contractor shall provide their GSA Schedule labor categories mapped as fully loaded rates to the NRC BPA Labor Categories. NRC is requesting an additional discount from the GSA Schedule Contract rates for the BPA. See Attachment 1.

B.3.2 BPA Call Pricing

Following the establishment of the multi-award BPAs, the NRC intends to issue individual Call Orders to awardees with more specifically described needs as they arise. BPA Calls will serve as a principle element in the evaluation of the Contractor's performance under the BPA and the NRC will articulate essential deliverables and work products at the time of issuance. Through this method, the Agency and Contractors will be able to work more collaboratively and responsively in a dynamic operating environment.

Following receipt of an issued BPA Call, the Contractor shall provide any assistance, skills, and expertise necessary to successfully complete performance as defined in that work package. All issued BPA Calls will be within the scope of the service areas described in the BPA scope of work.

The BPA Calls will, at a minimum:

- Detail the work to be performed by the Contractor;
- Specify essential deliverables and work products;
- Indicate whether the work mode is to be collaborative or independent;
- Set performance standards; and

- Set schedule objectives.

Labor rates referenced in paragraph B.3.1 shall be used by the Contractor as the maximum allowable ceiling on labor rates when submitting price quotes in response to BPA Call requests issued under this BPA.

Contractors may propose, or the NRC at its discretion may seek or negotiate, further price reductions on an individual basis as BPA Calls are issued.

Ordering instructions for BPA Calls are provided in section B.3.4.

The period of performance of an issued BPA Call may extend past the BPA expiration date for a period not to exceed one (1) year in total and within the limitations of GSA Schedule.

B.3.3 Travel/ Other Direct Costs (ODCs)

Travel will be reimbursed in accordance with FAR 31.205-46, Travel Costs, and NRC Clause 2052.215-77, Travel Approvals and Reimbursement, and the General Service Administration's Federal Travel Regulations (FTR), currently viewable at: http://www.gsa.gov/portal/content/104790.

B.3.4 Ordering Instructions for BPA Calls

The NRC will place orders with BPA holders in accordance with FAR 8.405-3(c)(2).

B.4 BPA Estimated Value

The combined estimated value of these BPAs (i.e., maximum of all BPA Calls for all BPA Holders) is $679,000,000 over 6 years. There will be no minimum guarantee or maximum order limit with these BPAs. The NRC is under no obligation to issue BPA Calls for every area within the scope of work, Section C.

B.5 Funding

No funding shall be obligated upon establishment of the BPAs. Funding for services provided will be obligated at the BPA Call level.

B.6 Incremental Funding on Time-and-Material and Labor-Hour BPA Calls

Funding may be added to T&M and L-H BPA Calls by the execution of modifications to the BPA Call, up to the BPA Call ceiling amount for the BPA Call's performance period. Residual funding at the end of a BPA Call's performance period may be de-obligated through a modification; inclusion of this funding in the following performance period of the BPA Calls is subject to budget approval based on appropriations and fiscal constraints.

B.7 Emergency Situations

Emergency situations and contingency operations at the NRC may require the Contractor to operate at times not considered normal operating hours, as directed by the CO. This normally involves utility outages, weather driven contingencies, or any work involving support for significant technical related services critical to the NRC mission.

B.8 National Security

On occasion, services may be required to support an activation or exercise of contingency plans outside the normal operating hours. Emergencies (i.e. accident and rescue operations, civil disturbances, terrorist attacks, and natural disasters) may necessitate the Contractor to provide increased or reduced support as determined by the CO. If deemed necessary, the NRC may negotiate an equitable adjustment with the Contractor for the cost of these emergency requirements.

SECTION C: DESCRIPTION/ SPECIFICATIONS

C.1 Agency Introduction

The U.S. Nuclear Regulatory Commission (NRC) was created as an independent Agency by Congress in 1974 to enable the nation to safely use radioactive materials for beneficial civilian purposes while protecting people and the environment. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements.

The NRC's headquarters are located in Rockville, Maryland. Approximately eighty percent (80%) of the Agency Staff and the Commission are located at headquarters. Additionally, the Agency has major locations (Regional Offices) in King of Prussia, Pennsylvania (Region I); Atlanta, Georgia (Region II); Lisle, Illinois (Region III); Arlington, Texas (Region IV); and a Technical Training Center (TTC) in Chattanooga, Tennessee. Regional Offices and the TTC vary in size, however on average each location supports 200-300 staff. Finally, Resident Inspectors and other personnel are located in approximately 60 offices throughout the United States and the average staffing at each office is 2-4 personnel.

The NRC Office of the Chief Information Officer (OCIO) manages information technology (IT) and Information Management (IM) resources throughout NRC and is the principal advisor to the NRC community regarding all IT/IM services that bridge technology to the agency's business strategies. OCIO is responsible for delivering the following types of IT/IM services to the agency:

- Develops and presents the strategic IT/IM direction and the major IT/IM investments in support of the critical business processes to NRC senior executives.
- Ensures that the NRC strategy for using state-of-the-art technology systems aligns with current and future business strategy.
- Manages, evaluates, promotes and tracks all investments within the FITARA guidelines.
- Manages and directs all cybersecurity policy and activities in support of the Agency's mission.
- Manages the purchase, maintenance, and support of all NRC furnished IT equipment.
- Coordinates with supporting contractors on the development of architecture, support, and IT hardware.
- Manages the design, development, and implementation of all software applications.
- Manages the Agency data center (currently located at the Headquarters) and supports subsidiary data centers located in each of the Regional Offices and the training facility.
- Manages the Agency enterprise data and voice networks.
- Manages the support requirements associated with Agency developed and fielded applications and related technologies.

As the NRC continues to improve services to its customers and increase operational efficiency, the OCIO must continually evaluate all IT/IM Agency services, capabilities, functions, systems and support to ensure that the cost to value benefit to the Agency remains viable. Additionally, OCIO is responsible for ensuring that any efficiencies gained remain supportive of the Agency's

overall health and safety mission. NRC intends to use the BPA Calls under this BPA to support a transformation of its current cost of IT/IM operations and maintenance support services, with a focus on leveraging alternatives to existing services and approaches for efficiency gains and service improvements.

On a broader level the NRC has recently begun an internal assessment of all Agency-wide capabilities and services under an initiative called Project AIM. This 21st century initiative will evaluate all Agency programs with the goal of realigning both the Agency cost model and the necessity, quality, timeliness and delivery standardization of Agency services. In order to support these goals, OCIO developed the GLobal INfrastructure and Development Acquisition (GLINDA) to procure the required IT/IM support services and solutions.

GLINDA represents a central component of this effort since it addresses all of the infrastructure and program support for IT/IM within the Agency. NRC is seeking contractor support under this BPA to assist with the realignment of IT/IM functions and services so that they can be reshaped, rebalanced, modernized, and structured to provide greater product innovation to the Agency workforce.

C.2 Background

C.2.1 Contract History

The majority of services envisioned under GLINDA are currently provided through two (2) contracts described in more detail below.

The NRC's Information Technology Infrastructure and Support Services (ITISS) contract is a single award Indefinite Delivery/Indefinite Quantity (IDIQ) contract which provides agency-wide IT/IM infrastructure and support services.

- Contract Type: Indefinite Delivery Indefinite Quantity (IDIQ)
- Contract Number: NRC-33-11-325
- Number of Task Orders: 3, only 1 active
- Incumbent: Dell Services Federal Group
- Period of Performance: 2/18/2011 - 5/17/2017

Although the number of previous and current Task Orders under this vehicle are few, this contract encompasses a substantial number of services critical to the agency's ongoing IT operational capability.

The NRC's Maintenance, Operation, and Modernization (MOM) Functional Area 2 (FA2) contracts are multiple award IDIQ contracts which provide agency-wide maintenance and operational IT/IM support services for current and future NRC automated computer systems.

- Contract Type: Indefinite Delivery Indefinite Quantity (IDIQ)
- Contract Numbers: NRC-HQ-11-C-33-0059 and NRC-HQ-11-C-33-0060
- Number of Task Orders: 37
- Incumbents: CGI Federal and Lockheed Martin

- Period of Performance: 9/26/2011 - 9/25/2021

The current combined ceilings of ITISS and MOM FA2 is $432,075,339.

In addition to the two contracts mentioned above, the NRC has various other contracts which may expire during the period of performance of GLINDA and fit under the scope of GLINDA. At NRC's discretion, some of these requirements may be procured under GLINDA as a BPA Call if the NRC determines that the GLINDA BPA is an appropriate vehicle for these services.

C.2.2 NRC's Current Security Environment

The NRC follows FISMA and NIST guidelines (see the Section J, Attachment for CSO IT Security Requirements Document) related to IT/IM security. All hardware and software must be tested and/or FedRAMP Compliant prior to use within any NRC or Licensee facility. All systems must be established within appropriate system boundaries and an Authority to Operate (ATO) must be granted prior to production.

The NRC utilizes a tiered approval process to approve changes to its environment. The top level of the process (major system upgrades; ATO; etc.) requires the approval of senior Agency management and the Chief Information Officer. The second level requires the approval of the Chief Information Officer and the Director, Information Security Directorate. The third tier of approval focuses primarily on patches, day-to-day changes and is approved by the Deputy Chief Information Officer and the Deputy Director, Information Security Directorate.

Major changes typically require full security tests, however, that requirement will vary based upon the type of change and system. All systems receive an ATO according to schedule and the Agency has implemented U.S. Department of Homeland Security's (DHS) Continuous Monitoring Program.

Contractors are responsible for building systems from a common image and ensuring that the image is compliant with the latest guidelines. Older images are expected to be brought up to the new standard on an annual basis. Contractors are also responsible for self-identifying and entering into the agency's database all Plan of Action and Milestones (POA&M) findings and addressing POA&Ms unless there are additional costs or architecture/solution impacts. In those cases, contractors are required to coordinate with the NRC, and when applicable contractors in other BPA Call areas, to ensure that the solution is appropriate, within appropriate cost constraints, and will not have an adverse impact upon other BPA Calls. In all cases, contractors shall maintain a common schedule for all patches, upgrades and POA&M resolutions so that those activities can be scheduled for test and evaluation prior to implementation.

Contractors also maintain all Continuity of Operations Planning (COOP) and Disaster Recovery documentation and participate in NRC tests as appropriate and as scheduled.

C.3 Purpose

The purpose of the BPA is to enable the Agency access to contractors that can:

- Provide enterprise-level IT operational, development, and integration support services.
- Identify, plan, and implement innovative service approaches that increase efficiency or improve the effectiveness of the Agency mission.
- Implement and maintain a comprehensive Configuration Management (CM) strategy.
- Implement a successful IT infrastructure Library (ITIL) oriented operational and support

environment and executing associated processes.

The BPA is expected to provide the NRC with a wide range of IT infrastructure and application maintenance and operations services that are included, but not limited to, the solutions currently provided by the current NRC ITISS and the MOM FA2 contracts. The services under the BPA will support OCIO's goal of ensuring business processes follow uniform practices and standardized governance procedures across the enterprise.

C.4 Objectives

The objective of this BPA is to support an enterprise approach to business practices at the NRC and may be used to support all program areas and location sites of the NRC. Additionally, this BPA shall strive to accomplish the following objectives:

- Establish secure, highly reliable, enterprise-wide, standardized IT/IM infrastructure services and application development and support solutions;
- Support continuous hardware and software maintenance and operational support for NRC's current and future enterprise application systems;
- Collaborate and coordinate with service providers in other task areas where appropriate;
- Increase flexibility, agility, and innovation in IT/IM service delivery;
- Deliver reliable, high quality, and cost effective IT/IM solutions;
- Improve and enhance the delivery of services through data driven service management;
- Enhance the capability of the NRC and each of the service areas through the incorporation of commodity and cloud services;
- Innovate in the use of information technology to increase the productivity of Agency users, improve the Agency's security posture, and reduce the cost of services provided while maintaining customer service expectations.

OCIO also requires the Contractor to adhere to Federal and NRC standards and policies in force at the time services are provided, including but not limited to:

- NRC Management Directives (MD)
- Enterprise Architecture (EA) Program Policy, which includes:
    - Systems architecture policies and standards
    - Systems engineering policies and standards
- Enterprise Systems Development Life Cycle (SDLC)
- Enterprise Requirements Management Process
- Project management policies and guidelines
- Cybersecurity policies and standards
- Physical security policies and standards

This list will evolve over the life of the BPA. It shall be the Contractors' responsibility to remain current on all relevant policies, standards, and guidelines which impact services rendered under

this BPA. The Contractors shall also comply with updated versions, when applicable. It is also expected that Contractors will consider the Agency's goals and objectives, which include identifying and implementing innovative improvements, when planning and implementing solutions.

C.5 Scope of Work

The BPA will utilize a variety of professional services defined in GSA Schedule 70 SIN 132-51 and 132-3. Individual BPA Calls under this BPA will primarily encompass SIN 132-51 but may also utilize other SINs as applicable to provide a total solution at the BPA Call level in order to address the Agency's service requirements (Service Areas).

Additionally the Contractor shall support one or more phases of support, including transition, operation, and/or over-arching management (Support Phases).

C.5.1 Service Areas

From an operational support perspective, the NRC envisions transitioning from a single outsource management contract (the current ITISS contract) to a hybrid approach based upon four (4) broad service areas:

- **Seat Services** – User-oriented hardware, software, mobile desktop, help desk, security, day-to-day user support, management/maintenance, etc.
- **Network Services** – Architecture for the Agency's network(s), telephony, conferencing, Networx circuit management, local area network management, hardware, software, maintenance, Network Operations Center, etc.
- **Data Center/Cloud Services** – Public cloud services, local data center(s), server virtualization, server images, security, performance, availability, failover to alternate site, failover within the site, standard development and test environments, etc.
- **Application Operations and Maintenance (O&M) Services** – Ongoing support for commercial and custom applications and platforms, administration, configuration, patching, user coordination, etc.

In order to provide an accurate understanding of the current state at the NRC, this SOW provides general details related to existing technologies and corresponding management practices. While this level of detail may appear to dictate specific technologies or solutions, the NRC is seeking innovative technologies, solutions, and/or practices that would increase efficiencies, reduce costs, and/or improve service levels.

The following service area summaries describe the general nature of the support envisioned and examples of potential opportunities to leverage innovative approaches to support the desired cost and service transformation the Agency is seeking. Contractors should not consider the examples mandating (except where indicated) nor limiting the types of service choices that the NRC would consider under this BPA.

The NRC reserves the right to obtain support outside of this BPA if it is more advantageous to the Agency to do so.

C.5.1.1 Seat Services

C.5.1.1.1 Current Environment

In the current NRC environment, most users rely upon a dedicated desktop system within the NRC's offices to support their roles. A smaller number of users use laptop systems in lieu of desktop systems. The Agency's desktops and laptops currently run the Microsoft (MS) Windows 7 operating system and MS Office suite in addition to a range of other custom and commercial software applications. Additionally, many users rely upon NRC-furnished or 'Bring Your Own Device' (BYOD) mobile devices for mobile access to certain NRC resources. There are also a limited number of stand-alone or unique devices within the Agency, however the majority of those devices are located at the Agency headquarters.

User systems use a common image that meets current Agency security specifications and all images contain the same basic software and version of MS Office products. All images have been tested and approved for use. While all devices use a common image, individual systems may be enhanced by additional custom or commercial applications based upon the need of the end-user.

Users are currently supported by an Agency Help Desk that services all Agency locations. The help desk functions 24x7x365 with call back after the prime business hours of 7 AM to 9 PM Monday through Friday. The help desk utilizes an ITIL-based foundation to manage service activities. It records all requests for service in a Contractor-provided and supported Remedy® service management system.

Additionally, the NRC currently utilizes Citrix to provide remote access in support of Agency requirements. The remote access has been configured to support approximately one-third (1/3) of the active user population in simultaneous use. Some of the Regional Offices have alternative systems that provide remote or mobile desktop capability.

The incumbent Contractor supplies all of the seat-related hardware, software, and corresponding maintenance and support under the current seat management approach as an inclusive per-user cost. NRC anticipates changes to this approach including the manner in which hardware, software, and services are bundled and procured.

C.5.1.1.2 Required Services

The Contractor may be required to provide a comprehensive set of Seat related services including but not limited to:

- Seat related equipment and software licenses
- Print/output management services
- Mail, file, and print management services
- Hardware and software provisioning/de-provisioning and relocation
- Seat support including help desk support and break/fix services supported by required problem diagnosis, resolution, and escalation management
- Hardware and software maintenance, patching, updates, and upgrades

These services may be required at all NRC locations including Resident Inspector sites.

C.5.1.1.3 Forecasted Initiatives

As a component of its delivery, the Contractor shall recommend competent approaches for innovation and transformation focused on improving efficiency and reducing costs while maintaining the required levels of service to the Agency. The NRC may require recommendations to be provided in multiple ways, ranging from informal advisory to more formal research studies. The Contractor shall be able to provide recommendations both informally as well as using more formal approaches.

Proactive Help Desk and Actionable Service Catalog – The Contractor shall work with the NRC to introduce and support help desk capabilities that provide 'how to,' 'self-help', and 'self- service' support options to users. The Contractor shall review commercially available capabilities and services and propose a solution based upon a capability that is available. End users should be able to contact the help desk and be routed to proactive help for all MS Office and other common commercially available applications.

Transition to Office 365 for Productivity Applications – The NRC envisions migrating its current MS Office licensing and management approach to Office 365. The Contractor responsible for this performance shall also coordinate with the Network Contractor(s) to ensure that the network was properly designed and sufficient to support the use of Office 365. Additionally, NRC is considering the consolidation of its existing SharePoint, Skype for Business, and network storage within the same environment and is seeking to maximize the number of features and functions available within the service offering. Ultimately, the final selection of individual services will be based upon cost and value. Contractors shall consider MS Exchange and MS Outlook as mandatory elements of this approach. The Contractor shall complete the aforementioned activities using Office 365 licenses provided by the NRC.

Reengineer the Desktop - The NRC currently utilizes a single-source desktop environment with physical desktops and laptops. The majority (99%) of NRC's desktop and laptop systems are from a single manufacturer and refreshed every three (3) years on a rolling basis of one-third each year. Related to its current desktop/laptop hardware, the NRC would like to consider less costly acquisition and/or maintenance solutions and/or hardware solutions where appropriate while maintaining a consistent level of support for Agency laptops. The Agency is open to a variety of options including the replacement of the desktop with a terminal based mobile desktop environment or other alternatives. The Agency currently supports several different mobile desktop environments and would like to expand the capability. However, the Agency is open to alternatives other than those already in place. Regardless of the architecture recommended, the Agency is focused on performance as perceived by the end user. Consequently, the recommendation and selection of an alternative desktop environment will need to substantiate the ability of the solution to support appropriate levels of performance.

Mobile Service Offerings – The Contractor may also be responsible for developing and expanding the Agency's mobility solutions. The Agency currently utilizes MaaS360 as its mobility platform and it anticipates supporting that platform for the near future. The platform supports both NRC Furnished Equipment (GFE) and personal devices (smartphones and tablets). The Contractor shall support the current platform and provide recommendations for future features and functions under that platform. In addition, the Contractor shall establish and operate a mobility service desk as part of its support to this area. The Contractor's mobility service desk shall integrate with other Agency Help Desk operations so that users can contact a single Help Desk number or e-mail address to request support services. The NRC

does not anticipate acquiring device and related service plans under this BPA.

The Contractor shall support efforts in collaboration with other agency stakeholders to identify and work with the Agency to develop an application catalog that can be supported under this platform. As the service area matures, the NRC anticipates changes in platform and architecture. The NRC will require Contractor support to follow the growth and evolution of its mobility environment accordingly.

Printer Consolidation and Management – Currently, file and printer servers exist along with dedicated MS Exchange servers at the Headquarters, the four (4) Regional Headquarters, and the TTC. These services were established to support improved performance at local levels and to provide continuing operation during periods of network outage.

A consolidation effort is currently underway to replace agency-wide print/copy equipment with multi-functional printers and multi-functional devices. This effort shall gradually and incrementally replace the legacy fleet in a phased approach, as current contracts at HQ and regional locations expire. The agency may require the GLINDA vendor with responsibility for print to assume management services, including all associated leases, maintenance, and supplies (except for paper). Additionally, the agency may require the contractor to provide administration, central reporting, and comprehensive monitoring of devices, including both vendor-provided and GFE. The specifications relating to the replacement of devices, maintenance, and management of services shall be specified at the individual delivery/task order levels.

C.5.1.2 Network

C.5.1.2.1 Current Environment

Currently the Agency's network is best described as a tree structure with the NRC's Rockville Headquarters as the apex of the structure (the majority of circuits terminate in Rockville, one of the Regional Offices, or the TTC). All internet circuits have been procured through GSA's Networx contract and will be covered along with their supporting systems under the DHS continuous monitoring contract at the time of contract execution.

From a telephony perspective, the NRC currently maintains multiple phone system configurations. Approximately 80% of Agency personnel are covered by PBX-based phone systems and environments. The remaining 20% are covered by Voice over Internet Protocol (VoIP) technologies and systems. The NRC also possesses and supports a number of video conferencing options. For major business conferences the Agency utilizes Tandberg systems, however, the Agency also supports Skype for Business and a number of other Web-based technologies.

Additionally, the NRC maintains a limited wireless profile. The NRC Headquarters has a visitor wireless network that is not connected to the corporate network and is available primarily in the Two White Flint North cafeteria. This network is publically accessible with very limited security. The Agency also maintains a second wireless installation at Region II which is connected to the corporate network. This is fully certified and operates under standard Agency network security protocols.

C.5.1.2.2 Required Services

The Contractor shall provide a comprehensive set of network related services including but not

limited to:

- Ongoing operational management of the Agency's voice and data networks including diagnostic support, maintenance (hardware and software), escalation, and reporting;
- Interface with Networx and other service providers to identify, isolate, and resolve outages in other service areas;
- Serve as the network and telephony architect the Agency network and telephony systems;
- Serve as the Agency's agent to coordinate with all service providers and plant licensees related to such services;
- Operator and teleconferencing management services.

The Network service area necessitates a significant level of coordination, collaboration, and interface with all of the BPA Calls and a number of external service providers.

C.5.1.2.3 Forecasted Initiatives

As a component of its delivery, the Contractor shall recommend competent approaches for innovation and transformation focused on improving efficiency and reducing costs while maintaining the required levels of service to the Agency. The NRC may require recommendations to be provided in multiple ways, ranging from informal advisory to more formal research studies. The Contractor shall be able to provide recommendations both informally as well as using more formal approaches.

Network Architectural Services (data and voice) - Key to the NRC's broader IT/IM goals will be the re-architecture of the NRC network (telephone and data). The success of the Agency's initiatives associated with cloud, seat management, application development, and systems operations is expected to rely on a network re-architecture to support a new style of computing. Additionally, since the network will become a single point-of-failure for many Agency sites, it is critical that the re-architecture examine alternatives and redundancies that will supply network services regardless of the loss of a single location, circuit, or office. For example, in follow-on task orders, the vendor will be asked to provide a plan, with options, and the cost with timeline to complete each phase of re-architecting and implementing network upgrades at the local building level, the connections between all buildings, regional buildings and certain licensee facilities.

Replace Existing Phone Operators and Conferencing Solution – Currently the NRC receives phone operator services during its core business hours. These same personnel also assign and register conference call requests. The NRC will evaluate the possibility of replacing these services with an automated call director solution that provides voice call routing to individuals and offices within the Agency. Contractor support may evaluate alternatives and present those alternatives to the NRC. Once the alternatives are presented, NRC may ask the Contractor to execute either all or part of the desired alternative, or NRC may determine if another execution approach should be taken. Additionally, the Agency is seeking solutions that would provide individual conference numbers that can be assigned to individual employees and projects.

Implement Recommended Web Performance Network –The Contractor may provide services for a network redesign to support adequate performance of desktop access to the forecasted web- based services across all NRC locations and offices. Once fully approved inclusive of required security approvals, the Contractor will implement the redesign according to the

approved schedule and architecture.

Re-architect NRC Voice Systems – The NRC seeks to simplify and improve telephony services throughout the Agency and at each NRC location. The Contractor may review the current state of telephony throughout the Agency; determine if alternative approaches (e.g., eliminate PBX's, VOIP, etc.) might be appropriate; define an appropriate strategy; and develop a business case for the Agency that would help reduce the cost of providing telephony services. Once the business case is presented, NRC may ask the Contractor to execute either all or part of the business case, or NRC may determine if another execution approach should be taken.

Wireless Systems Architecture – The NRC intends to make greater use of wireless technologies to service all of its locations. The Contractor will work with NRC to develop a comprehensive wireless plan. All technologies will be required to meet all wireless technology regulations and policies and be able to receive an ATO. The Contractor shall also work with the building management staff and NRC's staff to identify cost saving network options that will support the dynamic utilization and reconfiguration of space within the Headquarters and other NRC buildings. Once the wireless plan is presented, NRC may ask the Contractor to execute either all or part of the plan, or NRC may determine if another execution approach should be taken.

Re-engineer Video Conferencing – The Contractor may evaluate the current state of the video conferencing options available and recommend an architecture and consolidation approach that provides business ready video conferencing across the Agency. Once evaluated and approved by the NRC the Contractor may implement all or part of this solution according to the approved schedule, or NRC may determine if another execution approach should be taken.

C.5.1.3 Data Center/Cloud Services/ Security Operations

C.5.1.3.1 Current Environment

Currently, the Agency provides centralized server and storage services from seven (7) locations, two (2) data centers within the Headquarters complex, and five (5) additional data centers, one at each of the Regional Offices and the TTC. Within the headquarters environment, the majority of systems are hosted within VMWare-based virtualized environments using Contractor-provided and owned hardware and software. However, some systems, including the majority of those in the Regional Offices and the TTC rely on dedicated physical environments.

The primary operating system platform across the Agency is the MS Windows Server platform, however, the Agency also utilizes a limited number of Linux, HPUX, Solaris, and AIX platforms to support specific mission requirements.

Approximately 20% of the Agency's systems are supported through a disaster recovery environment located in Region IV and all systems have existing COOP plans. Additionally, the Agency's financial systems and several other applications are hosted external to the Agency data centers.

The Nuclear Regulatory Commission (NRC) Security Operations Center (SOC) monitors, detects, analyzes, mitigates, and responds to cyber threats and adversarial activity on the NRC Enterprise. The analytical methodology required involves a combination of direct monitoring

and response from the NRC SOC and coordinated activity with system administrators, system ISSO's, and other NRC Offices including regional locations. The NRC SOC has primary responsibility for monitoring and responding to security events and incidents detected on the agency's network and information assets as well as for administration and operation of IT security systems. Direction and coordination are achieved through a shared NRC incident tracking system and other means of coordination and communication with agency staff. Requirements include maintaining all current services at the NRC SOC during transition from the incumbent Contractor and providing core operations and related support services to achieve the goals of the NRC SOC. Core services include task order management, network monitoring and security event analysis, email security monitoring analysis, computer security incident response and management, vulnerability assessment, security engineering and architecture, cyber intelligence analysis and sharing, intrusion analysis, and continuity of operations for SOC services. Additionally, the Contractor is required to provide services throughout the NRC to remediate security breaches, seek out and thwart Advanced Persistent Threat (APT) attacks against the agency, and act as central coordination body for Incident Response and Assessment of the NRC infrastructure.

C.5.1.3.2 Required Services

The Contractor may provide a comprehensive set of data center/cloud related services including but not limited to:

- Server, storage, and related hardware and software including support for virtual environment hosting;
- Resource provisioning and de-provisioning;
- Resource performance management and optimization;
- Instance and image management including monitoring, diagnostics, troubleshooting, repair and replacement services, patching, and other ongoing support services;
- Asset and configuration management;
- Data center facility management services including rack, cabling, and environmental controls support.
- Security operations support described further within this section

Although the NRC is currently planning to leverage public cloud services as part of a larger scale data center re-architecture, the Agency believes that current security and/or investment limitations may inhibit its ability to move a significant portion of its existing systems to the cloud in the near term. Consequently, BPA Call(s) associated with this Service Area will require the incoming provider to support the existing, or an alternative, data center for those segments of the NRC's business that cannot be readily migrated to public cloud infrastructure.

The NRC also envisions that there will be a continual presence within the existing NRC headquarters data center and the Contractor shall manage and maintain all systems that reside within the data center according to the policies, processes and security protocols present in the

BPA Call. The NRC also expects that the majority of the environments that remain in the data center will be rated FISMA High. Consequently, as FedRAMP alternatives come to market to support FISMA High the NRC anticipates that the Contractor may evaluate those requirements and recommend appropriate alternative cloud-based service solutions. The NRC COR will work with the Contractor to evaluate recommendations and to determine the priority for migration. The NRC reserves the right to obtain support outside of this BPA if it is more advantageous to the Agency to do so.

All personnel performing work under this contract shall have pertinent technical and professional experience by discipline and technical area. Experience in these disciplines and technical areas must be related to the design, analysis, engineering, operation, maintenance, and security of an Enterprise network and the duties of a Security Operation Center including the following areas:

- Access Control and Authorization
- Advanced Threat Protection
- Application Security
- Continuous Diagnostics and Mitigation
- Data Loss Prevention
- Encryption
- Firewall Management
- Incident Response
- Intrusion Prevention and Detection
- Policy Enforcement
- Protocol Analysis
- Remote Access
- Vulnerability Assessment
- Web-filtering

Monitoring and analysis shall consist of security event detection, categorization, prioritization and reporting. Event categorization shall consist of analysis of the incoming data flow from security devices and searching data for indications of anomalous events from sources such as Intrusion Prevention Systems (IPS), web proxies, endpoint protection software, mail gateways, network access control systems, security information and event management systems, authentication gateways, VPN gateways, and firewalls.

Another key requirement for the SOC is identification of technical vulnerabilities in commercially available hardware, firmware and software products used by the NRC Enterprise and those in customized commercial products supporting standard NRC applications. The NRC SOC is responsible for scanning, identifying, and assessing vulnerabilities and configuration compliance for all systems attached to the Infrastructure and ensuring that data collected related to hardware inventory, software inventory, vulnerability management, and configuration compliance are made available for analysis and reporting to meet continuous diagnostics and mitigation requirements.

The SOC also actively participates in incident assessment and response activities and work with NRC Offices, contractors, and other organizations within and outside of NRC to assess, respond, and recover from any NRC computer security incident. Requirements include analysis of all of the artifacts from an intrusion to establish a timeline, determining the origin of the intrusion, identifying the actions taken to make the intrusion successful, determining the motivation (what the actor was after), developing a mitigation plan, and recovery from the incident.

The NRC SOC Contractor will work with the Security Operations and Systems Engineering (SOSEB) Branch Chief, the NRC SOC Operational Leads, and other NRC Government advisors to develop, pilot, refine, deploy, and execute a Performance and Investment Metrics Program for the NRC SOC, with all proposed metrics approved by the SOSEB Branch Chief prior to commencement of data collection. The Contractor's Performance and Investment Metrics Program shall routinely measure, analyze, and report weekly refined qualitative and quantitative measures and metrics on the impact of NRC cyber security incidents, the degree and effectiveness of computer network defense coverage across the NRC Infrastructure, and the effectiveness of the Contractor's implementation of the NRC intrusion defense chain (IDC) methodology in the NRC SOC. The NRC SOC Contractor's Performance and Investment Metrics Program shall include analysis of cybersecurity events, incidents, and incident response metrics and trends, with the goal of deriving predictive metrics, anticipating emerging and evolving threats and implementing countermeasures and mitigations. The Contractor's performance and investment metrics briefings and reports shall analyze trends in the number and level of threats of concern to NRC networks and systems as identified by external Government Agency sources.

C.5.1.3.3 Forecasted Initiatives

As a component of its delivery, the Contractor shall recommend competent approaches for innovation and transformation focused on improving efficiency and reducing costs while maintaining the required levels of service to the Agency. The Contractor shall provide recommendations in multiple ways, ranging from informal advisory to more formal research studies. The Contractor shall be able to provide recommendations both informally as well as using more formal approaches.

Some initiatives may be very complex and/or require substantial investment complete. As a result, In such a situation, the awardee(s) may choose to compete for such opportunities as long as a conflict of interest does not exist.

Cloud Migration – From a data center services perspective, the NRC's goal is to transition from a classic outsourced data center environment to a public cloud provider environment. Currently the NRC operates an on-premises virtual server environment that supports 80% of the Agency's applications. The NRC envisions additional systems currently supported by dedicated physical servers within the Regions, TTC, and other locations can readily be virtualized as well. The foundation technology is currently VMware's Hypervisor, however, the Agency is open to other alternatives. Additionally, the Agency is interested in cloud-based services beyond Infrastructure as a Service (IaaS), to include Platform as a Service (PaaS) options, where appropriate. Before any cloud migration activities begin, the NRC may elect to have additional studies conducted on this topic. If conducted, such studies may be performed independent of this BPA.

As part of the migration planning activities, the Contractor may be asked to develop a solution

architecture and implementation plan for review and concurrence by the NRC. Once approved, using IaaS and/or PaaS that is procured outside of GLINDA, the Contractor shall implement the plan according to the agreed upon schedule. The Contractor shall provide a FedRAMP approved environment at the appropriate FISMA level and the cloud provider shall offer provisioning and Cloud management portals sufficient to meet the day-to-day management needs of the Agency. Further, since all of NRC's locations will be targeted for consolidation into the Cloud, the NRC will look to the Contractor to identify and support availability and failover mechanisms, as well as broader disaster recovery capabilities within the cloud architecture.

Development, Test,* Configuration Management *and automated Deployment - The NRC also looks to the data center/cloud services and support Contractor to work with the Agency to develop and support a compatible development and test environment sufficient to support the Agency's application development and testing needs. The NRC seeks to transition to a more robust and controlled configuration management approach inclusive of the development, test, and production migration environments.

It is expected that solutions will enable high quality pre-production configuration control thorough security testing (in conjunction with the NRC identified security test provider), section 508 testing, functional testing, regression testing, performance testing, user acceptance testing, and other testing (if identified and required in the BPA Call) prior to production release. Once tested, the Contractor will support updates to the configuration management database to reflect the new version and maintain a current prior and potentially upcoming version in the database. Finally, the contractor will support the application of professional grade software migration techniques and tools to move the versions into production.

Robust Data Center/Cloud Failover/Disaster Recovery – The NRC seeks solutions that will support the local failover of critical systems located at its data center and, after migration to the cloud, failover of such systems located in the cloud environment. Further, the Contractor will develop, with support from the NRC, a robust disaster recovery plan that will provide a high level of continuity and rapid return to service should data center services be lost in either the local NRC data center or public cloud environments.

Finally, since application performance may be impacted by the network and other factors, the Contractor will work with the other Contractors and the NRC, as needed, to support the evaluation and development of recommended actions to improve performance. Once the recommendations are made, the NRC may ask the Contractor to either execute part or all of the recommendation, or the NRC may determine that another execution approach should be taken. Included within this service area will also be, but not limited to, performance management, hardware and software upgrades, patch management, support for NRC disaster recovery and COOP testing, and support for NRC software testing and implementation.

C.5.1.4 Application Operations and Maintenance (O&M) Services

C.5.1.4.1 Current Environment

The NRC utilizes numerous commercial and custom information systems to support its mission. OCIO coordinates the Agency's IT business system development and operations activities to ensure that applications are effectively developed and maintained to support current and emerging agency business needs.

Ongoing maintenance and operational support for the majority of the Agency's information

systems is provided by Contractors under individual task orders that specify the required services to address performance, analytical, planning, development, implementation, evaluation, or support needs and challenges.

Maintenance and support activities are carried out within the Agency's common operating processes for configuration and engineering change control. These processes are further supported by the Agency's Architecture Review Board which reviews and approves requests for changes and updates to the NRC's Production Operating Environment (POE). The Agency's current configuration management system is the IBM Rational platform and related IBM Rational tools.

C.5.1.4.2 Required Services

To support effective maintenance and support of legacy systems, the Contractor may provide a comprehensive range of technical, analytical and project management services including, but not limited to:

- Maintenance and support for legacy systems;
- Operations of legacy systems;
- Cross-application, platform, program and project coordination.

Each of the required services is described in more detail in the following sub-sections. **T**he use of agile project management approaches where appropriate in accomplishing the work that arises from this service area is encouraged.

C.5.1.4.2.1 Maintenance and Support for Legacy Systems

The Contractor shall modify and/or correct application system code and/or data to make the application system perform as intended in support of the business process for which the code was written. These modifications may include those made to programs, scripts, job control languages, and data. The Contractor shall also support analysis of conditions and outputs to identify root causes of problems and define methods for correction by troubleshooting, executing backups, restoring archives, and housekeeping.

Contractor maintenance support may take the form of preventive, corrective, adaptive, or perfective actions or any combination of these actions:

- Preventive Maintenance – Identify potential future faults and modify the system to mitigate the risk.
- Corrective Maintenance – Identify current system faults and modify the system to fix them.
- Adaptive Maintenance – Modify the system to maintain compliance with changing IT infrastructure, IT security requirements, and technology upgrades.
- Perfective Maintenance – Modify the system to add minor new or improved functionality.

The Contractor shall implement changes to the legacy systems as required to deliver minor enhancements, implement best practices, facilitate user support during and prior to transitional periods of a new release, and/or apply cost effective approaches for facilitating maintenance

activities. The key objectives are:

- Implement best practices for maintenance activities
- Facilitate user support during and prior to and during transitional periods when moving users to a new release of the software with an increased improvement during normal operational periods.
- Apply cost effective approaches for providing all maintenance activities

Requirements – Key requirements may include, but are not limited to:

a. Providing maintenance support for all identified legacy NRC application systems. The Contractor shall ensure perfective maintenance actions are not to be performed while a system is being modernized.

b. Performing configuration management activities as part of all task orders under this work area

c. Use the IBM Rational tools and formal CM processes to manage stable baselines and change requests.

d. Performing maintenance actions using the current production baseline of the application system which is housed in Rational ClearCase or Rational Team Concert Versioned Object Base (VOBs).

e. Work with requirements and design Contractor(s) and the centralized environment support Contractor for any Rational tools used and ensure those tools, as directed in writing by the NRC COR, are integrated into the M&O processes.

f. The NRC COR or designee shall notify the Contractor of maintenance requests using the Rational Jazz or Rational Team Concert CR system and approve the CRs that will be included in each system release using the procedures specified in NRC Management Directive (MD) 2.8.

g. Updating all application system changes in the system and security documentation, including any changes that affect the security controls within the application system, prior to system deployment.

h. Coordinate, through the NRC COR, with the NRC Information Security Directorate (ISD) and Operations Division (OD) on changes relating to security controls.

i. Implementing changes to application systems using only the specific products defined in the application system baseline, unless authorization has been received in writing from the NRC COR (e.g., if the application is coded in Java 1.5, only Java 1.5 will be used in the changes).

j. Ensuring that the introduction of any new product to the application system is consistent with the authorized list of products (i.e., the Technical Reference Model (TRM)) or approved by the NRC Environmental Change Control Board (ECCB) prior to implementation.

k. Adhere to existing (or as modified by NRC) Maintenance, Operations, and Modernization Change Request Process as defined in the Standards for Maintenance and Modernization Attachment.

l. Adhere to documentation support requirements. The NRC Configuration Control Board (CCB) will consist of a Parent CCB board and children CCB, which will be subordinate to the Parent CCB. Parent CCB will review documentation requirements in conjunction with segment architecture to determine documentation needs for legacy systems.

m. Ensure all changes requested, while the legacy system is being modernized are formally approved in writing by the NRC CCB prior to system modification.

n. Ensure open communication and appropriate information transfer with the NRC COR and other Contractors during the period of performance of this acquisition.

C.5.1.4.2.2 Operations of Legacy Systems

The Contractor shall provide support to ensure that software is running properly and that the appropriate data is backed up and restored as needed. The Contractor shall also provide operational support to assist end users by answering their questions, analyzing the problems they are encountering with production systems, recording requests for new functionality, and making/applying fixes.

The Contractor shall also keep systems running, back-up and restore data based on the operations plan and system requirements, manage problems, perform periodic cleanup, fine tune system reconfigurations, monitor systems, and redeploy systems as necessary. Specific Contractor operational support includes but is not limited to, the following:

- Data Support – Perform light manual data entry on ad-hoc basis, interpretation, scanning, and verification of data.
- Report Generation – Produce standard and ad hoc reports.
- Production Support – Perform data transfers, system monitoring, and troubleshooting.
- Test Support – Perform application testing in accordance with testing procedures.
- Plan for Disaster Recovery – Define and update steps for staff to follow to achieve critical system back up and operation in the event of a catastrophic outage.
- Disaster Recovery – Maintain, store, and execute the Disaster Recovery Plan to ensure timely recovery of critical systems.

The Contractor shall perform these and other related activities to ensure the applicable systems remain operational and comply with Agency requirements and leading practices.

The key objective is:

- Implement best practices for operational support activities.

Requirement – Key requirements may include, but are not limited to:

a. Using the IBM Rational tools and formal CM processes to manage stable baselines and change requests

b. Developing/Updating a Support Plan to include: how support will be provided, system contact personnel, defect reporting and enhancement request strategy, Performance Metrics, defect prioritization and resolution time periods, defect escalation criteria, how to deliver fixes into production outside the scope of an official release

c. Developing/Updating an Operations Plan to include how a system will be operated and supported in production

d. Modifying data

e. Performing data interpretation

f. Scanning documents

g. Performing Optical Character Recognition (OCR)

h. Entering data

i. Validating data

j. Report generation

k. Producing standard reports

l. Producing ad-hoc reports

m. Providing production support

n. Initiating schedule program sequences

o. Transferring data between systems through kick-off of electronic processes or inputs of tapes or other physical media

p. Performing system monitoring, troubleshooting, and applying immediate corrective measures to agency production application systems (in some cases on a 24-hour, on-call basis)

q. Planning for disaster recovery

r. Developing/updating a plan of actions in the event of disaster

s. Conducting staff training on the disaster recovery plan

t. Conducting periodic testing of the disaster recovery plan

u. Recovering from disaster

v. Developing/updating disaster recovery plan

w. Executing disaster recovery plan

x. Coordinating through the NRC COR with the NRC ISD and OD on changes relating to security controls.

NRC expects that achieving these objectives will require the Contractor to:

- Establish and maintain a strong understanding of the mission, goals, and objectives of NRC;
- Respond efficiently and effectively to a diverse and large portfolio of Task Order Requests for Proposals (TORFPs) throughout the life of the vehicle;
- Provide quality products and services that meet task order requirements the first-time, on budget and on schedule.

C.5.1.4.2.3 Cross-Platform, Program, and Project Coordination

The Contractor shall identify and participate in opportunities to facilitate cross-platform, program and project coordination/collaboration to advance IT/IM practices and systems within the Agency. As the Contractor gains institutional and technical knowledge of NRC while working on BPA Calls or conducting outreach activities, the Contractor may be required to provide this type of information to customers, stakeholders, and to other GLINDA Contractors on an ongoing basis. The Contractor may be also be required to present this information in the form of a report to the Agency. The Contractor shall also proactively support the sharing of lessons learned as well as opportunities for improved coordination, including opportunities for better leveraging NRC's IT/IM enterprise tools and services and improving the efficiency and effectiveness of NRC's IT/IM related activities.

C.5.2 Support Phases

The Contractor shall provide up to four (4) phases of support, within or adjacent to the Service Areas, for the BPA, including:

Phase 1 - BPA Transition: Contractor shall become knowledgeable about the NRC, NRC technology environment, hardware/software inventory, and the required services under this BPA. Contractors shall submit key personnel paperwork to obtain the required Agency security clearance.

Phase 2 – BPA Call Transition: After successfully winning any BPA Call, the Contractor shall transition existing services from the incumbent within the specified transition period of the BPA Call by facilitating specific knowledge transfer and duties to successfully perform the services and/or utilize corresponding equipment required by the BPA Call. Successful transition shall be defined as sufficient knowledge and capability to manage and deliver the BPA Call services and/or equipment at the service levels outlined in the BPA Call. Contractors shall be considered fully compliant with Phase 2 once all existing services, equipment, and support activities have been transitioned and are functioning at defined service levels.

Phase 3 – BPA Call Service Delivery: After successfully transitioning a BPA Call from the incumbent, the Contractor shall perform the specific service requirements of the BPA Call at or above the service levels required.

Phase 4 - Transition and Close-Out: The Transition and Close-Out process is defined as a smooth transition from one Contractor to another, in order to maintain the program's integrity required under this and future Agency awards/agreements. The Contractor shall take all actions necessary to achieve a successful transition to the incoming successful Contractor.

C.5.2.1 Phase 1 – BPA Transition

It is expected that the primary transition activities will occur as a component of each of the BPA Calls under Phase 2. However, since the BPA represents the initial step in transitional performance from the incumbent(s), the Contractor shall complete limited transition activities prior to becoming the Contractor on any specific BPA Call. The BPA transition shall focus on, but not be limited to, submission of clearance documents for Key Personnel and the review of inventory and other NRC provided documentation and procedures.

C.5.2.1.1 BPA - NRC Kick-Off

The Contractor shall attend a Kick-Off Orientation hosted by the NRC. The orientation will be held at NRC Headquarters no later than fifteen (15) business days after the BPA is awarded. The Contractor's BPA Key Personnel shall attend; other Contractor staff participation is left to the discretion of the Contractor. The orientation will review the BPA in detail and outline the next steps for transitional support as well as BPA Call forecasts. The orientation shall not exceed eight (8) hours.

C.5.2.1.2 BPA - Knowledge Transfer

The Contractor shall review technical and administrative policies, processes, and documentation necessary to support the specific operational areas covered under the BPA. Knowledge transfer is anticipated to begin upon the BPA's award in order to strengthen the BPA Contractor's ability to respond to the BPA Calls. In-depth knowledge transfer shall be performed once the specific BPA Calls are issued.

This documentation shall expand, as applicable, to any additional requirements outlined in subsequently issued BPA Calls. In addition, the Contractor shall develop a "living" knowledge transfer process to be used throughout the lifecycle of this BPA that includes but may not be limited to open communication both oral and written, technical assistance, and demonstrations with both other Contractor support and NRC Staff. The documented processes may be shared, at the Agency's discretion, with other contractors supporting adjoining Call Orders or support Contractors/staff to assure synchronization and common understanding across different boundaries.

The Contractor shall retain a copy of all delivered BPA-level artifacts in a historical repository for the life of the BPA. The repository contents shall be available to the NRC at its request throughout the entire period of performance of the BPA.

C.5.2.1.3 Preliminary Asset Assessment

The current NRC IT environment is a mix of assets leased or owned by the incumbent ITISS Contractor and assets owned by the Agency. However, the majority of the assets are leased by NRC from the incumbent ITISS Contractor.

During Phase 1, or the period between BPA award and BPA Call release, the NRC will provide an inventory list prepared by the incumbent ITISS Contractor of NRC and non-NRC hardware and software. The inventory will denote whether the asset is NRC Owned, Leased, or Incumbent Owned. Additionally, NRC will provide the findings from an independent auditor who evaluated the inventory to assess appropriate valuation of the current non-NRC owned inventory NRC anticipates needing to transition to or replacement by the successful BPA Call Contractor. This inventory will be used to support the BPA Call release and corresponding Contractor response.

Upon award of the GLINDA BPA, the Contractors shall review the documentation described above and select the assets to be purchased or leases to be transitioned from the incumbent ITISS Contractor. The incoming Contractor shall choose one of several options to transition needed equipment and be prepared to articulate their proposed solutions in BPA Call proposals as applicable:

1. The incoming Contractor can negotiate and assume leases with the leasing company or incumbent and complete the term of each lease or establish new lease terms;

2. The Contractor can decline to utilize the previous incumbent leases or equipment and provide replacement equipment pricing (leasing or buying) in their BPA Call quote. However, Contractors should note that new equipment may require additional security, performance and operational review; testing and approval (approximately 90 days from the date the equipment has been identified and sample devices are available for testing) prior to production operation; or
3. A combination of the two options above.

If there are assets that span different BPA Calls or questions of ownership exist, the Contractor shall discuss/clarify NRC's intent or need and then negotiate appropriately with the incumbent to resolve the issue before validating resolution with the NRC. via their response to corresponding BPA Calls.

C.5.2.2 Phase 2 - BPA Call Transition

The BPA Call transition period will commence once the BPA Call is awarded. The Phase 2 transition process objectives are a smooth but activity-intensive transition from one Contractor to another, focused on delivery continuity. Further, the contractor shall take all actions necessary to collaborate and coordinate with other Contractors in related BPA Call areas or performing work under different contracts. It is envisioned that BPA Call transition will take approximately 90 days from the date of the BPA Call award to full operational performance (Phase 3). During this time period there will be overlap between the incumbent and the BPA Call Contractor. The incumbent shall maintain operational duties until their contractual period of performance is complete, while the BPA Call Contractor shall conduct the appropriate transitional activities to be fully operational after the incumbent's departure.

However, actual transition times will be subject to the needs of individual BPA Calls and the available time allotted after BPA Call establishment. Individual BPA Calls may require additional or specific transition processes. Specific processes will be identified in each BPA Call. The following BPA Call transition activities represent the expected minimum requirements for each BPA Call.

C.5.2.2.1 BPA Call Kick-Off

The Contractor shall arrange and schedule a Kick-Off Orientation. The orientation will be held at NRC Headquarters or BPA Call specified location no later than five (5) business days after the BPA Call is awarded. The incoming Contractor's BPA Call Key Personnel shall attend; other Contractor staff participation is left to the discretion of the Contractor. The orientation will review the BPA Call in detail and outline the next steps for transitional support as well as finalize the BPA Call transition plan and BPA Call management plan (and/or other documents required in the BPA Call Quote process).

C.5.2.2.2 BPA Call Knowledge Transfer

The Contractor shall learn and/or document technical and administrative policies and processes necessary to support the specific Service Areas in the BPA Call. Additionally, these processes may be shared, at the NRC's discretion, with adjoining support Contractors to ensure synchronization and common understanding across service, project, or program boundaries. BPA Call knowledge transfer is anticipated to begin upon issuance of the BPA Call.

The Contractor shall develop or, if the NRC designates a centralized capability, use a "living" knowledge transfer process throughout the lifecycle of the BPA Call that includes but may not

be limited to open communication both oral and written, technical assistance, and demonstrations with both other Contractor support and NRC Staff.

The Contractor shall retain a copy of all BPA Call artifacts in one or more designated NRC repositories. Additionally, the Contractor shall document and retain lessons learned during performance of the BPA Call. The "lessons learned" documentation shall be available to the NRC upon request within ten (10) business days.

C.5.2.2.3 Asset Transition

Some BPA Calls may require full or partial asset transition. Upon BPA Call establishment and legal transfer of the assets from the incumbent ITISS Contractor to the incoming Contractor, the incumbent ITISS Contractor's responsibility for prior contract services will terminate. This will occur before the BPA Call transition period ends.

The BPA Call Contractor shall be responsible for all costs associated with providing (as needed), provisioning, maintaining, and operating the BPA Call assets. All costs of inventory and transfer will be the responsibility of the BPA Call Contractor and incumbent contractor.

C.5.2.2.4 Transition Management Plan and Execution

During the BPA Call transition period, the Contractor shall assign a Transition Lead and team to coordinate with the NRC to ensure that the Contractor has all the resources they need to effectively learn the environment (current programs, projects, priorities, impending deadlines, etc.) and to train the Contractor's delivery team on NRC processes and procedures.

As part of its BPA Call responses, the Contractor shall describe their transition plan (how they intend to assume management and delivery of the services), which includes at a minimum the following:

- Description of Transition team (e.g., names, roles, experience summary, and responsibilities)
- Processes to clear staff in a timely manner and meet proposed staffing levels before full operational performance
- Transfer and/or procurement of required assets/products, if needed
- Transition management approach and objectives
- Management tools (software, etc.) including installation, and training
- Methodology to successfully transfer ongoing integration projects from the incumbent contractor(s)
- Transition execution steps with detailed milestones and deliverables
- What the Contractor will need from the NRC to be successful, including identification of barriers or risks NRC can control

The Contractor shall follow the NRC approved transition plan as discussed in the BPA Call Kick-Off Meeting. Any revisions made during the Kick-Off Meeting shall be documented and resubmitted to the Contracting Officer's Representative (COR) for final acceptance within three
(3) business days of the meeting.

The NRC requires a security review and clearance of Contractor employees in order to gain access to NRC facilities. All proposed staff must be US Citizens in order to be cleared to provide services under this BPA and associated BPA Calls. If awarded a BPA Call, the Contractor must be prepared to submit completed security paperwork for proposed personnel within three (3) business days after award. Paperwork may be submitted on an 'as completed' basis. For planning purposes, a typical clearance review takes two to six weeks, but will vary depending on the individual's circumstances.

C.5.2.3 Phase 3 - BPA Call Service Delivery

Upon completion of BPA Call transition, the Contractor shall perform the operational or project support activities as described in the BPA Call requirements. Specific performance and service level requirements, as well as mechanisms for tracking and reporting will be defined within each BPA Call.

C.5.2.4 Phase 4 - Transition and Close-Out

The Transition and Close-Out process is defined as a straightforward and frictionless transition from one Contractor to another in order to maintain the integrity and continuity of services required under this and future Agency awards/agreements. The Contractor shall take all actions necessary to achieve a successful transition to the incoming successful Contractor.

C.5.2.4.1 Knowledge Transfer

The Contractor shall remain functional and operational up until the point of expiration or cancellation of the BPA and/or BPA Calls. The Contractor shall submit to the NRC a phase-out plan 90 calendar days before the period of performance is complete or cancellation occurs. The phase-out plan shall address, but may not be limited to, the following.

- Procedures for retaining the staffing and/or performance levels necessary to maintain required BPA Call services through the last day of performance.
- Procedures and responsibilities for performing a physical inventory and reconciliation of NRC Furnished Equipment (GFE) and NRC Furnished Information (GFI).
- Procedures and responsibilities for reconciling and certifying material and equipment on- hand levels and accuracy.
- Procedures and mechanisms for transferring knowledge and documentation.
- A list of all ongoing tasks and activities of the current staff, including a summary description of the work. For each task/activity, the Phase-Out Plan shall include upcoming milestones and their individual status, the level of effort being applied, and current or anticipated risks associated with task completion.

The Contractor shall confirm it has retained all delivered BPA Call artifacts in one or more of the Agency's designated repositories.

C.5.2.4.2 Transition Assurance

The Contractor shall facilitate the transition of contracted activities and services to the NRC or to a follow-on Contractor at the end of performance for either the BPA as a whole, or any individual BPA Call issued under it, or, alternatively, as any activities are transitioned to performance by the Agency itself.

The Contractor shall ensure adequate planning, staffing, and management to implement an orderly transition of services to the end of their contractual period of performance. Transition activities shall include, but may not be limited to, the following:

- Providing adequate NRC badged staff to perform work.
- Transferring Information Technology Infrastructure (ITI) components, as required.
- Installation and training of management tools (software, etc.).
- Transferring ongoing projects.
- Providing the NRC with current and accurate versions of all standard operating procedures, guidelines, performance reports, specifications for hardware and software, and other pertinent information needed to continue the services being performed by the Contractor.
- Providing "shadowing" and other knowledge transfer meetings and opportunities to facilitate the transfer of information, processes, and data needed to continue the services being performed by the Contractor.
- Providing current and accurate program management documents.
- Removing and purging of all non-public or other protected NRC information and data from any Contractor owned system, and certification thereof.
- Actively participating in transition management activities with a transition team comprised of NRC and/or successor Contractor personnel.

The Contractor shall coordinate its transition out activities with the incoming Contractor to ensure a smooth and orderly transition at the end of the period of performance. The Contractor shall remove all Contractor-owned property from the NRC spaces or facilities by close of business on the last day of the period of performance.

C.5.2.4.3 Transfer of Assets to a Successor Contractor or the NRC

If applicable, the Contractor shall execute its proposed and accepted asset transfer plan to be enacted and executed at the conclusion of the associated BPA Call. Where applicable, upon expiration of the BPA Call the Contractor shall transfer ownership of all installed hardware, software, maintenance agreements, operational data (including CMDB data, incident data, and known error/knowledge data), and associated documentation to the NRC or incoming Contractor. This transfer shall be accomplished in accordance with terms and conditions mutually agreed to upon award.

All assets that are not transferred will be the responsibility of the Contractor. The NRC is not liable for disposal of the assets. Under no circumstances will the NRC or the successor Contractor be liable for any leases extending beyond the end of the BPA Call, or for any leases extending into an unexercised option period.

C.5.3 Over-Arching BPA/BPA Call Management

In addition to the general business and technical capabilities of the Contractor, the success of GLINDA is based upon the Contractor's ability to consistently and efficiently execute BPA and BPA Call related processes including but not limited to:

- Staffing qualified individuals focused on high quality delivery and continuous

improvement and innovation, consistent with the requirements of this BPA.

- Managing delivery performance, quality, and benefits realization including mechanisms for helping ensure the Agency achieves its desired quality and efficiency objectives.
- Executing sound project management inclusive of BPA Call schedule, risk, and financial management practices and controls.
- Managing subcontractors and coordinating with other Agency Contractors under different contracts or BPA Calls to help ensure seamless delivery.
- Conducting effective BPA Call and related activity communications to a broad group of direct and indirect stakeholders.

The NRC is seeking Contractors capable of articulating and demonstrating an ability to successfully and collaboratively execute the processes that help ensure the NRC consistently receives high quality services throughout the life of the BPA.

Additionally, the Contractor may be required to attend senior level meetings and collaborate with NRC staff to provide briefings, status reports, "after action reports" and other informational meetings. With the potential for BPA Calls to support requirements across the NRC, it is the NRC's expectation that the Contractor shall centrally monitor and manage all services provided under this BPA.

C.5.3.1 Personnel

Each BPA Call will require a broad range of capabilities for assigned support personnel. The Contractor shall be responsible for ensuring continued delivery of qualified, capable, and competent personnel to perform the services required by the BPA Call. The Contractor shall fill any vacancies within thirty (30) business days of Contractor staff departure, not inclusive of the NRC security clearance process. The COR may require the Contractor to provide evidence that personnel possess the proper qualifications, certifications, skills, experience, and education.

C.5.3.2 Key Personnel

This BPA requires a specialized level of Contractor expertise and the NRC maintains the right to accept or reject finished deliverables. The NRC will not create an employee-employer relationship with the Contractor personnel, but rather expects the Contractor to ensure quality assurance and control for the deliverables produced and the Contractor personnel utilized to produce these deliverables. The Contractor shall ensure a stable workforce during the performance of this BPA and shall fill any vacancies within thirty (30) business days of Contractor staff departure, not inclusive of the NRC security clearance process.

Two Key Personnel positions under this BPA are the Program Manager and Deputy Program Manager. These individuals will be responsible for all activity under this BPA and the resulting completion of each BPA Call. These individuals should have experience in similar engagements
-- not only technically similar, but also involving collaboration among multiple Contractors and client stakeholder groups. In addition, these individuals should possess an ITIL Expert level certification or higher within 1 year of BPA award, and successfully maintain this certification for the duration of the BPA. Additional key personnel may be identified at the BPA Call level.

Given the criticality of the key positions to performance of this BPA, the proposed key personnel shall possess demonstrated experience in the different skill sets required and functions to be performed. The skill level and qualifications of the BPA key personnel shall be maintained through completion of the BPA.

C. 6 BPA Labor Categories and Descriptions

Below is a list of labor categories required for this BPA. Based on corresponding duties and requirements, each schedule holder shall match their GSA Schedule 70 labor categories to the ones listed below. BPA Holder(s) may use any of their GSA Schedule 70 labor categories to represent more than one of the BPA labor categories, as long as the labor category is capable of performing the duties described and fulfills the requirements.

The Education Experience Equivalent for this RFQ is as follows:

Associate's Degree 2 Years Relevant Experience

Bachelor's Degree 4 Years Relevant Experience

Master's Degree 6 Years Relevant Experience

C.6.1 Administrative Assistant I

Example of duties:

- Provide administrative support specifically dedicated to the requirements of the project team.
- Plan and produce correspondence, reports, proposals, memos, and other documentation using a personal computer.
- Operate spreadsheet software such as Excel to produce finished documents.
- Proofread completed documents.
- Provide copying and production support as needed.

Requirements:

- High School Diploma plus 0-3 years of relevant experience

C.6.2 Administrative Assistant II

Example of duties:

- Provide administrative support specifically dedicated to the requirements of the project team.
- Perform a wide range of clerical and administrative duties including, for example, typing, filing, tracking of time records, word processing, dictation, and composition of correspondence.

Requirements:

- Associate's Degree plus 3+ years of relevant experience

C.6.3 Communications Hardware Specialist

Example of duties:

- Analyze network and computer communications hardware characteristics and recommends equipment procurement, removals, and modifications.
- Add, delete, and modify, as required, host, terminal, and network devices.
- Assist and coordinate with communications network specialists in the area of communication software.
- Analyze and implement communications standards and protocols according to site requirements.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.4 Systems Engineer I

Example of duties:

- Responsible for the planning and engineering of an organization's systems infrastructure.
- Includes the implementation and design of hardware and software.
- Monitors the performance of systems.
- Relies on limited experience and judgment to plan and accomplish goals.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience demonstrating familiarity with standard systems engineering concepts, practices, and procedures.

C.6.5 Systems Engineer II

Example of duties:

- Responsible for the planning and engineering of an organization's systems infrastructure.
- Includes the implementation and design of hardware and software. Monitors the performance of systems.
- Relies on limited experience and judgment to plan and accomplish goals.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience demonstrating familiarity with standard systems engineering concepts, practices, and procedures.

C.6.6 Systems Engineer III

Example of duties:

- Responsible for the planning and engineering of an organization's systems infrastructure.
- Includes the implementation and design of hardware and software. Monitors the

performance of systems.

- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- May lead and direct the work of others.

Requirements:

- Bachelor's Degree plus 4+ years of relevant experience demonstrating familiarity with standard systems engineering concepts, practices, and procedures.

C.6.7 Facilitator

Example of duties:

- Assist group members of teams formed in developing information system specifications and functionality to communicate their ideas, information, and opinions more effectively. Manage the team meetings and workshops.
- Keep the team focused on the subject at hand to achieve objectives.
- Assures discussions are brought to conclusion.

Requirements:

- Bachelor's Degree plus 2-5 years of relevant experience.

C.6.8 Project Leader

Example of duties:

- Consult in a specific functional area of project.
- Support the development of work plans to fulfill government requirements.
- Support formulation of milestone schedules or other documented plans.

Requirements:

- Bachelor's Degree plus 5-10 years of relevant experience.

C.6.9 Project Manager

Example of duties:

- Serves as project manager for a large, complex task order or a group of task and shall assist the Program Manager in working with the ordering activity Contracting Officer (CO), the contract-level Contracting Officer's Representative (COR), the task order-level COR(s), ordering activity management personnel and customer agency representatives.
- Under the guidance of the Program Manager, responsible for the overall management of the specific task order(s).
- Ensures that the technical solutions and schedules for the task order are implemented in a timely manner.
- Performs enterprise wide horizontal integration planning and interfaces to other functional systems.

- Assists the Program Manager in the technical direction of TO support activities and in monitoring contractor performance with respect to deliverables, project milestones and project expenditures.
- Responsible for technical direction of projects which support one or more of major NRC program areas.
- Identifies issues associated with Delivery Orders, particularly those which might impact the Agency's Information Technology Architecture.
- Upon identifying issues, notifies the Program Manager, NRC COR, and appropriate officials of the architectural issues and potential impacts.
- Ensures that contractor personnel are kept abreast of emerging technologies that could impact the Agency's architecture.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.10 Deputy Program Manager

Example of duties:

- Supports program management in areas such as, but not limited to, application and systems development
- Experienced in analyzing, design and development of web projects and database and software programs.

Requirements:

- Bachelor's Degree
- Information Technology Infrastructure Library (ITIL) Expert Level Certification shall be obtained within one year of award and maintained for the duration of the BPA.
- 10+ years of relevant experience, including 3+ years of experience being a Project Manager

C.6.11 Program Manager

Example of duties:

- Provides technical direction and administrative management of contract activities;
- Develops overall program plans, guidance and procedures necessary to adequately provide support required by diverse technical, administrative and program functions and operation of NRC.
- Reviews IT support requirements, determines the necessary skills and personnel resources, formulates policies and procedures necessary to achieve effective project planning and control, budget projections and quality assurance;
- Meets with management, technical and operating personnel within client organizations to review requirements, present proposed action plans and to discuss and resolve technical, administrative and management problems and issues;

- Evaluates proposed computer systems to determine technical feasibility, costs for development and functional adequacy.
- Responsible for ensuring those contractor personnel providing services under this contract are kept abreast of emerging technologies that could impact the Agency's architecture.

Requirements:

- Bachelor's Degree
- Information Technology Infrastructure Library (ITIL) Expert Level Certification shall be obtained within one year of award and maintained for the duration of the BPA.
- 15+ years of relevant experience, with 3+ years specifically as a Deputy Program Manager or Project Manager over an extremely large enterprise project.

C.6.12 Program Management SME

Example of duties:

- Supporting the NRC as a Project Management Consultant
- Provide project management, security compliance and configuration management assistance for numerous systems.

Requirements:

- Bachelor's Degree plus 15+ years of relevant experience

C.6.13 Senior Program Manager

Example of duties:

- Directs all phases of programs from inception through completion.
- Responsible for coordinating subordinate employee recruitment, selection and training, performance assessment, work assignments, salary, and recognition/disciplinary actions.
- Responsible for the cost, schedule and technical performance of company programs or subsystems of major programs.
- Participates in the negotiation of contract and contract changes.
- Coordinates the preparation of proposals, business plans, proposal work statements and specifications, operating budgets and financial terms/conditions of contract.
- Acts as primary customer contact for program activities, leading program review sessions with customer to discuss cost, schedule, and technical performance.
- Establishes design concepts, criteria and engineering efforts for product research, development, integration and test.
- Develops new business or expands the product line with the customer.
- Establishes milestones and monitors adherence to master plans and schedules, identifies program problems and obtains solutions, such as allocation of resources or changing contractual specifications.

- Directs the work of employees assigned to the program from technical, manufacturing and administrative areas.

Requirements:

- Bachelor's Degree
- Information Technology Infrastructure Library (ITIL) Expert Level Certification
- 15+ years of relevant experience, including 3+ years experience as a Program Manager

C.6.14 SOC Tier 1 Analysts

All Tier 1 analyst candidates shall have a minimum of two (2) years professional experience in network or UNIX/Linux system administration, software engineering, software development, and/or a bachelor's degree in Computer Science, Engineering, Information Technology, Cybersecurity, or related field. The candidates must have some experience working with various security methodologies and processes, knowledge of Transmission Control Protocol / Internet Protocol (TCP/IP) protocols, knowledge and experience configuring and implementing a diverse array of technical security solutions, and experience providing analysis and trending of security log data from a large number of heterogeneous security devices.

C.6.15 SOC Tier 2 Analysts

All Tier 2 Analyst candidates shall have a minimum of four (4) years of professional experience in incident detection and response, malware analysis, or cyber forensics, and a bachelor's degree in

Computer Science, Engineering, Information Technology, Cybersecurity, or related field. Candidates must have extensive experience working with various security methodologies and processes, advanced knowledge of TCP/IP protocols, experience configuring and implementing various of technical security solutions, extensive experience providing analysis and trending of security log data from a large number of heterogeneous security devices, and must possess expert knowledge in two or more of the following areas related to cybersecurity:

- Vulnerability Assessment
- Continuous diagnostics and mitigation
- Intrusion Prevention and Detection
- Access Control and Authorization
- Endpoint Protection
- Application Security
- Protocol Analysis
- Firewall Management
- Incident Response
- Encryption
- Web-filtering
- Advanced Threat Protection
- Data Loss Prevention

In additional to the foundation requirements above, Tier 2 Analyst candidates shall have the following specialized experience:

Security Engineering: Candidates shall have a minimum of three (3) years of specialized

professional experience in cybersecurity, information risk management, or information systems risk assessment, and must be knowledgeable in several areas such as: Vulnerability Assessments, Intrusion Prevention and Detection, Access Control and Authorization, Policy Enforcement, Application Security, Protocol Analysis, Firewall Management, Incident Response, Data Loss

Prevention, Encryption, Two-Factor Authentication, Web-filtering, Advanced Threat Protection, DNSSEC administration, and packet analysis.

Incident Response Analyst: Candidates shall have a minimum of three (3) years of specialized professional experience responding to information system security incidents and an ability to use the NRC furnished toolset to identify and determine root causes of incidents, provide any required documentation and possible evidence to authorized legal or investigative authorities, and assist with incident remediation efforts..

Cyber Intelligence Analyst: Candidates shall have at least three (3) years of specialized professional experience in threat detection, network monitoring and/or cyber intelligence analysis, and a bachelor's degree in Computer Science, Engineering, Information Technology, Cybersecurity, or related field.

C.6.16 SOC Tier 3 Analysts

All Tier 3 Analyst candidates shall have a minimum of six (6) years of professional experience in incident detection and response, malware analysis, or cyber forensics, and a bachelor's degree in Computer Science, Engineering, Information Technology, Cybersecurity, or related field. The candidates must have extensive experience analyzing and synthesizing information with other relevant data sources, providing guidance and mentorship to others in cyber threat analysis and operations, evaluating, interpreting, and integrating all sources of information, and fusing computer network attack analyses with counterintelligence and law enforcement investigations.

In additional to the foundation requirements above, Tier 3 Analyst candidates shall have the following specialized experience for their position:

Security Engineering Analyst: Candidates shall have a minimum of five (5) years of specialized professional experience in security, information risk management, or information systems risk assessment, and must be knowledgeable in many areas such as: Vulnerability Assessments, Intrusion Prevention and Detection, Access Control and Authorization, Policy Enforcement, Application Security, Protocol Analysis, Firewall Management, Incident Response, Data Loss

Prevention (DLP), Encryption, Two-Factor Authentication, Web-filtering, Advanced Threat Protection, security architecture, DNSSEC administration, and packet analysis.

Incident Response Analyst: Candidates shall have a minimum of five (5) years of specialized professional experience responding to information system security incidents. Ability to use the agency furnished toolset to identify and determine root causes of incidents, provide any required documentation and possible evidence to security investigators, and lead incident remediation efforts.

Cyber Intelligence Analyst: Candidates shall have at least five (5) years of specialized professional experience in one or more of the following areas: collecting, synthesizing, fusing, or authoring unclassified and classified cyber threat intelligence products, email security, including identification of phishing attempts, malware detonation, and knowledge of commonly used email analysis tools, and digital media forensic analysis including static malware code disassembly/analysis, and/or runtime malware code analysis.

C.6.17 Information Assurance Team – Tier 2

The candidates shall have at least three (3) years of professional experience in information assurance and security compliance, and a bachelor's degree in Computer Science, Engineering, Information Technology, Cybersecurity, or related field.

C.6.18 Information Assurance Team – Tier 3

The candidates shall have at least five (5) years of professional experience in information assurance and security compliance, and a bachelor's degree in Computer Science, Engineering, Information Technology, Cybersecurity, or related field.

C.6.19 Security Program Manager

The Contractor's Program Manager shall possess, at a minimum, eight (8) years of direct project and program management experience in delivery of information systems or computer network support services and/or a Bachelor's Degree in Computer Science, Engineering, Information Technology, or Cybersecurity. The Program Manager shall have demonstrated capabilities to analyze highly complex cybersecurity and network issues, recommend plans of action for SOC Contractor and SOC Government staff, and manage Contractor teams supporting resolution of these issues. This individual shall serve as the Contractor's primary contact for the SOSEB Branch Chief, NRC SOC Government personnel and the NRC CISO.

C.6.20 Disaster Recovery Specialist

Example of duties:

- Provide support in the development of a government agencies emergency management and business recovery plans.
- Perform functions pertaining to the agencies business risk assessments.
- Review and develop business recovery strategies; draft procedures for identifying failures and invoking contingency plans.
- Create response procedures and identifying communications channels.
- Communicate with various response teams during testing and actual execution of recovery procedures.
- Support the design, development, installation, implementation and administration of backup solutions.
- Make recommendations to the user community and the operations group on system enhancements.

Requirements:

- Bachelor's Degree
- 5+ years of experience working with business recovery and/or disaster recovery planning subject matter
- General knowledge of business processes, management structures, and technology programs/platforms preferred
- Excellent verbal and written communication skills

C.6.21 Systems Architect I

Example of duties:

- Designs and defines system architecture for new or existing complex computer systems.
- Determines systems specifications, input/output processes, and working parameters for hardware/software compatibility and maintenance of system security.
- Coordinates design of subsystems and integration of total system.
- Identifies, analyzes, and resolves program support deficiencies.
- Develops and recommends corrective actions.
- May provide technical guidance for database administrators and software developers.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.22 Systems Architect II

Example of duties:

- Designs and defines system architecture for new or existing complex computer systems.
- Determines systems specifications, input/output processes, and working parameters for hardware/software compatibility and maintenance of system security.
- Coordinates design of subsystems and integration of total system.
- Identifies, analyzes, and resolves program support deficiencies.
- Develops and recommends corrective actions.
- May provide technical guidance for database administrators and software developers.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.23 Systems Architect III

Example of duties:

- Designs and defines system architecture for new or existing complex computer systems.
- Determines systems specifications, input/output processes, and working parameters for hardware/software compatibility and maintenance of system security.
- Coordinates design of subsystems and integration of total system.
- Identifies, analyzes, and resolves program support deficiencies.
- Develops and recommends corrective actions.
- May provide technical guidance for database administrators and software developers.

Requirements:

- Bachelor's Degree plus 6-8 years of relevant experience

C.6.24 Systems Architect IV

Example of duties:

- Designs and defines system architecture for new or existing complex computer systems.
- Determines systems specifications, input/output processes, and working parameters for hardware/software compatibility and maintenance of system security.
- Coordinates design of subsystems and integration of total system.
- Identifies, analyzes, and resolves program support deficiencies.
- Develops and recommends corrective actions.
- May provide technical guidance for database administrators and software developers.

Requirements:

- Bachelor's Degree plus 8-10 years of relevant experience

C.6.25 Systems Architect SME

Example of duties:

- Supporting the NRC as a Software Developer and Architect on various projects.
- Experienced SME in developing technical and management solutions.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.26 Research Analyst I

Example of duties:

- Studies emerging trends in the information technology field and their ramifications on the organization.
- Educates staff on the use of new technology.
- Ensures products and solutions are applied in a manner that maximizes their worth. Familiar with the field's concepts, practices, and procedures.
- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.27 Research Analyst II

Example of duties:

- Studies emerging trends in the information technology field and their ramifications on the organization.
- Educates staff on the use of new technology.
- Ensures products and solutions are applied in a manner that maximizes their worth.

Familiar with the field's concepts, practices, and procedures.

- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.

Requirements:

- Bachelor’s Degree plus 4+ years of relevant experience

C.6.28 Technical Writer I

Example of duties:

- Writes, edits, and rewrites manuscript copy for reference manuals, operations manuals, user manuals, and programming manuals for software and computer operations.
- Coordinates with programmers and software engineering to verify knowledge of subject in preparation for writing assignment.
- Oversees preparation of illustrative material, selecting drawings, sketches, diagrams, and charts.
- May assist in preparation and layout of work for publication.

Requirements:

- Bachelor’s Degree plus 0-2 years of relevant experience

C.6.29 Technical Writer II

Example of duties:

- Writes, edits, and rewrites manuscript copy for reference manuals, operations manuals, user manuals, and programming manuals for software and computer operations.
- Coordinates with programmers and software engineering to verify knowledge of subject in preparation for writing assignment.
- Oversees preparation of illustrative material, selecting drawings, sketches, diagrams, and charts.
- May assist in preparation and layout of work for publication.

Requirements:

- Bachelor’s Degree plus 2-4 years of relevant experience

C.6.30 Technical Writer III

Example of duties:

- Writes, edits, and rewrites manuscript copy for reference manuals, operations manuals, user manuals, and programming manuals for software and computer operations.
- Coordinates with programmers and software engineering to verify knowledge of subject in preparation for writing assignment.
- Oversees preparation of illustrative material, selecting drawings, sketches, diagrams, and charts.

- May assist in preparation and layout of work for publication.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.31 Technical Writer IV

Example of duties:

- Writes, edits, and rewrites manuscript copy for reference manuals, operations manuals, user manuals, and programming manuals for software and computer operations.
- Coordinates with programmers and software engineering to verify knowledge of subject in preparation for writing assignment.
- Oversees preparation of illustrative material, selecting drawings, sketches, diagrams, and charts.
- May assist in preparation and layout of work for publication.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.32 Document Control Assistant I

Example of duties:

- Maintains central, controlled supply of classified and unclassified documents originating within the company.
- Reviews documents to determine pre-established classification level based on contracts or security manual, distribution requirements and processes distribution requests according to established procedures.
- Ensures generation of quality assurance checklist for product release packages in support of production schedules.
- May be required to maintain a secure, computerized document revision system, a periodic review system, and status tracking for all process-related documents and records.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.33 Documentation Specialist I

Example of duties:

- Prepares and/or maintains documentation pertaining to programming, systems operation and user documentation.
- Translates business specifications into user documentation.
- Plans, writes, and maintains systems and user support documentation efforts, including online help screen.
- Familiar with standard concepts, practices, and procedures within a particular field.

- Relies on limited experience and judgment to plan and accomplish goals. Performs a variety of tasks.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 2+ years of relevant experience

C.6.34 IT Asset Management Administrator

Example of duties:

- Responsible for administrative duties within the IT procurement and inventory management function.
- Maintains records and databases containing information regarding licenses, warranties, and service agreements for the organization's hardware and software.
- Minimizes organizational cost through product standardization and tracking.
- Tracks quality throughout the product lifetime.
- Has knowledge of commonly-used concepts, practices, and procedures within a particular field.
- Relies on instructions and pre-established guidelines to perform the functions of the job.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 2+ years of relevant experience

C.6.35 Configuration Management Specialist I

Example of duties:

- Analyzes changes of product design to determine the effect on the end product design and function and determines and prepares documentation necessary for change.
- Coordinates with customers and manufacturers to determine a process for change reporting.
- Reviews released engineering change data and changes documenting activities to ensure adherence to configuration management procedures and policies.
- Familiar with standard concepts, practices, and procedures within a particular field.
- Relies on limited experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 2+ years of relevant experience

C.6.36 Data Standardization Specialist

Example of duties:

- Provide technical support in the evaluation of prime object names, data elements, and other objects.
- Evaluate proposed objects and their attributes.
- Ensure that proposed object definitions are clear, concise, technically correct, and that they represent singular concepts.
- Ensure that the values of object attributes and domains are accurate and correct.
- Ensure that the proposed objects are consistent with data and process models.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.37 Database Administrator I

Example of duties:

- Develops, implements, administers, and maintains policies and procedures for ensuring the security and integrity of the company database.
- Implements data models, database designs, data access and table maintenance codes.
- Resolves database performance and capacity issues, and replication and other distributed data issues.
- Familiar with standard concepts, practices, and procedures within a particular field.
- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.38 Database Administrator II

Example of duties:

- Develops, implements, administers, and maintains policies and procedures for ensuring the security and integrity of the company database.
- Implements data models, database designs, data access and table maintenance codes.
- Resolves database performance and capacity issues, and replication and other distributed data issues.
- Familiar with standard concepts, practices, and procedures within a particular field.
- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 4+ years of relevant experience

C.6.39 Database Engineer I

Example of duties:

- Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management.
- Uses data mapping, data mining and data transformational analysis tools to design and develop databases.
- Determines data storage and optimum storage requirements.
- Prepares system requirements, source analysis and process analyses.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.40 Database Engineer II

Example of duties:

- Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management.
- Uses data mapping, data mining and data transformational analysis tools to design and develop databases.
- Determines data storage and optimum storage requirements.
- Prepares system requirements, source analysis and process analyses.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.41 Database Engineer III

Example of duties:

- Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management.
- Uses data mapping, data mining and data transformational analysis tools to design and develop databases.
- Determines data storage and optimum storage requirements.
- Prepares system requirements, source analysis and process analyses.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.42 Database Engineer IV

Example of duties:

- Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management.
- Uses data mapping, data mining and data transformational analysis tools to design and develop databases.
- Determines data storage and optimum storage requirements.
- Prepares system requirements, source analysis and process analyses.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.43 System Administrator I

Example of duties:

- Maintains smooth operation of multi-user computer systems, including coordination with network administrators.
- Duties may include setting up administrator and service accounts, maintaining system documentation, tuning system performance, installing system wide software and allocate mass storage space.
- Interacts with users and evaluates vendor products.
- Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery.
- Develops and monitors policies and standards for allocation related to the use of computing resources.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.44 System Administrator II

Example of duties:

- Maintains smooth operation of multi-user computer systems, including coordination with network administrators.
- Duties may include setting up administrator and service accounts, maintaining system documentation, tuning system performance, installing system wide software and allocate mass storage space.
- Interacts with users and evaluates vendor products.
- Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery.

- Develops and monitors policies and standards for allocation related to the use of computing resources.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.45 System Administrator III

Example of duties:

- Maintains smooth operation of multi-user computer systems, including coordination with network administrators.
- Duties may include setting up administrator and service accounts, maintaining system documentation, tuning system performance, installing system wide software and allocate mass storage space.
- Interacts with users and evaluates vendor products.
- Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery.
- Develops and monitors policies and standards for allocation related to the use of computing resources.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.46 System Administrator IV

Example of duties:

- Maintains smooth operation of multi-user computer systems, including coordination with network administrators.
- Duties may include setting up administrator and service accounts, maintaining system documentation, tuning system performance, installing system wide software and allocate mass storage space.
- Interacts with users and evaluates vendor products.
- Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery.
- Develops and monitors policies and standards for allocation related to the use of computing resources.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.47 IT Service Management Consultant

Example of duties:

- Researches and analyzes basic and complex issues surrounding the IT service management processes and systems of an organization.

- Makes recommendations surrounding improving IT service processes, efficiency and practices.
- Simulates and tests process improvements.
- Communicates changes and may provide training to impacted business units.
- Familiar with broad range of ITIL concepts, practices, and procedures.
- Relies on extensive experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.

Requirements:

- Bachelor's Degree
- Information Technology Infrastructure Library (ITIL) Foundations Level Certification required. ITIL Intermediate Level Certification or higher preferred.
- 8+ years of relevant experience

C.6.48 Computer Scientist

Example of duties:

- Act as a senior consultant in complex or mission critical client requirements.
- Develop, modify, and apply computer modeling and programming applications to analyze and solve mathematical and scientific problems affecting system and program performance.
- Participate in all phases of scientific and engineering projects such as research, design, development, testing, modeling, simulating, training, and documentation.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.49 Technologist SME

Example of duties:

- Responsible for the long-range direction of a program's technology function.
- Directs the strategic design, acquisition, management, and implementation of an program-wide technology infrastructure.
- Maintains technology standards for the program.
- Directs the activities necessary to keep the technology infrastructure running seamlessly, efficiently, and effectively while ensuring compliance with established standards and policies.
- Demonstrates expertise in a variety of the field's concepts, practices, and procedures.
- Relies on extensive experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- Leads and directs the work of others.

Requirements:

- Bachelor's Degree plus 10-12 years of relevant experience

C.6.50 Subject Matter Expert II

Example of duties:

- Analyze user needs to determine functional requirements and define problems and develop plans and requirements in the subject matter area for moderately complex to complex systems related to information systems architecture, networking; telecommunications, automation, communications protocols, risk management/electronic analysis, software, lifecycle management, software development methodologies, and modeling and simulation.
- Perform functional allocation to identify required tasks and their interrelationships. Identify resources required for each task.

Requirements:

- Bachelor's Degree
- 12-15 years of relevant experience in new and related older technology that directly relates to the required area of expertise.
- Possess requisite knowledge and expertise so recognized in the professional community that the Government is able to quality the individual as an expert in the field for an actual task order.
- Exceptional oral and written communication skills.

C.6.51 Subject Matter Expert III

Example of duties:

- Provide technical, managerial, and administrative direction for problem definition, analysis, requirements development, and implementation for complex to extremely complex systems in the subject matter area.
- Make recommendations and advise on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; communications protocols; risk management/electronic analysis; software; lifecycle management; software development methodologies; and modeling and simulation.

Requirements:

- Bachelor's Degree
- 15+ years of relevant experience in new and related older technology that directly relates to the required area of expertise.
- Possess requisite knowledge and expertise so recognized in the professional community that the Government is able to quality the individual as an expert in the field for an actual task order.

C.6.52 Help Desk Specialist

Example of duties:

- Provides support to end users on a variety of issues.
- Identifies, researches, and resolves technical problems.
- Responds to telephone calls, email and personnel requests for technical support.
- Documents, tracks and monitors the problem to ensure a timely resolution.
- Has knowledge of commonly-used concepts, practices, and procedures within a particular field.
- Relies on instructions and pre-established guidelines to perform the functions of the job.
- Works under immediate supervision.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.53 Integration Architect

Example of duties:

- Develops and implements solutions coordinating applications across the enterprise or its units/departments.
- Evaluates existing components or systems to determine integration requirements and to ensure final solutions meet organizational needs.
- Reuses components when possible and assists management in buy/build decisions.
- Familiar with the standard concepts, practices, and procedures.
- Relies on experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- May lead or direct the work of others.

Requirements:

- Bachelor's Degree plus 3-5+ years of relevant experience

C.6.54 Hardware Installation Technician I

Example of duties:

- Conduct site surveys; assess and document current site network configuration and user requirements.
- Design and optimize network topologies.
- Analyze existing requirements and prepare specifications for hardware acquisitions.
- Prepare engineering plans and site installation Technical Design Packages.
- Develop hardware installation schedules.

- Prepare drawings documenting configuration changes at each site.
- Prepare site installation and test reports.
- Configure computers, communications devices, and peripheral equipment. Install network hardware.
- Train site personnel in proper use of hardware.
- Build specialized interconnecting cables.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.55 Hardware Installation Technician II

Example of duties:

- Organize and direct hardware installations on site surveys.
- Assess and document current site network configuration and user requirements.
- Design and optimize network topologies.
- Analyze and develop new hardware requirements and prepare specifications for hardware acquisitions.
- Direct and lead preparation of engineering plans and site installation Technical Design Packages.
- Develop hardware installation schedules.
- Mobilize installation team.
- Direct and lead preparation of drawings documenting configuration changes at each site.
- Prepare site installation and test reports.
- Coordinate post installation operations and maintenance support.

Requirements:

- Bachelor's Degree plus 4+ years of relevant experience

C.6.56 Hardware Specialist – Information Technology

Example of duties:

- Review computer systems in terms of machine capabilities and man-machine interface.
- Prepare reports and studies concerning hardware.
- Prepare functional requirements and specifications for hardware acquisitions.
- Ensure that problems have been properly identified and solutions will satisfy the user's requirements.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.57 Operations Manager

Example of duties:

- Manages the information technology department.
- Implements and maintains policies and goals that support the organization's IT needs.
- Ensures proper functioning of IT operations and oversees necessary improvements.
- Helps business operations groups utilize information systems to improve their efficiency.
- Ensures computer equipment, hardware, and software are updated to meet organizational needs.
- Familiar with a variety of the field's concepts, practices, and procedures.
- Relies on extensive experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- Leads and directs the work of others.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.58 Communications Specialist

Example of duties:

- Analyze network characteristics (e.g., traffic, connect time, transmission speeds, packet sizes, and throughput) and recommend procurement, removals, and modifications to network components.
- Design and optimize network topologies and site configurations.
- Plan installations, transitions, and cutovers of network components and capabilities.
- Coordinate requirements with users and suppliers.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.59 Network Specialist I

Example of duties:

- Assists in the development and maintenance of network communications.
- Uses knowledge of LAN/WAN systems to install and administer internal and external networks.
- Tests and evaluates network systems to eliminate problems and make improvements.
- Has knowledge of commonly-used concepts, practices, and procedures within a particular field.
- Relies on experience, and judgement to perform the functions of the job.

- Works under general supervision.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.60 Network Support Technician

Example of duties:

- Provide support to monitor, install and perform maintenance on personal computers, laptop computers, software, and networks.
- Provide support in responding to system user requests for assistance.
- Provide support for on-the-spot diagnostic evaluations, implementation of corrections, and training users in proper operation of systems and programs.
- Provide support to: install and provide basic support for approved PC software; perform upgrades to all computer platforms, train office staff on computers, maintain logs and inventory of equipment repairs, assist in administering all computer platforms as directed and assist in resolving any operations problems.
- Support the agency LAN Administrator with server maintenance and administration.

Requirements:

- Bachelor's Degree
- 5+ years of relevant experience demonstrating general knowledge of network products including, but not limited to, Novell, CISCO, and UNIX.

C.6.61 Network Administrator

Example of duties:

- Support the installation, implementation, troubleshooting, and maintenance of agency wide-area networks (WANs) and local-area networks (LANs).
- Assist in designing and managing the WAN infrastructure and any processes related to the WAN.
- Provide Production Support of the Network, including: day-to-day operations, monitoring and problem resolution client Networks.
- Provide second level problem identification, diagnosis and resolution of problems.
- Support the dispatch of circuit and hardware vendors involved in the resolution process.
- Support the escalation and communication of status to agency management and internal customers.

Requirements:

- Bachelor's Degree
- 5+ years of relevant experience demonstrating working knowledge in various software systems, architectures, communications protocols, and network hardware devices.

C.6.62 Network Draftsman

Example of duties:

- Develop engineering drawings, using computer based drawing packages such as Aptitude.
- Develop engineering drawings for site plans, network configuration and design.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.63 Network Engineer I

Example of duties:

- Assists in the development and maintenance of network communications.
- Uses knowledge of LAN/WAN systems to help design and install internal and external networks.
- Tests and evaluates network systems to eliminate problems and make improvements.
- Has knowledge of commonly-used concepts, practices, and procedures within a particular field.
- Relies on experience, and judgement to perform the functions of the job.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.64 Network Engineer II

Example of duties:

- Assists in the development and maintenance of network communications.
- Uses knowledge of LAN/WAN systems to help design and install internal and external networks.
- Tests and evaluates network systems to eliminate problems and make improvements.
- Has knowledge of commonly-used concepts, practices, and procedures within a particular field.
- Relies on experience, and judgement to perform the functions of the job.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 4+ years of relevant experience

C.6.65 Communications Network Manager

Example of duties:

- Evaluate communication hardware and software, troubleshoot local-, metropolitan-, and

wide-area networks (LAN/MAN/WAN) and other network related problems; provide technical expertise for performance and configuration of networks.

- Perform general LAN/MAN/WAN administration; provide technical leadership in the integration and test of complex large-scale computer integrated networks.
- Schedule conversions and cutovers.
- Oversee network control center.
- Supervise maintenance of systems.
- Coordinate with all responsible users and sites.
- Supervise staff.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.66 Wireless Support Specialist

Example of duties:

- Assists clients in the implementation of wireless systems, software, or solutions.
- Evaluates client needs, develops approaches that support business processes, plans and executes on delivery and implementation plans, and tests and troubleshoots final system setups.
- Provides training and end-user support during and after the implementation process.
- Familiar with standard concepts, practices, and procedures within a particular field.
- Relies on limited experience and judgment to plan and accomplish goals.
- Performs a variety of tasks.
- Works under general supervision.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.67 Telecommunications Specialist I

Example of duties:

- Assist senior personnel in formulating and developing communications requirements and design standards.
- Perform complex studies to determine networking capacities and reliability, and make recommendations to augment and/or enhance existing communications networks.
- Provide technical problem diagnoses and resolution support for all associated subsystems, including line monitoring, modem loop-back tests, LAN performance monitoring and terminal failure determination.
- Provide hardware and software installation and configuration support.

Requirements:

- Bachelor's Degree plus 3-6 years of relevant experience

C.6.68 Telecommunications Specialist II

Example of duties:

- Formulate and develop communications requirements and design standards.
- Perform complex studies to determine networking capacities and reliability, and make recommendations to augment and/or enhance existing communications networks.
- Provide technical problem diagnoses and resolution support for all associated subsystems, including line monitoring, modem loop-back tests, LAN performance monitoring and terminal failure determination.
- Provide hardware and software installation and configuration support.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.69 Telecommunications Engineer I

Example of duties:

- Provide support in the translation of business requirements into telecommunications requirements, designs and orders.
- Provide in-depth engineering analysis of telecommunications alternatives for government agencies in support of their strategic modernization efforts.
- Provide telecommunications enhancement designs for medium and large-scale telecommunication infrastructures.
- Provide interface support to telecommunications end users, telecommunications operations personnel, and telecommunications strategic program management.
- Support telecommunications infrastructure using technology, and telecommunications engineering best practices; Transport Control Protocol / Internet Protocol (TCP/IP), routing protocols, LAN switching, Internet and Intranet systems, and Simple Network Management Protocol (SNMP) based network management systems.
- Lead design efforts that require in-depth technical knowledge of both wide area and local area communications.
- Analyze network performance with tools such as Sniffers, Concord Network Health, or Network Informant; network management tools such as Hewlett Packard Openview or Tivoli; the conduct of capacity planning and performance engineering; modeling and simulation tools such as COMNET III, Netmaker Mainstation, NetRule, or OPNET products.
- Perform comparative analysis of systems and designs based on merit and cost (in terms of capital and ongoing operations); and/or engineering economics (engineering-related cost benefit analysis).

Requirements:

- Bachelor's Degree plus 3-6 years of relevant experience

C.6.70 Telecommunications Engineer II

Example of duties:

- Manage the translation of business requirements into telecommunications requirements, designs and orders.
- Provide in-depth engineering analysis of telecommunications alternatives for government agencies in support of their strategic modernization efforts.
- Provide telecommunications enhancement designs for medium and large-scale telecommunication infrastructures.
- Provide interface support to telecommunications end users, telecommunications operations personnel, and telecommunications strategic program management.
- Support telecommunications infrastructure using technology, and telecommunications engineering best practices; Transport Control Protocol / Internet Protocol (TCP/IP), routing protocols, LAN switching, Internet and Intranet systems, and Simple Network Management Protocol (SNMP) based network management systems.
- Lead design efforts that require in-depth technical knowledge of both wide area and local area communications.
- Analyze network performance with tools such as Sniffers, Concord Network Health, or Network Informant; network management tools such as Hewlett Packard Openview or Tivoli; the conduct of capacity planning and performance engineering; modeling and simulation tools such as COMNET III, Netmaker Mainstation, NetRule, or OPNET products.
- Perform comparative analysis of systems and designs based on merit and cost (in terms of capital and ongoing operations); and/or engineering economics (engineering-related cost benefit analysis).
- May provide daily supervision and direction to support staff.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.71 Cost/Schedule Analyst I

Example of duties:

- Sets up cost control system, monitors and controls costs and schedules on contracts requiring validated cost schedule control system.
- Performs analyses and prepares reports in order to ensure that contracts are within negotiated and agreed-upon parameters and government cost control guidelines.
- Prepares budgets and schedules for contract work and performs and/or assists in financial analyses such as funding profiles, sales outlook, and variance analysis.

- Prepares program plans to ensure program requirements and statement of work are captured and scheduled.
- Performs schedule risk assessments to identify and mitigate program cost and scheduling risks.
- Ensures adequate funding availability by maintaining accurate records of expenditures, directing preparation of expenditure projections, and submitting timely requests for additional funding to the government.
- Incorporates contractual changes into control systems by staying aware of outstanding work against each contract in order to maintain realistic contract cost and schedule baselines.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.72 Cost/Schedule Analyst II

Example of duties:

- Sets up cost control system, monitors and controls costs and schedules on contracts requiring validated cost schedule control system.
- Performs analyses and prepares reports in order to ensure that contracts are within negotiated and agreed-upon parameters and government cost control guidelines.
- Prepares budgets and schedules for contract work and performs and/or assists in financial analyses such as funding profiles, sales outlook, and variance analysis.
- Prepares program plans to ensure program requirements and statement of work are captured and scheduled.
- Performs schedule risk assessments to identify and mitigate program cost and scheduling risks.
- Ensures adequate funding availability by maintaining accurate records of expenditures, directing preparation of expenditure projections, and submitting timely requests for additional funding to the government.
- Incorporates contractual changes into control systems by staying aware of outstanding work against each contract in order to maintain realistic contract cost and schedule baselines.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.73 Cost/Schedule Analyst III

Example of duties:

- Sets up cost control system, monitors and controls costs and schedules on contracts requiring validated cost schedule control system.
- Performs analyses and prepares reports in order to ensure that contracts are within negotiated and agreed-upon parameters and government cost control guidelines.

- Prepares budgets and schedules for contract work and performs and/or assists in financial analyses such as funding profiles, sales outlook, and variance analysis.
- Prepares program plans to ensure program requirements and statement of work are captured and scheduled.
- Performs schedule risk assessments to identify and mitigate program cost and scheduling risks.
- Ensures adequate funding availability by maintaining accurate records of expenditures, directing preparation of expenditure projections, and submitting timely requests for additional funding to the government.
- Incorporates contractual changes into control systems by staying aware of outstanding work against each contract in order to maintain realistic contract cost and schedule baselines.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.74 Cost/Schedule Analyst IV

Example of duties:

- Sets up cost control system, monitors and controls costs and schedules on contracts requiring validated cost schedule control system.
- Performs analyses and prepares reports in order to ensure that contracts are within negotiated and agreed-upon parameters and government cost control guidelines.
- Prepares budgets and schedules for contract work and performs and/or assists in financial analyses such as funding profiles, sales outlook, and variance analysis.
- Prepares program plans to ensure program requirements and statement of work are captured and scheduled.
- Performs schedule risk assessments to identify and mitigate program cost and scheduling risks.
- Ensures adequate funding availability by maintaining accurate records of expenditures, directing preparation of expenditure projections, and submitting timely requests for additional funding to the government.
- Incorporates contractual changes into control systems by staying aware of outstanding work against each contract in order to maintain realistic contract cost and schedule baselines.

Requirements:

- Bachelor's Degree plus 6-10 years of relevant experience

C.6.75 Project Scheduler SME

Example of duties:

- Master Scheduler and senior level project controller experience.
- Sets up cost control system, monitors and controls costs and schedules on contracts requiring validated cost schedule control system.
- Performs analyses and prepares reports in order to ensure that contracts are within negotiated and agreed-upon parameters and government cost control guidelines.
- Prepares budgets and schedules for contract work and performs and/or assists in financial analyses such as funding profiles, sales outlook, and variance analysis.
- Prepares program plans to ensure program requirements and statement of work are captured and scheduled.
- Performs schedule risk assessments to identify and mitigate program cost and scheduling risks.
- Ensures adequate funding availability by maintaining accurate records of expenditures, directing preparation of expenditure projections, and submitting timely requests for additional funding to the government.
- Incorporates contractual changes into control systems by staying aware of outstanding work against each contract in order to maintain realistic contract cost and schedule baselines.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience, most of which spent performing project scheduling and Earned Value Management (EVM) work
- Trained in Primavera P3 and Oracle P6, Microsoft Project, and Suretrak

C.6.76 Cost/Schedule Manager

Example of duties:

- Manages the set up of the cost control system, monitoring the control of costs and schedules on contracts requiring validated cost schedule control system.
- Responsible for coordinating subordinate employee recruitment, selection and training, performance assessment, work assignments, salary, and recognition/disciplinary actions.
- Directs the analyses and prepararation of reports in order to ensure that contracts are within negotiated and agreed-upon parameters and government cost control guidelines.
- Manages the preparation of budgets and schedules for contract work and performs and/or assists in financial analyses such as funding profiles, sales outlook, and variance analysis.
- Oversees program plans to ensure program requirements and statement of work are captured and scheduled.
- Ensures schedule risk assessments are performed to identify and mitigate program cost and scheduling risks.
- Ensures adequate funding availability by maintaining accurate records of expenditures, directing preparation of expenditure projections, and submitting timely requests for

additional funding to the government.

- Monitors contractual changes are incorporated into control systems by staying aware of outstanding work against each contract in order to maintain realistic contract cost and schedule baselines.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience, including experience acting in a managerial / team leader role

C.6.77 Electronic Data Interchange (EDI) Specialist

Example of duties:

- Analyze, design, and develop specifications for enhancements and extensions with Electronic Data Interchange (EDI) application interfaces and maps.
- Coordinate EDI testing and trading partner implementation initiatives.
- Provide support for EDI database analysis, design, and operations.
- Establish and maintain communications within organization and with partners.
- Conduct and manage product evaluations.
- Provide product installation, configuration, and training.
- Perform systems maintenance to update records, specifications, and operating procedures of partner systems.
- Maintain EDI account transaction activities.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.78 ERP Systems Analyst I

Example of duties:

- Analyzes, evaluates, modifies, configures, tests and implements enterprisewide purchased systems (e.g. SAP, PeopleSoft, etc.)
- Prepares application system specifications.
- Plans, implements and coordinates system upgrades, enhancements or maintenance.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.79 ERP Systems Analyst II

Example of duties:

- Analyzes, evaluates, modifies, configures, tests and implements enterprisewide purchased systems (e.g. SAP, PeopleSoft, etc.)
- Prepares application system specifications.

- Plans, implements and coordinates system upgrades, enhancements or maintenance.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.80 ERP Systems Analyst III

Example of duties:

- Analyzes, evaluates, modifies, configures, tests and implements enterprisewide purchased systems (e.g. SAP, PeopleSoft, etc.)
- Prepares application system specifications.
- Plans, implements and coordinates system upgrades, enhancements or maintenance.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.81 ERP Systems Analyst IV

Example of duties:

- Analyzes, evaluates, modifies, configures, tests and implements enterprisewide purchased systems (e.g. SAP, PeopleSoft, etc.)
- Prepares application system specifications.
- Plans, implements and coordinates system upgrades, enhancements or maintenance.

Requirements:

- Bachelor's Degree plus 6-8 years of relevant experience

C.6.82 ERP Systems Analyst V

Example of duties:

- Analyzes, evaluates, modifies, configures, tests and implements enterprisewide purchased systems (e.g. SAP, PeopleSoft, etc.)
- Prepares application system specifications.
- Plans, implements and coordinates system upgrades, enhancements or maintenance.

Requirements:

- Bachelor's Degree plus 8-10 years of relevant experience

C.6.83 ERP Systems Analyst SME

Example of duties:

- Analyzes, evaluates, modifies, configures, tests and implements enterprisewide purchased systems (e.g. SAP, PeopleSoft, etc.)
- Prepares application system specifications.

- Plans, implements and coordinates system upgrades, enhancements or maintenance.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.84 Oracle PeopleSoft SME

Example of duties:

- Support the NRC with Configuration Management in the upgrade of their PeopleSoft software and systems
- Experienced PeopleSoft Implementation specialist.

Requirements:

- Bachelor's Degree
- 15+ years of relevant experience, most of which spent working with PeopleSoft related product.

C.6.85 Junior Systems Analyst I

Example of duties:

- Performs a variety of activities in one or more of the following and/or related areas: personal computer applications training, data control and scheduling coordination, systems administration, data security administration, and associated fields

Requirements:

- Associate's Degree plus 0-2 years of relevant experience

C.6.86 Junior Systems Analyst II

Example of duties:

- Performs a variety of activities in one or more of the following and/or related areas: personal computer applications training, data control and scheduling coordination, systems administration, data security administration, and associated fields

Requirements:

- Associate's Degree plus 2-4 years of relevant experience

C.6.87 Junior Systems Analyst III

Example of duties:

- Performs a variety of activities in one or more of the following and/or related areas: personal computer applications training, data control and scheduling coordination, systems administration, data security administration, and associated fields

Requirements:

- Associate's Degree plus 4-6 years of relevant experience

C.6.88 Junior Systems Analyst IV

Example of duties:

- Performs a variety of activities in one or more of the following and/or related areas: personal computer applications training, data control and scheduling coordination, systems administration, data security administration, and associated fields

Requirements:

- Associate's Degree plus 6-8 years of relevant experience

C.6.89 Junior Systems Analyst V

Example of duties:

- Performs a variety of activities in one or more of the following and/or related areas: personal computer applications training, data control and scheduling coordination, systems administration, data security administration, and associated fields

Requirements:

- Associate's Degree plus 8+ years of relevant experience

C.6.90 Systems Analyst I

Example of duties:

- Designs, develops, programs, installs, implements, conducts research for, and maintains internal data processing computer systems and utilities, and/or for customers on a contract basis.
- Analyzes internal or external customers' needs, and determines equipment and software requirements for solutions to problems by means of automated systems; develops customized solutions to customer/user problems.
- Establishes system parameters and formats; ensures hardware/software compatibility; and coordinates and/or modifies user requirements in terms of existing and projected computer capacity and capabilities.
- May make programming changes as required to adapt or enhance existing or new programs and/or utilities.
- Maintains supplied software packages for internal users.
- Analyzes new hardware to determine its need or application in the existing or proposed system.
- Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements, and makes trade-off analyses.
- Develops general and detailed documentation describing system specifications and operating instructions.
- Revises existing systems and procedures to correct deficiencies and maintain more effective data handling, conversion, input/output requirements, and storage.

Requirements:

- Bachelor’s Degree plus 0-2 years of relevant experience

C.6.91 Systems Analyst II

Example of duties:

- Designs, develops, programs, installs, implements, conducts research for, and maintains internal data processing computer systems and utilities, and/or for customers on a contract basis.
- Analyzes internal or external customers' needs, and determines equipment and software requirements for solutions to problems by means of automated systems; develops customized solutions to customer/user problems.
- Establishes system parameters and formats; ensures hardware/software compatibility; and coordinates and/or modifies user requirements in terms of existing and projected computer capacity and capabilities.
- May make programming changes as required to adapt or enhance existing or new programs and/or utilities.
- Maintains supplied software packages for internal users.
- Analyzes new hardware to determine its need or application in the existing or proposed system.
- Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements, and makes trade-off analyses.
- Develops general and detailed documentation describing system specifications and operating instructions.
- Revises existing systems and procedures to correct deficiencies and maintain more effective data handling, conversion, input/output requirements, and storage.

Requirements:

- Bachelor’s Degree plus 2-4 years of relevant experience

C.6.92 Systems Analyst III

Example of duties:

- Designs, develops, programs, installs, implements, conducts research for, and maintains internal data processing computer systems and utilities, and/or for customers on a contract basis.
- Analyzes internal or external customers' needs, and determines equipment and software requirements for solutions to problems by means of automated systems; develops customized solutions to customer/user problems.
- Establishes system parameters and formats; ensures hardware/software compatibility; and coordinates and/or modifies user requirements in terms of existing and projected computer capacity and capabilities.

- May make programming changes as required to adapt or enhance existing or new programs and/or utilities.
- Maintains supplied software packages for internal users.
- Analyzes new hardware to determine its need or application in the existing or proposed system.
- Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements, and makes trade-off analyses.
- Develops general and detailed documentation describing system specifications and operating instructions.
- Revises existing systems and procedures to correct deficiencies and maintain more effective data handling, conversion, input/output requirements, and storage.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.93 Systems Analyst IV

Example of duties:

- Designs, develops, programs, installs, implements, conducts research for, and maintains internal data processing computer systems and utilities, and/or for customers on a contract basis.
- Analyzes internal or external customers' needs, and determines equipment and software requirements for solutions to problems by means of automated systems; develops customized solutions to customer/user problems.
- Establishes system parameters and formats; ensures hardware/software compatibility; and coordinates and/or modifies user requirements in terms of existing and projected computer capacity and capabilities.
- May make programming changes as required to adapt or enhance existing or new programs and/or utilities.
- Maintains supplied software packages for internal users.
- Analyzes new hardware to determine its need or application in the existing or proposed system.
- Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements, and makes trade-off analyses.
- Develops general and detailed documentation describing system specifications and operating instructions.
- Revises existing systems and procedures to correct deficiencies and maintain more effective data handling, conversion, input/output requirements, and storage.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.94 Management Analyst I

Example of duties:

- Provide analytical consultative services required to administer programs throughout all phases of business requirements analysis, software design, system and performance testing, and implementation.
- Analyze and review budget, schedule, and other program resources.
- Identify resource shortfalls and make corrective recommendations.
- Participate in analysis sessions to provide program requirements.
- Review the business and system, software and system integration requirements to ensure the requirements meet the program needs.
- Consider alternatives and develop recommendations. Identify, communicate and resolve risks.
- Identify and resolve issues to eliminate or mitigate the occurrence of consequences that may impact the success of the project.
- Research and analyze resource material.
- Monitor system tests; reviews test results; identify project issues.

Requirements:

- Bachelor's Degree plus 0-3 years of relevant experience

C.6.95 Management Analyst II

Example of duties:

- Provide analytical consultative services required to administer programs throughout all phases of business requirements analysis, software design, system and performance testing, and implementation.
- Analyze and review budget, schedule, and other program resources.
- Identify resource shortfalls and make corrective recommendations.
- Participate in analysis sessions to provide program requirements.
- Review the business and system, software and system integration requirements to ensure the requirements meet the program needs.
- Consider alternatives and develop recommendations. Identify, communicate and resolve risks.
- Identify and resolve issues to eliminate or mitigate the occurrence of consequences that may impact the success of the project.
- Research and analyze resource material.

- Monitor system tests; reviews test results; identify project issues.

Requirements:

- Bachelor's Degree plus 3-6 years of relevant experience

C.6.96 Management Analyst III

Example of duties:

- Provide analytical consultative services required to administer programs throughout all phases of business requirements analysis, software design, system and performance testing, and implementation.
- Analyze and review budget, schedule, and other program resources.
- Identify resource shortfalls and make corrective recommendations.
- Participate in analysis sessions to provide program requirements.
- Review the business and system, software and system integration requirements to ensure the requirements meet the program needs.
- Consider alternatives and develop recommendations. Identify, communicate and resolve risks.
- Identify and resolve issues to eliminate or mitigate the occurrence of consequences that may impact the success of the project.
- Research and analyze resource material.
- Monitor system tests; reviews test results; identify project issues.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.97 Business Analyst I

Example of duties:

- Provide expertise in business process and system analysis, design, improvement, and implementation efforts and in translating business process needs into technical requirements.
- Provide expertise in change management and training support.
- Provide organizational and strategic planning for a wide variety of technical and functional environments.
- Provide expertise in, but not limited to, Configuration Management, Strategic Planning, Knowledge Management, Business Analysis and Technical Analysis.

Requirements:

- Bachelor's Degree plus 0-3 years of relevant experience

C.6.98 Business Analyst II

Example of duties:

- Assist in applying common best practices for the industry to the customer using a knowledge base to create conceptual business models and to identify relevant issues and considerations in selecting application software packages.
- Assess the operational and functional baseline of an organization and its organizational components, and help to define the direction and strategy for an engagement while ensuring the organizational needs are being addressed.
- Typical areas addressed include Human Resources, Finance, Supply, and operations. Identify information technology inadequacies and/or deficiencies that affect the functional area's ability to support/meet organizational goals.
- Support the development of functional area strategies for enhanced IT.

Requirements:

- Bachelor's Degree plus 3-6 years of relevant experience

C.6.99 Business Analyst III

Example of duties:

- Assist in applying common best practices for the industry to the customer using a knowledge base to create conceptual business models and to identify relevant issues and considerations in selecting application software packages.
- Assess the operational and functional baseline of an organization and its organizational components, and help to define the direction and strategy for an engagement while ensuring the organizational needs are being addressed.
- Typical areas addressed include Human Resources, Finance, Supply, and operations. Identify information technology inadequacies and/or deficiencies that affect the functional area's ability to support/meet organizational goals.
- Generate functional area strategies for enhanced IT operations in a cross-functional area mode throughout the organization.
- Participate in account strategy sessions, strategic assessments and design reviews to validate enterprise approach and associated work products, such as ERP implementations coordinating the resolution of highly complex problems and tasks.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.100 Information Systems Training Specialist

Example of duties:

- Provide support for coordinating, developing, and delivering computer-related training to the user community.
- Provide second level support and coordinate training with help desks.
- Provide standards, services, and guidance on IT related training programs that are

designed to enable government agency personnel to use information technologies and systems more productively.

- Services include the development, delivery, and/or coordination of training courses and materials that address specific agency needs.
- Possess thorough knowledge of appropriate hardware and software (ex. - PCs, Microsoft (MS) Windows, MS Office, and applications such as from SAP and Peoplesoft).

Requirements:

- Bachelor's Degree
- 5+ years of relevant experience demonstrating understanding of computer functions, related technical terminology and how they are applied in everyday business situations.
- Exceptional interpersonal skills
- Superior oral and written communication skills

C.6.101 Communications Software Specialist

Example of duties:

- Analyze network and computer communications software characteristics and recommend software procurement, removals, and modifications.
- Add, delete, and modify as required, host, terminal, and network devices in light of discerned software needs/problems.
- Assist and coordinate with communications network specialists in the area of communications software.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.102 Graphical User Interface (GUI) Designer

Example of duties:

- Provide specialized expertise in the design and layout of graphical user interfaces, particularly, screen layouts and functionality for client-server applications (e.g. Microsoft Windows presentation screens).
- Conduct studies, testing and evaluation of screen prototypes for functionality, ease of use, efficiency, and accuracy.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.103 Software Engineer I

Example of duties:

- Plans, conducts, and coordinates programming application activities.

- Writes business applications computer software that contains logical and mathematical solutions to business problems or questions.
- Develops statements of problems, designs systems and programs, and writes programs in computer language for solution by means of data processing equipment.
- Applies knowledge of computer hardware and software, subject matter to be programmed in business applications, information processing techniques used, and information gathered from system users to develop software.
- Corrects program errors, prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.104 Software Engineer II

Example of duties:

- Plans, conducts, and coordinates programming application activities.
- Writes business applications computer software that contains logical and mathematical solutions to business problems or questions.
- Develops statements of problems, designs systems and programs, and writes programs in computer language for solution by means of data processing equipment.
- Applies knowledge of computer hardware and software, subject matter to be programmed in business applications, information processing techniques used, and information gathered from system users to develop software.
- Corrects program errors, prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.105 Software Engineer III

Example of duties:

- Plans, conducts, and coordinates programming application activities.
- Writes business applications computer software that contains logical and mathematical solutions to business problems or questions.
- Develops statements of problems, designs systems and programs, and writes programs in computer language for solution by means of data processing equipment.
- Applies knowledge of computer hardware and software, subject matter to be programmed

in business applications, information processing techniques used, and information gathered from system users to develop software.

- Corrects program errors, prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.106 Software Engineer IV

Example of duties:

- Plans, conducts, and coordinates programming application activities.
- Writes business applications computer software that contains logical and mathematical solutions to business problems or questions.
- Develops statements of problems, designs systems and programs, and writes programs in computer language for solution by means of data processing equipment.
- Applies knowledge of computer hardware and software, subject matter to be programmed in business applications, information processing techniques used, and information gathered from system users to develop software.
- Corrects program errors, prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.107 Software Engineering Manager I

Example of duties:

- Manages software development activities.
- Responsible for coordinating subordinate employee recruitment, selection and training, performance assessment, work assignments, salary, and recognition/disciplinary actions.
- Oversees the design, development, documentation, and testing of software that contains logical and mathematical solutions to business/mission problems or questions in computer language for solutions by means of data processing equipment.
- Applies the appropriate standards, processes, procedures, and tools throughout the development life cycle.
- Applies knowledge of computer hardware and software, subject matter to be programmed in business/mission applications, information processing techniques used, and information gathered from system users to develop software.

- Ensures software standards are met.

Requirements:

- Bachelor's Degree plus 8-10 years of relevant experience

C.6.108 Software Engineering Manager II

Example of duties:

- Manages software development activities.
- Responsible for coordinating subordinate employee recruitment, selection and training, performance assessment, work assignments, salary, and recognition/disciplinary actions.
- Oversees the design, development, documentation, and testing of software that contains logical and mathematical solutions to business/mission problems or questions in computer language for solutions by means of data processing equipment.
- Applies the appropriate standards, processes, procedures, and tools throughout the development life cycle.
- Applies knowledge of computer hardware and software, subject matter to be programmed in business/mission applications, information processing techniques used, and information gathered from system users to develop software.
- Ensures software standards are met.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

C.6.109 Application Programmer Analyst I

Example of duties:

- Builds and codes applications and/or modules using languages such as C++, visual basic, ABAP, JAVA, XTML, etc.
- Provides patches and upgrades to existing systems.
- May design graphical user interface (GUI) to meet the specific needs of users.
- Prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.
- May build add-on modules using application program language.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.110 Application Programmer Analyst II

Example of duties:

- Builds and codes applications and/or modules using languages such as C++, visual basic, ABAP, JAVA, XTML, etc.

- Provides patches and upgrades to existing systems.
- May design graphical user interface (GUI) to meet the specific needs of users.
- Prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.
- May build add-on modules using application program language.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.111 Application Programmer Analyst III

Example of duties:

- Builds and codes applications and/or modules using languages such as C++, visual basic, ABAP, JAVA, XTML, etc.
- Provides patches and upgrades to existing systems.
- May design graphical user interface (GUI) to meet the specific needs of users.
- Prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.
- May build add-on modules using application program language.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.112 Application Programmer Analyst IV

Example of duties:

- Builds and codes applications and/or modules using languages such as C++, visual basic, ABAP, JAVA, XTML, etc.
- Provides patches and upgrades to existing systems.
- May design graphical user interface (GUI) to meet the specific needs of users.
- Prepares operating instructions, compiles documentation of program development, and analyzes system capabilities to resolve questions of program intent, output requirements, input data acquisition, programming techniques, and controls.
- May build add-on modules using application program language.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.113 Test Engineer I

Example of duties:

- Designs, develops, and implements testing methods and equipment.
- Plans and arranges the labor, schedules, and equipment required for testing and evaluating standard and special devices.
- Provides test area with parameters for sample testing and specifies tests to be performed.
- Compiles data and defines changes required in testing equipment, testing procedures, manufacturing processes, or new testing requirements.
- Responsible for testing all customer samples and for special tests that cannot be performed in the test area.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.114 Test Engineer II

Example of duties:

- Designs, develops, and implements testing methods and equipment.
- Plans and arranges the labor, schedules, and equipment required for testing and evaluating standard and special devices.
- Provides test area with parameters for sample testing and specifies tests to be performed.
- Compiles data and defines changes required in testing equipment, testing procedures, manufacturing processes, or new testing requirements.
- Responsible for testing all customer samples and for special tests that cannot be performed in the test area.

Requirements:

- Bachelor's Degree plus 2+ years of relevant experience

C.6.115 Software Quality Engineer I

Example of duties:

- Develops, modifies, applies, and maintains standards for software quality operating methods, processes, systems and procedures.
- Conducts software inspection, testing, verification and validation. Implements software development and maintenance processes and methods.
- Ensures measures meet acceptable reliability standards.
- Develops overall operating criteria to ensure implementation of the software quality program according to project, process and contract requirements and objectives.
- Ensures that project and process control documentation are compliant with requirements, objectives and/or contract.
- Reviews software design, change specifications, and plans against contractual and/or process requirements.

- Reviews include applicable specifications, materials, tools, techniques, and methodologies.
- Performs or directs verification of software requirement allocations, traceability, and testability.

Requirements:

- Bachelor's Degree plus 0-2 years of relevant experience

C.6.116 Software Quality Engineer II

Example of duties:

- Develops, modifies, applies, and maintains standards for software quality operating methods, processes, systems and procedures.
- Conducts software inspection, testing, verification and validation. Implements software development and maintenance processes and methods.
- Ensures measures meet acceptable reliability standards.
- Develops overall operating criteria to ensure implementation of the software quality program according to project, process and contract requirements and objectives.
- Ensures that project and process control documentation are compliant with requirements, objectives and/or contract.
- Reviews software design, change specifications, and plans against contractual and/or process requirements.
- Reviews include applicable specifications, materials, tools, techniques, and methodologies.
- Performs or directs verification of software requirement allocations, traceability, and testability.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.117 Software Quality Engineer III

Example of duties:

- Develops, modifies, applies, and maintains standards for software quality operating methods, processes, systems and procedures.
- Conducts software inspection, testing, verification and validation. Implements software development and maintenance processes and methods.
- Ensures measures meet acceptable reliability standards.
- Develops overall operating criteria to ensure implementation of the software quality program according to project, process and contract requirements and objectives.
- Ensures that project and process control documentation are compliant with requirements, objectives and/or contract.

- Reviews software design, change specifications, and plans against contractual and/or process requirements.
- Reviews include applicable specifications, materials, tools, techniques, and methodologies.
- Performs or directs verification of software requirement allocations, traceability, and testability.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.118 Quality Assurance Manager

Example of duties:

- Establish and maintain a process for evaluating software and associated documentation.
- Determine the resources required for quality control.
- Maintain the level of quality throughout the software life cycle.
- Conduct formal and informal reviews at pre-determined points throughout the development life cycle.
- Provide daily supervision and direction to support staff.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience working with increasingly complex software quality subject matter

C.6.119 Graphics Specialist

Example of duties:

- Conceptualize, design, and develop a wide variety of information materials (technical, promotional, informational), such as forms, labels, brochures, meeting and conference handouts, slides, posters, and other presentation aids.
- Design other visuals such as logos, mastheads, and illustrations for articles in technical manuals, health journals, and other publications using advanced desktop publishing, page layout, and/or typesetting software to design and develop high qualify textual and graphic compositions that communicate complex technical information.
- Develop systems for scheduling and tracking requests for graphics/artwork to insure timely and efficient completion of all work products.

Requirements:

- Bachelor's Degree plus 5+ years of relevant experience

C.6.120 Website Designer I

Example of duties:

- Designs, develops, troubleshoots, debugs, configures and maintains website(s) for internal and external communications for the company and/or for external customers and

clients.

- Ensures website(s) is available to the desired audience with appropriate links and security.
- Develops, assesses and communicates website usage and security policies and procedures.
- Designs web page layout, graphics, color schemes and infrastructure to maintain a cohesive website based on the organization's communications strategies and goals.
- Researches and evaluates new related technologies.

Requirements:

- Bachelor's Degree plus 2-4 years of relevant experience

C.6.121 Website Designer II

Example of duties:

- Designs, develops, troubleshoots, debugs, configures and maintains website(s) for internal and external communications for the company and/or for external customers and clients.
- Ensures website(s) is available to the desired audience with appropriate links and security.
- Develops, assesses and communicates website usage and security policies and procedures.
- Designs web page layout, graphics, color schemes and infrastructure to maintain a cohesive website based on the organization's communications strategies and goals.
- Researches and evaluates new related technologies.

Requirements:

- Bachelor's Degree plus 4-6 years of relevant experience

C.6.122 Website Designer III

Example of duties:

- Designs, develops, troubleshoots, debugs, configures and maintains website(s) for internal and external communications for the company and/or for external customers and clients.
- Ensures website(s) is available to the desired audience with appropriate links and security.
- Develops, assesses and communicates website usage and security policies and procedures.
- Designs web page layout, graphics, color schemes and infrastructure to maintain a cohesive website based on the organization's communications strategies and goals.
- Researches and evaluates new related technologies.

Requirements:

- Bachelor's Degree plus 6+ years of relevant experience

C.6.123 Web Software Developer

Example of duties:

- Provide support to develop Web based applications including on line customer service to transform government agencies to be able to deliver their services on line.
- Provide support in developing the site concept, interface design, and architecture of the web-site.
- Provide support for the implementation of interfaces to applications.

Requirements:

- Bachelor's Degree
- 5+ years of experience demonstrating working knowledge and experience working with Java, Active Server Pages (ASPs), JavaScript, Visual Basic, Access, HTML, DBMS (ex. Oracle, Sybase, SQL Server, etc.), Drupal, and SQL.

C.6.124 Web Project Manager

Example of duties:

- Provide support in managing the development of agency Web sites.
- Lead team of Content Administrators, Software Developers and Designers.
- Preference for project management skills and Web development skills.
- Provide leadership to a team to gather/analyze client requirements, write/edit web copy, work with internal/external resources on design, coordinate with IT Services on development, and work with Legal/Regulatory on content approvals.
- Coordinate/document all aspects of the project.
- Develop/manage client request/review process.
- Track all requests/changes.
- Adhere to a project timeline.

Requirements:

- Bachelor's Degree plus 10+ years of relevant experience

SECTION D: PACKAGING AND MARKING

D.1 Payment of Postage and Fees

All postage and fees related to the submission of information, including forms, reports, etc., to the CO, the COR, or the person(s) designated to receive, shall be the responsibility of the Contractor.

D.2 Packing for Domestic Shipment

Material shall be packed for shipment in such a manner that will ensure acceptance by common carriers and safe delivery at destination. Containers and closures shall comply with the Interstate Commerce Commission regulations, Uniform Freight Classification rules, or regulations of other carriers as applicable to the mode of transportation.

D.3 Marking Deliverables

The BPA and the BPA Call number shall be placed on, or adjacent to, all exterior mailing or shipping labels of deliverable items called for by the BPA and/or BPA Calls, except for reports.

Mark deliverables for the BPA COR or the specific BPA Call COR. Additional deliverable markings may be outlined in awarded work packages.

SECTION E: INSPECTION AND ACCEPTANCE

Inspection and acceptance of the deliverable items to be furnished hereunder shall be made by the NRC Contracting Officer's Representative (COR) at the destination, accordance with FAR 52.247-34 - F.o.b. Destination.

Contract Deliverables:

See statement of work for BPA deliverables.

(End of Clause)

SECTION F: DELIVERIES AND PERFORMANCE

F.1 Period of Performance

NRC will establish a period of performance for the BPA effective as follows:

- Base Period (approximately 3 years): Date of Award to 9/29/2019
- Option Period 1 (3 years): 09/30/2019 to 9/29/2022

Each individual BPA Call under the BPA will have its own period of performance. BPA Calls may contain options, if included at initial issuance of the BPA Call.

The Prime/CTA Contractor shall have an active GSA Schedule 70 at the time of proposal submission. At any time, if the Prime's/CTA's GSA Schedule 70 contract is cancelled or not renewed, the Prime's/CTA's BPA will be cancelled at the end of any current task order period and no modifications to existing orders will be allowed. As per FAR 8.405-3(d)(3), the BPA may be established with Contractor(s) even if the BPA extends beyond the Contractor(s)'s current term (five year period of performance) of their GSA Schedule Contract, so long as there are option periods in the Contractor(s)'s GSA Schedule Contract that, if exercised, will cover this BPA's total period of performance. BPAs will be reviewed per FAR 8.405-3(e) each year.

F.2 Place of Performance

Work shall be primarily performed in the Washington, D.C. Metro area, and at the NRC Headquarters and Regional Offices. Government space may be assigned for this support. The hours, exact location, and assignment of government space shall be identified in each individual

BPA Call; however, unless explicitly stated in the BPA Call, telework shall be supported at the Government Site Rate. Contractor meetings shall be conducted at the NRC Headquarters buildings unless specified otherwise.

If travel is required based on individual BPA Calls, the Government will negotiate travel expenses and authorize the travel in writing prior to the occurrence of travel. The Government will reimburse the Contractor for all travel expenses in accordance with the Federal Travel Regulation (FTR). Travel expenses shall be submitted upon completion of each authorized travel occurrence.

Local travel is not reimbursable. Local travel shall be considered within fifty (50) miles of the NRC Headquarters and within fifty (50) miles from each Regional Office Buildings.

Information on the NRC locations can be found on the website at http://www.nrc.gov/aboutnrc/locations.html. The NRC has its Headquarters in Rockville, Maryland, and a number of other offices around the United States as follows:

- The three-building headquarters complex (http://www.nrc.gov/aboutnrc/locations/hq.html) in Rockville, Maryland, houses the NRC headquarters staff, contractors, and our Public Document Room (http://www.nrc.gov/reading-rm/pdr.html). There are approximately 4,300 ITI users at this location.

- The Region I Office (http://www.nrc.gov/about-nrc/locations/region1.html) in King of Prussia, Pennsylvania, oversees the NRC's regulatory activities in the northeastern United States. There are approximately 200 ITI users at this location.
- The Region II Office (http://www.nrc.gov/about-nrc/locations/region2.html) in Atlanta, Georgia, oversees the NRC's regulatory activities in the southeastern United States. There are approximately 200 ITI users at this location.
- The Region III Office (http://www.nrc.gov/about-nrc/locations/region3.html) in Lisle, Illinois, oversees the NRC's regulatory activities in the northern mid-western United States. There are approximately 200 ITI users at this location.
- The Region IV Office (http://www.nrc.gov/about-nrc/locations/region4.html) in Arlington, Texas, oversees the NRC's regulatory activities in the western and southern Midwestern United States. There are approximately 200 ITI users at this location.
- The NRC Technical Training Center (http://www.nrc.gov/aboutnrc/locations/training.html) in Chattanooga, Tennessee, provides training for the staff in various technical disciplines associated with the regulation of nuclear materials and facilities. There are approximately 25 ITI users at this location.
- The NRC also has onsite inspectors permanently stationed at each reactor licensee that it regulates (http://www.nrc.gov/info-finder/reactor/). These Resident Inspectors require broadband access to the NRC network and use applications that are hosted at NRC Headquarters, the Regional Offices, and on the internet. There are approximately 100 locations that must be supported.

The NRC also supports an application support facility in Rockville, Maryland. This facility is provided by an application development support contractor. There are approximately 75 ITI users at this location.

F.3 Hours of Operation

Currently, normal working hours at NRC Headquarters are 6am-6pm Eastern Standard Time (EST) /Eastern Daylight Time (EDT) Monday thru Friday excluding Federal Holidays. NRC Regional Offices in different time zones generally have normal working hours of 6am – 6pm local time. Contractor personnel are expected to conform to NRC's normal operating hours, with exceptions for those functions which require 24 x 7 x 365 support. Additional exceptions to normal working hours would be for maintenance and production changes, made outside of normal working hours so as to not disrupt agency operations.

F.4 Federal Holidays

Federal Holidays are located at https://www.opm.gov/policy-data-oversight/snow-dismissal-procedures/federal-holidays/#url=2016

F.5 BPA Deliverables

Deliverable	Due Date	SOW Section	Due To
Annual Small Business Goal Report	Annually on August 10th	G.3	BPA's Contracting Officer

Quarterly Status Reports	Quarterly by 5 PM ET on • January 10th; • April 10th; • July 10th; and • October 10th	G.4	BPA's Contracting Officer and COR
BPA Quality Control Plan	Quarterly by 5 PM ET on • January 10th; • April 10th; • July 10th; and • October 10th	H.1.1	BPA's Contracting Officer and COR
Document of CMMI or ISO process management approach	Ongoing	F.5.1	BPA's Contracting Officer and COR
Ownership and Location of Data	Ongoing	F.6	BPA's Contracting Officer and COR

SECTION G: CONTRACT ADMINISTRATION DATA

G.1 Subcontractors vs. Contractor Teaming Arrangement (CTA)

The terms Subcontractor and Teaming Partner are not interchangeable in this SOW. Under a Contractor Team Arrangement (CTA), two (2) or more GSA Schedule contractors work together to meet ordering activity needs. By complementing each other's capabilities, the team offers a total solution to the ordering activity's requirement. The CTA differs from a relationship between a Prime Contractor and Subcontractor in that all members of the team are equal parties to the contract. Important differences are detailed below:

Contractor Team Arrangement (CTA)	Prime Contractor / Subcontractor Agreement
Each team member must have a GSA Schedule contract.	Only the prime contractor must have a GSA Schedule contract.
Each team member is responsible for duties addressed in the CTA document.	The prime contractor cannot delegate responsibility for performance to subcontractors.
Each team member has privity of contract with the government and can interact directly with the government.	Only the prime contractor has privity of contract with the government and can interact with the government. The prime contractor is responsible for its subcontracting activities. (Ordering activities are encouraged to specify in the Request for Quotation (RFQ) that the use of subcontractors requires prior approval by the ordering activities.)
The ordering activity is invoiced at each team member's unit prices or hourly rates as agreed in the task or delivery order or GSA Schedule BPA.	The ordering activity is invoiced in accordance with the prime contractor's GSA Schedule contract, including any applicable price reductions.
Total solutions, otherwise impossible under individual GSA Schedule contracts, can be put together quickly and easily.	The prime contractor is limited to the supplies and/or services awarded on its GSA Schedule contract.

If proposing a CTA, Contractors shall identify one (1) Teaming Partner as the Lead Teaming Partner. This distinction is necessary due to NRC's acquisition software only being able to identify one (1) Contractor name on the BPA establishment documentation.

Per www.gsa.gov/contractorteamarrangements and the chart above, all Teaming Partners shall have a GSA Schedule 70 Contract. Subcontractors are not required to have a GSA Schedule 70 Contract. Only the Prime Contractor or the Lead Teaming Partner is required to have the NAICS 541519. GSA will allow large and small businesses to cross team (i.e., a large business subcontracts to a small business and that same small business subcontracts to the large business, which results in two different quote submissions).

NRC will compete and issue BPA Calls for specific requirements once the BPA is established. BPA Calls issued against this BPA may come from other NRC Regions or Offices outside of OCIO and/or Headquarters.

The following partnership(s), joint venture(s) and/or subcontractor(s) have been approved under the BPA. The Contractor shall not propose any additional CTAs after the establishment of the BPA. However, the Contractor may utilize additional subcontractors at the BPA Call level as long as they are listed in their BPA Call proposal and provide a signed subcontracting agreement at time of submission. The proposed partner(s) and/or current subcontractor(s) are:

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

G.2 Subcontracting Plans

Each large business BPA Call holder shall document annually their plan to utilize small businesses to perform at least 40% of the dollars issued through their prime BPA Calls.

G.3 Annual Small Business Goal Report

Each large business BPA Call Holder shall submit an Annual Small Business Goal Report to the CO by August 10th of each Government fiscal year the BPA exists. This report shall account for all small business goals that have occurred during the current Government fiscal year (October 1st- July 31st) and outline the anticipated goals for the remaining portion of the fiscal year (August 1st- September 30th). If the large business fails to meet the designated 40% small business goals, the CO could cancel the BPA Call Holder's BPA. The Annual Small Business Goal Report will be a combined report reflecting all awarded BPA calls.

G.4 Quarterly BPA Reports and Reviews

Quarterly Status Reviews shall be held for each BPA Call. The CO/COR shall determine the method and date of reviews after the BPA is established. Most likely the review will be an hour long meeting to discuss the Quarterly BPA Report and any issues of the BPA or BPA Calls.

The BPA Holder's Program Manager shall provide all Quarterly Status Reports, via email, to the CO and COR by 5:00PM ET on the following dates:

- January 10th;
- April 10th;

- July 10th; and
- October 10th.

The BPA quarterly status reports shall include:

- Progress for each BPA Call;
- Updates and Changes;
- Users/Projects involved with each BPA Call's initiatives;
- Lessons Learned;
- Subcontracting/ Small Business Reporting; and
- Plan of Action and Milestones (POA&M).

SECTION H: SPECIAL CONTRACT REQUIREMENTS

H.1 CMMI Level III / ISO 9001:2008 Compliance

H.1.1 Quality Control

This BPA requires the Contractor to maintain a thorough quality control program in compliance with Capability Maturity Model® Integration (CMMI) Level III or International Organization of Standards (ISO) 9001:2008 with the aim of preventing, identifying, and correcting deficiencies in the quality of both development and services provided to the Government. The Contractor shall have proof of their appraised CMMI or ISO level.

As part of the Quality Control Program, the Contractor shall develop a BPA Quality Control Plan (QCP) that describes the Contractor's procedures for monitoring the overall performance on the BPA, as well as, QCPs for individual BPA Calls as specified. At a minimum, the QCPs shall include the following.

- The practices and protocols for compliance with CMMI Level III or ISO 9001:2008 to be utilized at NRC.
- A description of the practices, protocols, and inspection system to cover all services listed in the SOW. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis and frequency of these inspections.
- A description of follow-up procedures to ensure that deficiencies are corrected and the time frames involved in correcting these deficiencies.
- A description of the records to be kept to document inspections and corrective or preventive actions taken.

The records of inspections shall be kept and made available to the Government, when requested, throughout the performance period, and for the period after completion, until final settlement of any claims under this agreement.

H.1.2 Standards (CMMI / ISO)

The requirement for this BPA shall be performed under conditions of process management to ensure the quality of deliverables and services are managed at every stage of development in conformance with either ISO 9001:2008 or CMMI Level III. The Contractor shall describe and document their CMMI or ISO process management approach throughout the software/systems development life cycle and IT services processes demonstrating the utilization of process management through either CMMI level III or ISO 9001:2008.

H.2 Ownership and Location of Data

The NRC will, at all times, retain the ownership of any data provided by the NRC to the contractor during the period of performance of the GLINDA Contract or data that has been created under any and all BPA Calls. At the expiration of the contract and at any point during the contract, the contractor shall provide the NRC with all data in an easily portable format that maintains any relational information. All data must be maintained and stored within the continental United States and only in facilities that have received appropriate FedRamp Certification.

SECTION I: CONTRACT CLAUSES

I.1 Federal Acquisition Regulation Clauses

52.217-8 OPTION TO EXTEND SERVICES

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 before expiration of the BPA.

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MARCH 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor before the BPA expires provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 10 days before the BPA expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended BPA shall be considered to include this option clause.

(c) The total duration of this BPA including the exercise of any options under this clause, shall not exceed 6 years.

52.204-15 SERVICE CONTRACT REPORTING REQUIREMENTS FOR INDEFINITE-DELIVERY CONTRACTS.

Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Jan 2014)

(a) Definitions.

“First-tier subcontract” means a subcontract awarded directly by the Contractor for the purpose of acquiring supplies or services (including construction) for performance of a prime contract. It does not include the Contractor’s supplier agreements with vendors, such as long-term arrangements for materials or supplies that benefit multiple contracts and/or the costs of which are normally applied to a Contractor’s general and administrative expenses or indirect costs.

(b) The Contractor shall report, in accordance with paragraphs (c) and (d) of this clause, annually by October 31, for services performed during the preceding Government fiscal year (October 1-

September 30) under this contract for orders that exceed the thresholds established in 4.1703(a)(2).

(c) The Contractor shall report the following information:

(1) Contract number and order number.

(2) The total dollar amount invoiced for services performed during the previous Government fiscal year under the order.

(3) The number of Contractor direct labor hours expended on the services performed during the previous Government fiscal year.

(4) Data reported by subcontractors under paragraph (f) of this clause.

(d) The information required in paragraph (c) of this clause shall be submitted via the internet at www.sam.gov. (See SAM User Guide). If the Contractor fails to submit the report in a timely manner, the Contracting Officer will exercise appropriate contractual remedies. In addition, the Contracting Officer will make the Contractor's failure to comply with the reporting requirements a part of the Contractor's performance information under FAR subpart 42.15.

(e) Agencies will review Contractor reported information for reasonableness and consistency with available contract information. In the event the agency believes that revisions to the Contractor reported information are warranted, the agency will notify the Contractor no later than November 15. By November 30, the Contractor shall revise the report, or document its rationale for the agency.

(f)(1) The Contractor shall require each first-tier subcontractor providing services under this contract, with subcontract(s) each valued at or above the thresholds set forth in 4.1703(a)(2), to provide the following detailed information to the Contractor in sufficient time to submit the report:

(i) Subcontract number (including subcontractor name and DUNS number), and

(ii) The number of first-tier subcontractor direct-labor hours expended on the services performed during the previous Government fiscal year.

(2) The Contractor shall advise the subcontractor that the information will be made available to the public as required by section 743 of Division C of the Consolidated Appropriations Act, 2010.

I.2 NRC Local Clauses

NRCH020 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (SEP 2013)

The Contractor shall ensure that all its employees, subcontractor employees or consultants who are assigned to perform the work herein for contract performance for periods of more than 30 calendar days at NRC facilities, are approved by the NRC for unescorted NRC building access.

The Contractor shall conduct a preliminary federal facilities security screening interview or review for each of its employees, subcontractor employees, and consultants and submit to the NRC only the names of candidates for contract performance that have a reasonable probability of obtaining approval necessary for access to NRC's federal facilities. The Contractor shall pre-screen its applicants for the following

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) years.

The Contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the applicant verify the pre-screening record or review, sign and date it. Two (2) copies of the pre-screening signed record or review shall be supplied to the Division of Facilities and Security, Personnel Security Branch (DFS/PSB) with the Contractor employee's completed building access application package.

The Contractor shall further ensure that its employees, any subcontractor employees and consultants complete all building access security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed records of the Contractor's signed pre-screening record or review and building access security applications (submitted for candidates that have a reasonable probability of obtaining the level of access authorization necessary for access to NRC's facilities) is a contract requirement. Failure of the Contractor to comply with this contract administration requirement may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of cancellation or termination, the NRC may select another firm for contract award.

A Contractor, subcontractor employee or consultant shall not have access to NRC facilities until he/she is approved by DFS/PSB. Temporary access may be approved based on a favorable NRC review and discretionary determination of their building access security forms. Final building access will be approved based on favorably adjudicated checks by the Government. However, temporary access approval will be revoked and the Contractor's employee may subsequently be denied access in the event the employee's investigation cannot be favorably determined by the NRC. Such employee will not be authorized to work under any NRC contract requiring building access without the approval of DFS/PSB. When an individual receives final access, the individual will be subject to a review or reinvestigation every five (5) or ten (10) years, depending on their job responsibilities at the NRC.

The Government shall have and exercise full and complete control and discretion over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. Individuals performing work under this contract at NRC facilities for a period of more than 30 calendar days shall be required to complete and submit to the Contractor representative an acceptable OPM Standard Form 85 (Questionnaire for Non-Sensitive Positions), and two (2) FD 258 (Fingerprint Charts). Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than five (5) years residency in the U.S. will not be approved for building access. The Contractor shall submit the documents to the NRC Contracting Officer’s Representative (COR) who will give them to DFS/PSB.

DFS/PSB may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the OPM Standard Form 85 and the Contractor's pre-screening record. Also, in the exercise of its authority, the Government may, among other things, grant or deny permanent building access approval based on the results of its review or investigation. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the NRC work sites for an extended period of time during the term of the contract. In the event that DFS/PSB are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the Contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The Contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

CANCELLATION OR TERMINATION OF BUILDING ACCESS/ REQUEST

The Contractor shall immediately notify the COR when a Contractor or subcontractor employee or consultant's need for NRC building access approval is withdrawn or the need by the Contractor employee's for building access terminates. The COR will immediately notify DFS/PSB (via e-mail) when a Contractor employee no longer requires building access. The Contractor shall be required to return any NRC issued badges to the COR for return to DFS/FSB (Facilities Security Branch) within three (3) days after their termination.

(End of Clause)

NRCI020 COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973, AS AMENDED (SEP 2013)

In 1998, Congress amended the Rehabilitation Act of 1973 (29 U.S.C. §794d) as amended by the Workforce Investment Act of 1998 (P.L. 105 - 220), August 7, 1998 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. Inaccessible technology interferes with an ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, open new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. §794d), agencies must give disabled employees and members of the public access to information that is comparable to access available to others.

Specifically, Section 508 of that Act requires that when Federal agencies develop, procure, maintain, or use EIT, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. (36 C.F.R. §1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at: http://www.access-board.gov/sec508/standards.htm)

Exceptions.

All EIT that the government acquires by purchase or by lease/rental under this contract must meet the applicable accessibility standards at 36 C.F.R. Part 1194, unless one or more of the following exceptions at FAR 39.204 applies to this acquisition (applicable if checked):

[ ] The EIT is for a national security system.

[ ] The EIT is acquired by a contractor incidental to a contract.

[ ] The EIT is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

[ ] Compliance with the applicable 36 C.F.R. Part 1194 provisions would impose an undue burden on the agency.

Applicable Standards.

The following accessibility standards from 36 C.F.R. Part 1194 have been determined to be applicable to this contract/order. See www.section508.gov for more information:

Will be specified at the individual BPA Call level.

[ ] 1194.21 Software applications and operating systems.

[ ] 1194.22 Web-based intranet and internet information and applications. 16 rules.

[ ] 1194.23 Telecommunications products.

[ ] 1194.24 Video and multimedia products.

[ ] 1194.25 Self contained, closed products.

[ ] 1194.26 Desktop and portable computers.

[ ] 1194.31 Functional performance criteria.

[ ] 1194.41 Information, documentation, and support.

Note: Under the Exceptions paragraph, the Contracting Officer should check the boxes for any exceptions that apply. If no exceptions apply, then the Contracting Officer should, under the Applicable Standards paragraph, check the boxes that indicate which of the standards apply. See FAR Subpart 39.2 and www.section508.gov for additional guidance.

(End of Clause)

NRCD020 BRANDING

The Contractor is required to use the statement below in any publications, presentations, articles, products, or materials funded under this contract/order, to the extent practical, in order to provide NRC with recognition for its involvement in and contribution to the project. If the work performed is funded entirely with NRC funds, then the contractor must acknowledge that information in its documentation/presentation.

Work Supported by the U.S. Nuclear Regulatory Commission (NRC), Office of [*Insert office name here*], under Contract/order number [*Insert contract/order number here*].

(End of Clause)

NRCD010 PACKAGING AND MARKING

(a) The Contractor shall package material for shipment to the NRC in such a manner that will ensure acceptance by common carrier and safe delivery at destination. Containers and closures shall comply with the Surface Transportation Board, Uniform Freight Classification Rules, or regulations of other carriers as applicable to the mode of transportation.

(b) On the front of the package, the Contractor shall clearly identify the contract number under which the product is being provided.

(c) Additional packaging and/or marking requirements are as follows: [*Insert packaging and/or marking requirements here*].

(End of Clause)

NRCF010PLACE OF DELIVERY--REPORTS (AUG 2011)

The items to be furnished hereunder shall be delivered to:

*To be incorporated into any resultant BPA Calls.

NRCH470 GREEN PURCHASING (SEP 2015)

(a) In furtherance of the sustainable acquisition goals of Executive Order (EO) 13693, "Planning for Federal Sustainability in the Next Decade," products and services provided under this contract/order shall be energy efficient (EnergyStar® or Federal Energy Management Program - FEMP-designated products), water efficient, biobased, environmentally preferable (excluding EPEAT®-registered products), non-ozone depleting, contain recycled content, or are non- or low toxic alternatives or hazardous constituents (e.g., non-VOC paint), where such products and services meet agency performance requirements. See: Executive Order (EO) 13693, "Planning for Federal Sustainability in the Next Decade."

(b) The NRC and contractor may negotiate during the contract term to permit the substitution or addition of designated recycled content products (i.e., Comprehensive Procurement Guidelines - CPG), EPEAT®-registered products, EnergyStar®- and FEMP designated energy efficient products and appliances, USDA designated biobased products (Biopreferred® program), environmentally preferable products, WaterSense and other water efficient products, products containing non- or lower-ozone depleting substances (i.e., SNAP), and products containing non- or low-toxic or hazardous constituents (e.g., non-VOC paint), when such products and services are readily available at a competitive cost and satisfy the NRC's performance needs.

(c) The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order.

(End of Clause)

NRCG030 ELECTRONIC PAYMENT (SEP 2014)

The Debt Collection Improvement Act of 1996 requires that all payments except IRS tax refunds be made by Electronic Funds Transfer. Payment shall be made in accordance with FAR 52.232-33, entitled "Payment by Electronic Funds-Central Contractor Registration".

To receive payment, the contractor shall prepare invoices in accordance with NRC's Billing Instructions. Claims shall be submitted on the payee's letterhead, invoice, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal – Continuation Sheet." The preferred method of submitting invoices is electronically to: NRCPayments@nrc.gov.

(End of Clause)

NRCH480 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS

The Debt Collection Improvement Act of 1996 requires that all Federal payments except IRS tax refunds be made by Electronic Funds Transfer. lt is the policy of the Nuclear Regulatory Commission to pay government vendors by the Automated Clearing House (ACH) electronic funds transfer payment system. Item 15C of the Standard Form 33 may be disregarded.

(End of Clause)

NRCH490 COMMITMENT OF PUBLIC FUNDS

(a) It is also brought to your attention that the contracting officer is the only individual who can legally obligate funds or commit the NRC to the expenditure of public funds in connection with this procurement. This means that unless provided in a contract document or specifically authorized by the contracting officer, NRC technical personnel may not issue contract

modifications, give formal contractual commitments, or otherwise bind, commit, or obligate the NRC contractually. Informal unauthorized commitments, which do not obligate the NRC and do not entitle the contractor to payment, may include:

(1) Encouraging a potential contractor to incur costs prior to receiving a contract;

(2) Requesting or requiring a contractor to make changes under a contract without formal contract modifications;

(3) Encouraging a contractor to incur costs under a cost-reimbursable contract in excess of those costs contractually allowable; and

(4) Committing the Government to a course of action with regard to a potential contract, contract change, claim, or dispute.

(End of Clause)

NRCH420 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS (SEP 2013)

Prior to occupying any Government provided space at NRC Headquarters in Rockville Maryland, the Contractor shall obtain written authorization to occupy specifically designated government space, via the NRC Contracting Officer's Representative (COR), from the Chief, Space Design Branch, Office of Administration. Failure to obtain this prior authorization can result in one, or a combination, of the following remedies as deemed appropriate by the Contracting Officer.

(1) Rental charge for the space occupied will be deducted from the invoice amount due the Contractor

(2) Removal from the space occupied

(3) Contract Termination

(End of Clause)

NRCH410 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES

(a) The U.S. Nuclear Regulatory Commission (NRC) contractor and its subcontractor are subject to the Whistleblower Employee Protection public law provisions as codified at 42 U.S.C. 5851. NRC contractor(s) and subcontractor(s) shall comply with the requirements of this Whistleblower Employee Protection law, and the implementing regulations of the NRC and the Department of Labor (DOL). See, for example, DOL Procedures on Handling Complaints at 29 C.F.R. Part 24 concerning the employer obligations, prohibited acts, DOL procedures and the requirement for prominent posting of notice of Employee Rights at Appendix A to Part 24

entitled: “Your Rights Under the Energy Reorganization Act”.

(b) Under this Whistleblower Employee Protection law, as implemented by regulations, NRC contractor and subcontractor employees are protected from discharge, reprisal, threats, intimidation, coercion, blacklisting or other employment discrimination practices with respect to compensation, terms, conditions or privileges of their employment because the contractor or subcontractor employee(s) has provided notice to the employer, refused to engage in unlawful practices, assisted in proceedings or testified on activities concerning alleged violations of the Atomic Energy Act of 1954 (as amended) and the Energy Reorganization Act of 1974 (as amended).

(c) The contractor shall insert this or the substance of this clause in any subcontracts involving work performed under this contract.

(End of Clause)

NRCH400 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS

Review and Approval of Reports

(a) Reporting Requirements. The contractor/grantee shall comply with the terms and conditions of the contract/grant regarding the contents of the draft and final report, summaries, data, and related documents, to include correcting, deleting, editing, revising, modifying, formatting, and supplementing any of the information contained therein, at no additional cost to the NRC. Performance under the contract/grant will not be deemed accepted or completed until it complies with the NRC’s directions. The reports, summaries, data, and related documents will be considered draft until approved by the NRC. The contractor/grantee agrees that the direction, determinations, and decisions on approval or disapproval of reports, summaries, data, and related documents created under this contract/grant remain solely within the discretion of the NRC.

(b) Publication of Results. Prior to any dissemination, display, publication, or release of articles, reports, summaries, data, or related documents developed under the contract/grant, the contractor/grantee shall submit them to the NRC for review and approval. The contractor/ grantee shall not release, disseminate, display or publish articles, reports, summaries, data, and related documents, or the contents therein, that have not been reviewed and approved by the NRC for release, display, dissemination or publication. The contractor/grantee agrees to conspicuously place any disclaimers, markings or notices, directed by the NRC, on any articles, reports, summaries, data, and related documents that the contractor/grantee intends to release, display, disseminate or publish to other persons, the public, or any other entities. The contractor/grantee agrees, and grants, a royalty-free, nonexclusive, irrevocable worldwide license to the government, to use, reproduce, modify, distribute, prepare derivative works, release, display or disclose the articles, reports, summaries, data, and related documents developed under

the contract/grant, for any governmental purpose and to have or authorize others to do so.

(c) Identification/Marking of Sensitive Unclassified Non-Safeguards Information (SUNSI) and Safeguards Information (SGI). The decision, determination, or direction by the NRC that information possessed, formulated or produced by the contractor/grantee constitutes SUNSI or SGI is solely within the authority and discretion of the NRC. In performing the contract/grant, the contractor/grantee shall clearly mark SUNSI and SGI, to include for example, OUO-Allegation Information or OUO-Security Related Information on any reports, documents, designs, data, materials, and written information, as directed by the NRC. In addition to marking the information as directed by the NRC, the contractor shall use the applicable NRC cover sheet (e.g., NRC Form 461 Safeguards Information) in maintaining these records and documents. The contractor/grantee shall ensure that SUNSI and SGI is handled, maintained and protected from unauthorized disclosure, consistent with NRC policies and directions. The contractor/grantee shall comply with the requirements to mark, maintain, and protect all information, including documents, summaries, reports, data, designs, and materials in accordance with the provisions of Section 147 of the Atomic Energy Act of 1954 as amended, its implementing regulations (10 CFR 73.21), Sensitive Unclassified Non-Safeguards and Safeguards Information policies, and NRC Management Directives and Handbooks 12.5, 12.6 and 12.7.

(d) Remedies. In addition to any civil, criminal, and contractual remedies available under the applicable laws and regulations, failure to comply with the above provisions, and/or NRC directions, may result in suspension, withholding, or offsetting of any payments invoiced or claimed by the contractor/grantee.

(e) Flowdown. If the contractor/grantee intends to enter into any subcontracts or other agreements to perform this contract/grant, the contractor/grantee shall include all of the above provisions in any subcontracts or agreements.

(End of Clause)

NRCH440 CONTRACTOR RESPONSIBILITY FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

In accordance with the Office of Management and Budget's guidance to Federal agencies and the Nuclear Regulatory Commission's (NRC) implementing policy and procedures, a contractor (including subcontractors and contractor employees), who performs work on behalf of the NRC, is responsible for protecting, from unauthorized access or disclosure, personally identifiable information (PII) that may be provided, developed, maintained, collected, used, or disseminated, whether in paper, electronic, or other format, during performance of this contract.

A contractor who has access to NRC owned or controlled PII, whether provided to the contractor by the NRC or developed, maintained, collected, used, or disseminated by the contractor during the course of contract performance, must comply with the following

requirements:

(1) General. In addition to implementing the specific requirements set forth in this clause, the contractor must adhere to all other applicable NRC guidance, policy and requirements for the handling and protection of NRC owned or controlled PII. The contractor is responsible for making sure that it has an adequate understanding of such guidance, policy and requirements.

(2) Use, Ownership, and Nondisclosure. A contractor may use NRC owned or controlled PII solely for purposes of this contract, and may not collect or use such PII for any purpose outside the contract without the prior written approval of the NRC Contracting Officer. The contractor must restrict access to such information to only those contractor employees who need the information to perform work under this contract, and must ensure that each such contractor employee (including subcontractors' employees) signs a nondisclosure agreement, in a form suitable to the NRC Contracting Officer, prior to being granted access to the information. The NRC retains sole ownership and rights to its PII. Unless the contract states otherwise, upon completion of the contract, the contractor must turn over all PII in its possession to the NRC, and must certify in writing that it has not retained any NRC owned or controlled PII except as otherwise authorized in writing by the NRC Contracting Officer.

(3) Security Plan. When applicable, and unless waived in writing by the NRC Contracting Officer, the contractor must work with the NRC to develop and implement a security plan setting forth adequate procedures for the protection of NRC owned or controlled PII as well as the procedures which the contractor must follow for notifying the NRC in the event of any security breach. The plan will be incorporated into the contract and must be implemented and followed by the contractor once it has been approved by the NRC Contracting Officer. If the contract does not include a security plan at the time of contract award, a plan must be submitted for the approval of the NRC Contracting Officer within 30 days after contract award.

(4) Breach Notification. The contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer’s Representative (COR) upon discovery of any suspected or confirmed breach in the security of NRC owned or controlled PII.

(5) Legal Demands for Information. If a legal demand is made for NRC owned or controlled PII (such as by subpoena), the contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer’s Representative (COR). After notification, the NRC will determine whether and to what extent to comply with the legal demand. The Contracting Officer will then notify the contractor in writing of the determination and such notice will indicate the extent of disclosure authorized, if any. The contractor may only release the information specifically demanded with the written permission of the NRC Contracting Officer.

(6) Audits. The NRC may audit the contractor's compliance with the requirements of this clause, including through the use of online compliance software.

(7) Flow-down. The prime contractor will flow this clause down to subcontractors that would

be covered by any portion of this clause, as if they were the prime contractor.

(8) Remedies:

(a) The contractor is responsible for implementing and maintaining adequate security controls to prevent the loss of control or unauthorized disclosure of NRC owned or controlled PII in its possession. Furthermore, the contractor is responsible for reporting any known or suspected loss of control or unauthorized access to PII to the NRC in accordance with the provisions set forth in Article 4 above.

(b) Should the contractor fail to meet its responsibilities under this clause, the NRC reserves the right to take appropriate steps to mitigate the contractor's violation of this clause. This may include, at the sole discretion of the NRC, termination of the subject contract.

(9) Indemnification. Notwithstanding any other remedies available to the NRC, the contractor will indemnify the NRC against all liability (including costs and fees) for any damages arising out of violations of this clause.

(End of Clause)

NRCH430 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS (OCT 2014)

All contractor employees, subcontractor employees, applicants, and consultants proposed for performance or performing under this contract shall be subject to pre-assignment, random, reasonable suspicion, and post-accident drug testing applicable to: (1) individuals who require unescorted access to nuclear power plants, (2) individuals who have access to classified or safeguards information, (3) individuals who are required to carry firearms in performing security services for the NRC, (4) individuals who are required to operate government vehicles or transport passengers for the NRC, (5) individuals who are required to operate hazardous equipment at NRC facilities, or (6) individuals who admit to recent illegal drug use or those who are found through other means to be using drugs illegally.

The NRC Drug Program Manager will schedule the drug testing for all contractor employees, subcontractor employees, applicants, and consultants who are subject to testing under this clause. The consequences of refusing to undergo drug testing or a refusal to cooperate in such testing, including not appearing at the scheduled appointment time, will result in the Agency’s refusal of the contractor employee to work under any NRC contract. Any NRC contractor employee found to be using, distributing or possessing illegal drugs, or any contractor employee who fails to receive a verified negative drug test result under this program while in a duty status will immediately be removed from working under the NRC contract. The contractor's employer will be notified of the denial or revocation of the individual's authorization to have access to

information and ability to perform under the contract. The individual may not work on any NRC contract for a period of not less than one year from the date of the failed, positive drug test and will not be considered for reinstatement unless evidence of rehabilitation, as determined by the NRC "drug testing contractor's" Medical Review Officer, is provided.

Contractor drug testing records are protected under the NRC Privacy Act Systems of Records, System 35, "Drug Testing Program Records - NRC" found at: http://www.nrc.gov/reading-rm/foia/privacy-systems.html

(End of Clause)

NRCH380 SECURITY REQUIREMENTS FOR ACCESS TO CLASSIFIED MATTER OR INFORMATION (SEP 2013)

Performance under this contract will require access to classified matter or information (National Security Information or Restricted Data) in accordance with the attached NRC Form 187 (See List of Attachments). Prime Contractor personnel, subcontractors or others performing work under this contract shall require a "Q" security clearance (allows access to Top Secret, Secret, and Confidential National Security Information and Restricted Data) or an "L" security clearance (allows access to Secret and Confidential National Security Information and/or Confidential Restricted Data).

The Contractor must identify all individuals to work under this contract. The NRC sponsoring office shall make the final determination of the type of security clearance required for all individuals working under this contract.

The Contractor shall conduct a preliminary security interview or review for each of its employees, subcontractor employees and consultants, and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed. The Contractor will pre-screen applicants for the following:

(a) pending criminal charges or proceedings; (b) felony arrest records including alcohol related arrest within the last seven (7) years; (c) record of any military courts-martial charges and proceedings in the last seven (7) years and courts-martial convictions in the last ten (10) years; (d)any involvement in hate crimes; (e) involvement in any group or organization that espouses extra-legal violence as a legitimate means to an end; (f) dual or multiple citizenship including the issuance of a foreign passport in the last seven (7) years; (g) illegal use possession, or distribution of narcotics or other controlled substances within the last seven (7) years; (h) financial issues regarding delinquent debts, liens, garnishments, bankruptcy and civil court actions in the last seven (7) years.

The Contractor will make a written record of their pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (h)), and have the candidate

verify the record, sign and date it. Two (2) copies of the signed interview record or review will be supplied to DFS/PSB with the applicant's completed security application package.

The Contractor will further ensure that all Contractor employees, subcontractor employees and consultants for classified information access approval complete all security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed security applications (submitted for candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed) is a contract requirement. Failure of the Contractor to comply with this condition may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of termination or cancellation, the Government may select another firm for contract award.

Such Contractor personnel shall be subject to the NRC Contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and 10 CFR Part 10.11, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Single Scope Background Investigation (SSBI) for "Q" clearances or a favorably adjudicated Access National Agency Check and Inquiries (ANACI), or higher level investigation depending on the position the individual will occupy, for "L" clearances.

A Contractor employee shall not have access to classified information until he/ she is granted a security clearance by DFS/PSB, based on a favorably adjudicated investigation. In the event the Contractor employee's investigation cannot be favorably adjudicated, any interim access approval could possibly be revoked and the individual could be subsequently removed from performing under the contract. If interim approval access is revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The individual will be subject to a reinvestigation every five (5) years for "Q" clearances and every ten (10) years for "L" clearances.

CORs are responsible for submitting the completed access/clearance request package as well as other documentation that is necessary to DFS/PSB. The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (online Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to DFS/PSB for review and adjudication, prior to submission to the Office of Personnel Management for investigation. The individual may start working under this contract before a final clearance is granted if a temporary access determination can be made by DFS/PSB after the review of the security package. If the individual is granted a temporary access authorization, the individual may not have access to classified information under this contract until DFS/PSB has granted them the appropriate security clearance, and the Contractor has read, understood, and signed the SF 312, "Classified Information Nondisclosure

Agreement." The Contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the Contractor in a sealed envelope), as set forth in NRC MD 12.3. Based on DFS/PSB review of the applicant's investigation, the individual may be denied his/her security clearance in accordance with the due process procedures set forth in MD 12.3, E.O. 12968, and 10 CFR Part 10.11.

In accordance with NRCAR 2052.204-70 cleared Contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments), MD 12.3, SF- 86 and Contractor's signed record or review of the pre-screening which furnishes the basis for providing security requirements to prime Contractors, subcontractors or others who have or may have an NRC contractual relationship which requires access to classified information.

CANCELLATION OR TERMINATION OF SECURITY CLEARANCE ACCESS/REQUEST

When a request for clearance investigation is to be withdrawn or canceled, the Contractor shall immediately notify the COR by telephone so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing by the Contractor to the COR who will forward the confirmation via email to DFS/PSB. Additionally, DFS/PSB must be immediately notified in writing when an individual no longer requires access to Government classified information, including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for access under the NRC "Personnel Security Program."

(End of Clause)

NRCH370 SAFETY OF ON-SITE CONTRACTOR PERSONNEL

Ensuring the safety of occupants of Federal buildings is a responsibility shared by the professionals implementing our security and safety programs and the persons being protected. The NRC's Office of Administration (ADM) Division of Facilities and Security (DFS) has coordinated an Occupant Emergency Plan (OEP) for NRC Headquarters buildings with local authorities. The OEP has been approved by the Montgomery County Fire and Rescue Service. It is designed to improve building occupants' chances of survival, minimize damage to property, and promptly account for building occupants when necessary.

The contractor's Project Director shall ensure that all personnel working full time on-site at NRC Headquarters read the NRC's OEP, provided electronically on the NRC Intranet at http://www.internal.nrc.gov/ADM/OEP.pdf. The contractor's Project Director also shall emphasize to each staff member that they are to be familiar with and guided by the OEP, as well as by instructions given by emergency response personnel in situations which pose an immediate health or safety threat to building occupants.

The NRC Contracting Officer's Representative (COR) shall ensure that the contractor's Project Director has communicated the requirement for on-site contractor staff to follow the guidance in the OEP. The NRC Contracting Officer's Representative (COR) also will assist in accounting for on-site contract persons in the event of a major emergency (e.g., explosion occurs and casualties or injuries are suspected) during which a full evacuation will be required, including the assembly and accountability of occupants. The NRC DFS will conduct drills periodically to train occupants and assess these procedures.

(End of Clause)

NRCH360 INTERNET

Neither NRC nor its third party contractors that manage or develop the NRC web site shall send persistent cookies, place persistent cookies on users' computers, nor collect personally identifiable information from visitors to the NRC web site unless in addition to clear and conspicuous notice, each of the following conditions are met: there is a compelling need to gather the data on the site; there are appropriate and publicly disclosed privacy safeguards for handling of information derived from "cookies"; and personal approval is obtained from the head of the agency.

(End of Clause)

NRCH350 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OVER CONTRACTOR

The National Industrial Security Program Operating Manual (NISPOM) implements the provisions of E.O. 12829, "National Industrial Security Program." A company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or otherwise, to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified information contracts. (See NRC Management Directive 12.2 – "NRC Classified Information Security Program")

(a) For purposes of this clause, a foreign interest is defined as any of the following:

(1) A foreign government or foreign government agency;

(2) Any form of business enterprise organized under the laws of any country other than the United States or its possessions;

(3) Any form of business enterprise organized or incorporated under the laws of the U.S., or a State or other jurisdiction within the U.S., which is owned, controlled, or influenced by a foreign government, agency, firm, corporation or person; or

(4) Any person who is not a U.S. citizen.

(b) A U.S. company determined to be under FOCI is not eligible for facility clearance (FCL). If a company already has an FCL, the FCL shall be suspended or revoked unless security measures are taken to remove the possibility of unauthorized access to classified information.

(c) For purposes of this clause, subcontractor means any subcontractor at any tier and the term "contracting officer" shall mean NRC contracting officer. When this clause is included in a subcontract, the term "contractor" shall mean subcontractor and the term "contract" shall mean subcontract.

(d) The contractor shall complete and submit and SF-328, DD-441 and DD-441-1 forms, prior to contract award. The information contained in these forms may be used in making a determination as to whether a contractor is eligible to participate in the National Industrial Security Program and have a facility security clearance.

(e) The contractor shall immediately provide the contracting officer written notice of any changes in the extent and nature of FOCI over the contractor which would affect the answers to the questions presented in SF-328, "Certificate Pertaining to Foreign Interest". Further, notice of changes in ownership or control which are required to be reported to the Securities and Exchange Commission, the Federal Trade Commission, or the Department of Justice shall also be furnished concurrently to the contracting officer.

(f) In those cases where a contractor has changes involving FOCI, the NRC must determine whether the changes will pose an undue risk to the common defense and security. In making this determination, the contracting officer shall consider proposals made by the contractor to avoid or mitigate foreign influences.

(g) The contractor agrees to insert terms that conform substantially to the language of this clause including this paragraph (g) in all subcontracts under this contract that will require access to classified information and shall require such subcontractors to submit completed SF-328, DD-441 and DD-441-1 forms prior to award of a subcontract. Information to be provided by a subcontractor pursuant to this clause may be submitted directly to the contracting officer.

(h) Information submitted by the contractor or any affected subcontractor as required pursuant to this clause shall be treated by NRC to the extent permitted by law, as business or financial information submitted in confidence to be used solely for purposes of evaluating FOCI.

(i) The requirements of this clause are in addition to the requirement that a contractor obtain and retain the security clearances required by the contract. This clause shall not operate as a limitation on NRC's rights, including its rights to terminate this contract.

(j) The contracting officer may terminate this contract for default either if the contractor fails to meet obligations imposed by this clause, e.g., provide the information required by this clause, comply with the contracting officer's instructions about safeguarding classified information, or

make this clause applicable to subcontractors, or if, in the contracting officer's judgment, the contractor creates a FOCI situation in order to avoid performance or a termination for default. The contracting officer may terminate this contract for convenience if the contractor becomes subject to FOCI and for reasons other than avoidance of performance of the contract, cannot, or chooses not to, avoid or mitigate the FOCI problem.

(End of Clause)

NRCH340 COMPLIANCE WITH U.S. IMMIGRATION LAWS AND REGULATIONS

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States immigration laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Permanent Resident Form I-551 (Green Card), or must present other evidence from the U.S. Department of Homeland Security/U.S. Citizenship and Immigration Services that employment will not affect his/her immigration status. The U.S. Citizenship and Immigration Services provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on their website, http://www.uscis.gov/portal/site/uscis.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC facilities or its equipment/services, and/or take any number of contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

(End of Clause)

NRCH320A COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL (ALTERNATE I)

(a) NRC facilities may not be available due to (1) designated federal holiday, any other day designated by federal statute, Executive Order, or by Presidential Proclamation; (2) early dismissal of NRC employees during working hours (e.g., special holidays or emergency situations); or (3) occurrence of emergency conditions during nonworking hours (e.g., inclement weather).

(b) When NRC facilities are unavailable, the compensation and deduction policy stated below shall be followed for contractor employees performing work on-site at the NRC facility:

(c) The contractor shall not charge the NRC for work performed by on- site contractor employees who were reassigned to perform other duties off site during the time the NRC facility was closed.

(d) On-site contractor staff shall be guided by the instructions given by a third party (e.g., Montgomery County personnel, in the case of a water emergency) in situations which pose an

immediate health or safety threat to employees.

(e) The contractor's Project Director shall first consult the NRC Contracting Officer's Representative (COR) before releasing on-site personnel in situations which do not impose an immediate safety or health threat to employees (e.g., special holidays). That same day, the contractor must then alert the Contracting Officer of the NRC Contracting Officer's Representative's (COR) direction. The contractor shall continue to provide sufficient personnel to perform the requirements of essential tasks as defined in the Statement of Work which already are in operation or are scheduled.

*To be incorporated into the resultant contract (End of Clause)

NRCH320 COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL

(a) NRC facilities may not be available due to (1) designated Federal holiday, any other day designated by

Federal Statute, Executive Order, or by President's Proclamation; (2) early dismissal of NRC employees during working hours (e.g., special holidays, water emergency); or (3) occurrence of emergency conditions during nonworking hours (e.g., inclement weather).

(b) When NRC facilities are unavailable, the contractor's compensation and deduction policy (date), incorporated herein by reference, shall be followed for contractor employees performing work on-site at the NRC facility. The contractor shall promptly submit any revisions to this policy to the Contracting Officer for review before they are incorporated into the contract.

(c) The contractor shall not charge the NRC for work performed by on-site contractor employees who were reassigned to perform other duties off site during the time the NRC facility was closed.

(d) On-site contractor staff shall be guided by the instructions given by a third party (e.g., Montgomery County personnel in situations which pose an immediate health or safety threat to employees (e.g., water emergency).

(e) The contractor's Project Director shall first consult the NRC Contracting Officer's Representative (COR) before releasing on-site personnel in situations which do not impose an immediate safety or health threat to employees (e.g., special holidays). That same day, the contractor must then alert the Contracting Officer of the NRC Contracting Officer's Representative's (COR) direction. The contractor shall continue to provide sufficient personnel to perform the requirements of essential tasks as defined in the Statement of Work which already are in operation or are scheduled.

(End of Clause)

NRCH310 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS

Annual and final evaluations of contractor performance under this contract will be prepared in accordance with FAR Subpart 42.15, "Contractor Performance Information," normally at or near the time the contractor is notified of the NRC's intent to exercise the contract option. If the multi-year contract does not have option years, then an annual evaluation will be prepared [*Insert time for annual evaluation here*]. Final evaluations of contractor performance will be prepared at the expiration of the contract during the contract closeout process.

The Contracting Officer will transmit the NRC Contracting Officer's Representative's (COR) annual and final contractor performance evaluations to the contractor's Project Manager, unless otherwise instructed by the contractor. The contractor will be permitted thirty days to review the document and submit comments, rebutting statements, or additional information.

Where a contractor concurs with, or takes no exception to an annual performance evaluation, the Contracting Officer will consider such evaluation final and releasable for source selection purposes. Disagreements between the parties regarding a performance evaluation will be referred to an individual one level above the Contracting Officer, whose decision will be final.

The Contracting Officer will send a copy of the completed evaluation report, marked "Source Selection Information", to the contractor's Project Manager for their records as soon as practicable after it has been finalized. The completed evaluation report also will be used as a tool to improve communications between the NRC and the contractor and to improve contract performance.

The completed annual performance evaluation will be used to support future award decisions in accordance with FAR 42.1502 and 42.1503. During the period the information is being used to provide source selection information, the completed annual performance evaluation will be released to only two parties - the Federal government personnel performing the source selection evaluation and the contractor under evaluation if the contractor does not have a copy of the report already.

(End of Clause)

NRCH080 CONTRACTOR ACQUIRED GOVERNMENT EQUIPMENT/PROPERTY

(a) The Contractor is authorized to acquire and/or fabricate the equipment/property listed below for use in the performance of this contract.

This information will be provided in BPA Calls.

(b) In the event that, during contract performance, the contractor determines that the acquisition cost for the above item(s) is expected to exceed the amount(s) contained in the contractor's

proposal, the contractor shall refer to the Limitation of Cost or Funds Clause when either is included in the contract.

(c) Only the equipment/property listed above, in the quantities shown, will be acquired by the contractor unless the contractor receives written authorization and approval from the contracting officer for the purchase of additional equipment/property. The above listed items are subject to FAR 52.245-1 – "Government Property".

(End of Clause)

NRCH070 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY

(a) The NRC will provide the contractor with the following items for use under this contract:

This information will be provided in each BPA Call.

Include an asterisk (*) if the item also applies to paragraph (b) below.

(b) The equipment/property listed below is hereby transferred from contract/agreement number:[*Insert contract/agreement number here*], to contract/agreement number:[*Insert contract/agreement number here*]:

This information will be provided in each BPA Call.

(c) Only the equipment/property listed above in the quantities shown will be provided by the Government. The contractor shall be responsible and accountable for all Government property provided under this contract and shall comply with the provisions of the FAR Government Property Clause under this contract and FAR Subpart 45.5, as in effect on the date of this contract. The contractor shall investigate and provide written notification to the NRC Contracting Officer (CO) and the NRC Division of Facilities and Security, Physical Security Branch of all cases of loss, damage, or destruction of Government property in its possession or control not later than 24 hours after discovery. The contractor must report stolen Government property to the local police and a copy of the police report must be provided to the CO and to the Division of Facilities and Security, Office of Administration.

(d) All other equipment/property required in performance of the contract shall be furnished by the Contractor.

(End of Clause)

INTERNET "COOKIES" (AUG 2011)

Neither NRC nor its third party contractors that manage or develop the NRC web site shall send persistent cookies, place persistent cookies on users' computers, nor collect personally identifiable information from visitors to the NRC web site unless in addition to clear and conspicuous notice, each of the following conditions are met: there is a compelling need to gather the data on the site; there are appropriate and publicly disclosed privacy safeguards for handling of information derived from "cookies"; and personal approval is obtained from the head of the agency.

NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2011)

NRC contractors shall ensure that their employees, consultants, and subcontractors with access to the agency's information technology (IT) equipment and/or IT services complete NRC's online initial and refresher IT security training requirements to ensure that their knowledge of IT threats, vulnerabilities, and associated countermeasures remains current. Both the initial and refresher IT security training courses generally last an hour or less and can be taken during the employee's regularly scheduled work day.

Contractor employees, consultants, and subcontractors shall complete the NRC's online annual, "Computer Security Awareness" course on the same day that they receive access to the agency's IT equipment and/or services, as their first action using the equipment/service. For those contractor employees, consultants,and subcontractors who are already working under this contract, the on-line training must be completed in accordance with agency Network Announcements issued throughout the year, within three weeks of issuance of this modification.

Contractor employees, consultants, and subcontractors who have been granted access to NRC information technology equipment and/or IT services must continue to take IT security refresher training offered online by the NRC throughout the term of the contract. Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC IT equipment and/or services, and/or take other appropriate contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

NRCH330 RULES OF BEHAVIOR FOR AUTHORIZED COMPUTER USE

In accordance with Appendix III, "Security of Federal Automated Information Resources," to Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," NRC has established rules of behavior for individual users who access all IT computing resources maintained and operated by the NRC or on behalf of the NRC. In response to the direction from OMB, NRC has issued the "Agency-wide Rules of Behavior for Authorized

Computer Use" policy, hereafter referred to as the rules of behavior. The rules of behavior for authorized computer use will be provided to NRC computer users, including contractor personnel, as part of the annual computer security awareness course.

The rules of behavior apply to all NRC employees, contractors, vendors, and agents (users) who have access to any system operated by the NRC or by a contractor or outside entity on behalf of the NRC. This policy does not apply to licensees. The next revision of Management Directive 12.5, "NRC Automated Information Security Program," will include this policy. The rules of behavior can be viewed at http://www.internal.nrc.gov/CSO/documents/ROB.pdf or use NRC's external Web-based ADAMS at http://wba.nrc.gov:8080/ves/ (Under Advanced Search, type ML082190730 in the Query box).

The rules of behavior are effective immediately upon acknowledgement of them by the person who is informed of the requirements contained in those rules of behavior. All current contractor users are required to review and acknowledge the rules of behavior as part of the annual computer security awareness course completion. All new NRC contractor personnel will be required to acknowledge the rules of behavior within one week of commencing work under this contract and then acknowledge as current users thereafter. The acknowledgement statement can be viewed at http://www.internal.nrc.gov/CSO/documents/ROB_Ack.pdf or use NRC's external Web-based ADAMS at http://wba.nrc.gov:8080/ves/ (Under Advanced Search, type ML082190730 in the Query box).

The NRC Computer Security Office will review and update the rules of behavior annually beginning in FY 2011 by December 31st of each year. Contractors shall ensure that their personnel to which this requirement applies acknowledge the rules of behavior before beginning contract performance and, if the period of performance for the contract lasts more than one year, annually thereafter. Training on the meaning and purpose of the rules of behavior can be provided for contractors upon written request to the NRC Contracting Officer's Representative (COR).

The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order if such subcontracts/agreements will authorize access to NRC electronic and information technology (EIT) as that term is defined in FAR 2.101.

(End of Clause)

NRCH039 IT SECURITY REQUIREMENTS – NRC AND CONTRACTOR (NON-NRC) FACILITIES (APR 2014)

Backups

The contractor shall ensure that backup media is created, encrypted (in accordance with information sensitivity) and verified to ensure that data can be retrieved and is restorable to NRC systems based on information sensitivity levels. Backups shall be executed to create readable

media that allows successful file/data restoration at the following frequencies:

- At least every 1 calendar day for a high sensitivity system
- At least every 1 calendar day for a moderate sensitivity system
- At least every 7 calendar days for a low sensitivity system

Perimeter Protection

The Contractor must employ perimeter protection mechanisms, such as firewalls and routers, to deny all communications unless explicitly allowed by exception.

The contractor must deploy and monitor intrusion detection capability and have an always deployed and actively engaged security monitoring capability in place for systems placed in operation for the NRC. Intrusion detection and monitoring reports will made available to the NRC upon request for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

(End of Clause)

NRCH038 IT SECURITY REQUIREMENTS – CERTIFICATION AND ACCREDITATION

SECURITY RISK ASSESSMENT

The contractor shall work with the NRC Contracting Officer's Representative (COR) in performing Risk Assessment activities according to NRC policy, standards, and guidance. The contractor shall perform Risk Assessment activities that include analyzing how the architecture implements the NRC documented security policy for the system, assessing how management, operational, and technical security control features are planned or implemented and how the system interconnects to other systems or networks while maintaining security.

SYSTEM SECURITY PLAN

The contractor shall develop the system security plan (SSP) according to NRC policy, standards, and guidance to define the implementation of IT security controls necessary to meet both the functional assurance and security requirements. The contractor will ensure that all controls required to be implemented are documented in the SSP.

ASSESSMENT PROCEDURES – SECURITY TEST & EVALUATION

The contractor shall follow NRC policy, standards, and guidance for execution of the test procedures. These procedures shall be supplemented and augmented by tailored test procedures based on the control objective as it applies to NRC. The contractor shall include verification and validation to ensure that appropriate corrective action was taken on identified security weaknesses.

The contractor shall perform ST&E activities, including but not limited to, coordinating the ST&E and developing the ST&E Plan, execution ST&E test cases and documentation of test results. The contractor shall prepare the Plan of Action and Milestones (POA&M) based on the ST&E results.

PLAN OF ACTION AND MILESTONES (POA&M) MAINTENANCE & REPORTING

The contractor shall provide a determination, in a written form agreed to by the NRC Contracting Officer's Representative (COR) and Computer Security Office, on whether the implemented corrective action was adequate to resolve the identified information security weaknesses and provide the reasons for any exceptions or risked-based decisions. The contractor shall document any vulnerabilities indicating which portions of the security control have not been implemented or applied.

The contractor shall develop and implement solutions that provide a means of planning and monitoring corrective actions; define roles and responsibilities for risk mitigation; assist in identifying security funding requirements; track and prioritize resources; and inform decision-makers of progress of open POA&M items.

The contractor shall perform verification of IT security weaknesses to ensure that all weaknesses identified through third party (e.g., OIG) audits are included in the POA&Ms that the quarterly reporting to OMB is accurate, and the reasons for any exceptions or risked-based decisions are reasonable and clearly documented. This verification process will be done in conjunction with the continuous monitoring activities.

CERTIFICATION & ACCREDITATION DOCUMENTATION

The contractor shall create, update maintain all Certification and Accreditation (C&A) documentation in accordance with the following NRC Certification and Accreditation procedures and guidance:

-C&A Non-SGI Unclassified Systems

-C&A SGI Unclassified Systems

-C&A Classified Systems

The Contractor must develop contingency plan and ensure annual contingency testing is completed within one year of previous test and provide an updated security plan and test report

according to NRC's policy and procedure.

The Contractor must conduct annual security control testing according to NRC's policy and procedure and update POA&M, SSP, etc. to reflect any findings or changes to management, operational and technical controls.

(End of Clause)

NRCH036 IT SECURITY REQUIREMENTS - DEVELOPMENT AND OPERATIONS AND MAINTENANCE REQUIREMENTS (APR 2014)

O&M Security Requirements

All system modifications to classified systems must comply with NRC security policies and procedures for classified systems, as well as federal laws, guidance, and standards to ensure Federal Information Security Management Act (FISMA) compliance.

The Contractor shall correct errors in contractor developed software and applicable documentation that are not commercial off-the-shelf which are discovered by the NRC or the contractor. Inability of the parties to determine the cause of software errors shall be resolved in accordance with the Disputes clause in Section I, FAR 52.233-1, incorporated by reference in the contract.

The Contractor shall adhere to the guidance outlined in NIST, SP 800-53, FIPS 200 and NRC guidance for the identification and documentation of minimum security controls.

The contractor shall provide the system requirements traceability matrix at the end of the initiation phase, development/acquisition phase, implementation/assessment phase, operation & maintenance phase and disposal phase that provides the security requirements in a separate section so that they can be traced through the development life cycle. The contractor shall also provide the software and hardware designs and test plan documentation, and source code upon request to the NRC for review.

All development and testing of the systems shall be protected at their assigned system sensitivity level and shall be performed on a network separate and isolated from the NRC operational network.

All system computers must be properly configured and hardened according to NRC policies, guidance, and standards and comply with all NRC security policies and procedures as commensurate with the system security categorization.

All contractor provided deliverables identified in the project plan will be subject to the review and approval of NRC Management. The contractor will make the necessary modifications to project deliverables to resolve any identified issues. Project deliverables include but are not limited to: requirements, architectures, design documents, test plans, and test reports.

Access Controls

The contractor shall not hardcode any passwords into the software unless the password only appears on the server side (e.g. using server-side technology such as ASP, PHP, or JSP).

The contractor shall ensure that the software does not contain undocumented functions and undocumented methods for gaining access to the software or to the computer system on which it is installed. This includes, but is not limited to, master access keys, back doors, or trapdoors.

Cryptography

Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 and must be operated in FIPS mode. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

Configuration Management and Control

The contractor must ensure that the system will be divided into configuration items (CIs). CIs are parts of a system that can be individually managed and versioned. The system shall be managed at the CI level.

The contractor must have a configuration management plan that includes all hardware and software that is part of the system and contains at minimum the following sections:

a. Introduction

i. Purpose & Scope

ii. Definitions

iii. References

b. Configuration Management

i. Organization

ii. Responsibilities

iii. Tools and Infrastructure

c. Configuration Management Activities

i. Specification Identification

ii. Change control form identification

iii. Project baselines

d. Configuration and Change Control

i. Change Request Processing and Approval

ii. Change Control Board

e. Milestones

i. Define baselines, reviews, audits

ii. Training and Resources

The Information System Security Officer's (ISSO's) role in the change management process must be described. The ISSO is responsible for the security posture of the system. Any changes to the system security posture must be approved by the ISSO. The contractor should not have the ability to make changes to the system's security posture without the appropriate involvement and approval of the ISSO.

The contractor shall track and record information specific to proposed and approved changes that minimally include:

a. Identified configuration change

b. Testing of the configuration change

c. Scheduled implementation the configuration change

d. Track system impact of the configuration change

e. Track the implementation of the configuration change

f. Recording & reporting of configuration change to the appropriate party

g. Back out/Fall back plan

h. Weekly Change Reports and meeting minutes

i. Emergency change procedures

j. List of team members from key functional areas

The contractor shall provide a list of software and hardware changes in advance of placing them into operation within the following timeframes:

- 30 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system

- 10 calendar days for a low sensitivity system

The contractor must maintain all system documentation that is current to within:

- 10 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

Modified code, tests performed and test results, issue resolution documentation, and updated system documentation shall be deliverables on the contract.

Any proposed changes to the system must have written approval from the NRC Contracting Officer's Representative (COR).

The contractor shall maintain a list of hardware, firmware and software changes that is current to within:

- 15 calendar days for a classified, SGI or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The contractor shall analyze proposed hardware and software configurations and modification as well as addressed security vulnerabilities in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The contractor shall provide the above analysis with the proposed hardware and software for NRC testing in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

Control of Hardware and Software

The contractor shall demonstrate that all hardware and software meet security requirements prior to being placed into the NRC production environment.

The contractor shall ensure that the development environment is separated from the operational environment using NRC CSO approved controls.

The contractor shall only use licensed software and in-house developed authorized software (including NRC and contractor developed) on the system and for processing NRC information. Public domain, shareware, or freeware shall only be installed after prior written approval is obtained from the NRC Chief Information Security Officer (CISO).

The contractor shall provide proof of valid software licensing upon request of the Contracting Officer, the NRC COR, a Senior Information Technology Security Officer (SITSO), or the Designated Approving Authorities (DAAs).

Information Security Training and Awareness Training

The contractor shall ensure that its employees, in performance of the contract, receive Information Technology (IT) security training in their role at the contractor's expense. The Contractor must provide the NRC written certification that training is complete, along with the title of the course and dates of training as a prerequisite to start of work on the contract.

The IT security role and associated type of training course and periodicity required to be completed are as follows:

Role Type of Training Required Frequency of Training

Auditor Vendor specific operating system and application security training, database security training Prior to appointment and then every three years

IT Functional Manager Vendor specific operating system and application security training, database security training Prior to appointment and then every two years

Additional system specific training upon a major system update/change

System Administrator Vendor specific operating system and application security training Prior to appointment and then every year:

- Training in operating system security in the area of responsibility occurs every 2 years
- Training in application security in the area of responsibility occurs every 2 years

Information Systems Security Officer ISSO role specific training (not awareness) provided by a government agency or by a vendor such as SANS

Vendor specific operating system and application security training Prior to appointment and then every year:

- Training in the ISSO role occurs every 3 years

- Training in operating system security in the area of responsibility occurs every 3 years
- Training in application security in the area of responsibility occurs every 3 years

Database Administrator Vendor specific database security training

Prior to appointment and then every 2 years:

- Training in database security in the area of responsibility occurs every 2 years

Network Administrator Network administrator role specific training (not awareness) provided by a government agency or by a vendor such as SANS

Network specific security training Prior to appointment and then every year:

- Training in the Network administrator role occurs every 3 years
- Training in network security in the area of responsibility occurs every year where network administrator role training does not occur

IT Managers

Vendor specific operating system and application security training, database security training. Prior to appointment and then every two years

Additional system specific training upon a major system update/change

IT System Developer Vendor specific operating system and application security training, database security training Prior to appointment and then every year

– training with system-specific training (ISS LoB or commercial) upon assuming the role, to become biannual with NRC provided training every other year.

The contractor must ensure that required refresher training is accomplished in accordance with the required frequency specifically associated with the IT security role.

Auditing

The system shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators or system security officers and other security relevant events. The system shall be able to audit any override of security controls.

The Contractor shall ensure auditing is implemented on the following:

- Operating System
- Application
- Web Server
- Web Services
- Network Devices
- Database
- Wireless

The contractor shall perform audit log reviews daily using automated analysis tools.

Contractor must log at least the following events on systems that process NRC information:

- Audit all failures
- Successful logon attempt
- Failure of logon attempt
- Permission Changes
- Unsuccessful File Access
- Creating users & objects
- Deletion & modification of system files
- Registry Key/Kernel changes
- Startup & shutdown
- Authentication
- Authorization/permission granting
- Actions by trusted users
- Process invocation
- Controlled access to data by individually authenticated user
- Unsuccessful data access attempt

- Data deletion
- Data transfer
- Application configuration change
- Application of confidentiality or integrity labels to data
- Override or modification of data labels or markings
- Output to removable media
- Output to a printer

(End of Clause)

NRCH034 INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS – GENERAL EXCEPTIONS

All purchases shall comply with the latest version of policy, procedures and standards. Individual task orders will reference latest versions of policy, procedures, standards or exceptions as necessary. These policy, procedures and standards include: NRC Management Directive (MD) volume 12 Security, Computer Security Office policies, procedures and standards, National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS), and Committee on National Security Systems (CNSS) policy, directives, instructions, and guidance. This information is available at the following links:

All procurements must be certified and accredited prior to being placed into an operational state.

All electronic processing of NRC sensitive information, including all system development and operations and maintenance activities performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the highest sensitivity of the information that is processed or will ultimately be processed.

All systems used to process NRC sensitive information shall meet NRC configuration standards available at: http://www.internal.nrc.gov/CSO/standards.html.

(End of Clause)

NRCH032 INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS – GENERAL (APR 2014)

Basic Contract IT Security Requirements

The contractor agrees to insert terms that conform substantially to the language of the IT security requirements, excluding any reference to the Changes clause of this contract, all subcontracts

under this contract.

For unclassified information used for the effort, the contractor shall provide an information security categorization document indicating the sensitivity of the information processed as part of this contract if the information security categorization was not provided in the statement of work. The determination shall be made using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 and must be approved by CSO. The NRC contracting officer and Contracting Officer's Representative (COR) shall be notified immediately before the contractor begins to process information at a higher sensitivity level.

If the effort includes use or processing of classified information, the NRC contracting officer and Contracting Officer's Representative (COR) shall be notified before the contractor begins to process information at a more restrictive classification level.

All work under this contract shall comply with the latest version of policy, procedures and standards. Individual task orders will reference latest versions of standards or exceptions as necessary. These policy, procedures and standards include: NRC Management Directive (MD) volume 12 Security, Computer Security Office policies, procedures and standards, National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS), and Committee on National Security Systems (CNSS) policy, directives, instructions, and guidance. This information is available at the following links:

NRC Policies, Procedures and Standards (CSO internal website):

http://www.internal.nrc.gov/CSO/policies.html

All NRC Management Directives (public website):

http://www.nrc.gov/reading-rm/doc-collections/management-directives/

NIST SP and FIPS documentation is located at:

http://csrc.nist.gov/

CNSS documents are located at:

http://www.cnss.gov/

When e-mail is used, the Contractors shall only use NRC provided e-mail accounts to send and receive sensitive information (information that is not releasable to the public) or mechanisms to protect the information during transmission to NRC that have been approved by CSO.

All Contractor employees must sign the NRC Agency-Wide Rules of Behavior for Authorized Computer Use prior to being granted access to NRC computing resources.

The Contractor shall adhere to following NRC policies, including but not limited to:

- Management Directive 12.5, Automated Information Security Program
- Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities
- Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information
- Computer Security Information Protection Policy
- Remote Access Policy
- Use of Commercial Wireless Devices, Services and Technologies Policy
- Laptop Security Policy
- Computer Security Incident Response Policy

Contractor will adhere to NRC's prohibition of use of personal devices to process and store NRC sensitive information.

All work performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the sensitivity level of the information being processed.

Contract Performance and Closeout

The contractor shall ensure that the NRC data processed during the performance of this contract shall be purged from all data storage components of the contractor's computer facility, and the contractor will retain no NRC data within 30 calendar days after contract is completed. Until all data is purged, the contractor shall ensure that any NRC data remaining in any storage component will be protected to prevent unauthorized disclosure.

When contractor employees no longer require access to an NRC system, the contractor shall notify the Contracting Officer's Representative (COR) within 24 hours.

Upon contract completion, the contractor shall provide a status list of all contractor employees who were users of NRC systems and shall note if any users still require access to the system to perform work if a follow-on contract or task order has been issued by NRC.

Control of Information and Data

The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any security controls or countermeasures either designed or developed by the contractor under this contract or otherwise provided by the NRC.

Any IT system used to process NRC sensitive information shall:

- Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to provide.

- Be able to authenticate data that includes information for verifying the claimed identity of individual users (e.g., passwords).

- Protect authentication data so that it cannot be accessed by any unauthorized user.

- Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user.

- Report to appropriate security personnel when attempts are made to guess the authentication data whether inadvertently or deliberately.

Access Controls

Any contractor system being used to process NRC data shall be able to define and enforce access privileges for individual users. The discretionary access controls mechanisms shall be configurable to protect objects (e.g., files, folders) from unauthorized access.

The contractor system being used to process NRC data shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

The contractors shall only use NRC approved methods to send and receive information considered sensitive or classified. Specifically,

- Classified Information - All NRC Classified data being transmitted over a network shall use NSA approved encryption and adhere to guidance in MD 12.2 NRC Classified Information Security Program, MD 12.5 NRC Automated Information Security Program and Committee on National Security Systems. Classified processing shall be only within facilities, computers, and spaces that have been specifically approved for classified processing.

- SGI Information – All SGI being transmitted over a network shall adhere to guidance in MD 12.7 NRC Safeguards Information Security Program and MD 12.5 NRC Automated Information Security Program. SGI processing shall be only within facilities, computers, and spaces that have been specifically approved for SGI processing. Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 overall level 2 and must be operated in FIPS mode. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

The most restrictive set of rights/privileges or accesses needed by users (or processes acting on

behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.

Separation of duties for contractor systems used to process NRC information must be enforced by the system through assigned access authorizations.

The mechanisms within the contractor system or application that enforces access control and other security features shall be continuously protected against tampering and/or unauthorized changes.

Configuration Standards

All systems used to process NRC sensitive information shall meet NRC configuration standards available at: http://www.internal.nrc.gov/CSO/standards.html.

Information Security Training and Awareness Training

Contractors shall ensure that their employees, consultants, and subcontractors that have significant IT responsibilities (e.g., IT administrators, developers, project leads) receive in-depth IT security training in their area of responsibility. This training is at the employer's expense.

Media Handling

All media used by the contractor to store or process NRC information shall be controlled in accordance with the sensitivity level.

The contractor shall not perform sanitization or destruction of media approved for processing NRC information designated as SGI or Classified. The contractor must provide the media to NRC for destruction.

Vulnerability Management

The Contractor must adhere to NRC patch management processes for all systems used to process NRC information. Patch Management reports will made available to the NRC upon request for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

For any contractor system used to process NRC information, the contractor must ensure that information loaded into the system is scanned for viruses prior to posting; servers are scanned for viruses, adware, and spyware on a regular basis; and virus signatures are updated at the following frequency:

- 1 calendar day for a high sensitivity system
- 3 calendar days for a moderate sensitivity system
- 7 calendar days for a low sensitivity system

(End of Clause)

NRCH030 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (SEP 2013)

The contractor must identify all individuals selected to work under this contract. The NRC Contracting Officer's Representative (COR) shall make the final determination of the level, if any, of IT access approval required for all individuals working under this contract/order using the following guidance. The Government shall have full and complete control and discretion over granting, denying, withholding, or terminating IT access approvals for contractor personnel performing work under this contract/order.

The contractor shall conduct a preliminary security interview or review for each employee requiring IT level I or II access and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of IT access approval for which the employee has been proposed. The contractor shall pre-screen its applicants for the following:

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) years.

The contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the employee verify the pre-screening record or review, sign and date it. The contractor shall supply two (2) copies of the signed contractor's pre-screening record or review to the NRC Contracting Officer's Representative (COR), who will then provide them to the NRC Office of Administration, Division of Facilities and Security, Personnel Security Branch with the employee's completed IT access application package.

The contractor shall further ensure that its personnel complete all IT access approval security applications required by this clause within fourteen (14) calendar days of notification by the NRC Contracting Officer's Representative (COR) of initiation of the application process. Timely receipt of properly completed records of the pre-screening record and IT access approval applications (submitted for candidates that have a reasonable probability of obtaining the level of security assurance necessary for access to NRC's IT systems/data) is a requirement of this contract/order. Failure of the contractor to comply with this requirement may be a basis to

terminate the contract/order for cause, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the contractor.

SECURITY REQUIREMENTS FOR IT LEVEL I

Performance under this contract/order will involve contractor personnel who perform services requiring direct access to or operate agency sensitive information technology systems or data (IT Level I). The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access.

Contractor personnel shall not have access to sensitive information technology systems or data until they are approved by DFS/PSB and they have been so informed in writing by the NRC Contracting Officer's Representative (COR). Temporary IT access may be approved by DFS/PSB based on a favorable review or adjudication of their security forms and checks. Final IT access may be approved by DFS/PSB based on a favorably review or adjudication of a completed background investigation. However, temporary access authorization approval will be revoked and the employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract/order requiring IT access without the approval of DFS/PSB, as communicated in writing to the contractor by the NRC Contracting Officer's Representative (COR). Where temporary access authorization has been revoked or denied by DFS/PSB, the contractor shall assign another contractor employee to perform the necessary work under this contract/order without delay to the contract/order performance schedule, or without adverse impact to any other terms or conditions of the contract/order. When an individual receives final IT access approval from DFS/PSB, the individual will be subject to a reinvestigation every ten (10) years thereafter (assuming continuous performance under contract/order at NRC) or more frequently in the event of noncontinuous performance under contract/order at NRC.

CORs are responsible for submitting the completed access/clearance request package as well as other documentation that is necessary to DFS/PSB. The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (online Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to DFS/PSB for review and adjudication, prior to the individual being authorized to perform work under this contract/order requiring access to sensitive information technology systems or data. Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant

with less than seven (7) years residency in the U.S. will not be approved for IT Level I access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB. The contractor shall ensure that all forms are accurate, complete, and legible. Based on DFS/PSB review of the contractor employee's security forms and/or the receipt of adverse information by NRC, the contractor individual may be denied access to NRC facilities and sensitive information technology systems or data until a final determination is made by DFS/PSB and thereafter communicated to the contractor by the NRC Contracting Officer's Representative (COR) regarding the contractor person's eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 and SF-86 which furnishes the basis for providing security requirements to contractors that have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems and data; access on a continuing basis (in excess more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

SECURITY REQUIREMENTS FOR IT LEVEL II

Performance under this contract/order will involve contractor personnel that develop and/or analyze sensitive information technology systems or data or otherwise have access to such systems or data (IT Level II).

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions.

Contractor personnel shall not have access to sensitive information technology systems or data until they are approved by DFS/PSB and they have been so informed in writing by the NRC Contracting Officer's Representative (COR). Temporary access may be approved by DFS/PSB based on a favorable review of their security forms and checks. Final IT access may be approved by DFS/PSB based on a favorably adjudication. However, temporary access authorization approval will be revoked and the contractor employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract/order requiring IT access without the approval of DFS/PSB, as communicated in writing to the contractor by the NRC Contracting Officer's Representative (COR). Where temporary access authorization has been revoked or denied by DFS/PSB, the contractor is responsible for assigning another contractor employee to perform the necessary work under this contract/order without delay to the contract/order performance schedule, or without adverse impact to any other terms or conditions of the contract/order. When a contractor employee receives final IT access approval from DFS/PSB, the individual will be subject to a review or reinvestigation every ten (10) years (assuming continuous performance under contract/order at NRC) or more frequently in the event of

noncontinuous performance under contract/order at NRC.

CORs are responsible for submitting the completed access/clearance request package as well as other documentation that is necessary to DFS/PSB. The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (online Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to DFS/PSB for review and adjudication, prior to the contractor employee being authorized to perform work under this contract/order. Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than seven (7) years residency in the U.S. will not be approved for IT Level II access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB. The contractor shall ensure that all forms are accurate, complete, and legible. Based on DFS/PSB review of the contractor employee's security forms and/or the receipt of adverse information by NRC, the contractor employee may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made by DFS/PSB regarding the contractor person's eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187, SF-86, and contractor's record of the pre-screening which furnishes the basis for providing security requirements to contractors that have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems or data; access on a continuing basis (in excess of more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for IT access is to be withdrawn or canceled, the contractor shall immediately notify the NRC Contracting Officer's Representative (COR) by telephone so that the access review may be promptly discontinued. The notification shall contain the full name of the contractor employee and the date of the request. Telephone notifications must be promptly confirmed by the contractor in writing to the NRC Contracting Officer's Representative (COR), who will forward the confirmation to DFS/PSB. Additionally, the contractor shall immediately notify the NRC Contracting Officer's Representative (COR) in writing, who will in turn notify DFS/PSB, when a contractor employee no longer requires access to NRC sensitive automated information technology systems or data, including the voluntary or involuntary separation of employment of a contractor employee who has been approved for or is being processed for IT access.

The contractor shall flow the requirements of this clause down into all subcontracts and agreements with consultants for work that requires them to access NRC IT resources.

(End of Clause)

NRCH020 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (SEP 2013)

The Contractor shall ensure that all its employees, subcontractor employees or consultants who are assigned to perform the work herein for contract performance for periods of more than 30 calendar days at NRC facilities, are approved by the NRC for unescorted NRC building access.

The Contractor shall conduct a preliminary federal facilities security screening interview or review for each of its employees, subcontractor employees, and consultants and submit to the NRC only the names of candidates for contract performance that have a reasonable probability of obtaining approval necessary for access to NRC's federal facilities. The Contractor shall pre-screen its applicants for the following:

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) years.

The Contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the applicant verify the pre-screening record or review, sign and date it. Two (2) copies of the pre-screening signed record or review shall be supplied to the Division of Facilities and Security, Personnel Security Branch (DFS/PSB) with the Contractor employee's completed building access application package.

The Contractor shall further ensure that its employees, any subcontractor employees and consultants complete all building access security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed records of the Contractor's signed pre-screening record or review and building access security applications (submitted for candidates that have a reasonable probability of obtaining the level of access authorization necessary for access to NRC's facilities) is a contract requirement. Failure of the Contractor to comply with this contract administration requirement may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of cancellation or termination, the NRC may select another firm for contract award.

A Contractor, subcontractor employee or consultant shall not have access to NRC facilities until

he/she is approved by DFS/PSB. Temporary access may be approved based on a favorable NRC review and discretionary determination of their building access security forms. Final building access will be approved based on favorably adjudicated checks by the Government. However, temporary access approval will be revoked and the Contractor's employee may subsequently be denied access in the event the employee's investigation cannot be favorably determined by the NRC. Such employee will not be authorized to work under any NRC contract requiring building access without the approval of DFS/PSB. When an individual receives final access, the individual will be subject to a review or reinvestigation every five (5) or ten (10) years, depending on their job responsibilities at the NRC.

The Government shall have and exercise full and complete control and discretion over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. Individuals performing work under this contract at NRC facilities for a period of more than 30 calendar days shall be required to complete and submit to the Contractor representative an acceptable OPM Standard Form 85 (Questionnaire for Non-Sensitive Positions), and two (2) FD 258 (Fingerprint Charts). Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than five (5) years residency in the U.S. will not be approved for building access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB.

DFS/PSB may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the OPM Standard Form 85 and the Contractor's pre-screening record. Also, in the exercise of its authority, the Government may, among other things, grant or deny permanent building access approval based on the results of its review or investigation. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the NRC work sites for an extended period of time during the term of the contract. In the event that DFS/PSB are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the Contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The Contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

CANCELLATION OR TERMINATION OF BUILDING ACCESS/ REQUEST

The Contractor shall immediately notify the COR when a Contractor or subcontractor employee or consultant's need for NRC building access approval is withdrawn or the need by the Contractor employee's for building access terminates. The COR will immediately notify DFS/PSB (via e-mail) when a Contractor employee no longer requires building access. The Contractor shall be required to return any NRC issued badges to the COR for return to DFS/FSB (Facilities Security Branch) within three (3) days after their termination.

(End of Clause)

REGISTRATION IN FEDCONNECT® (JULY 2014)

The Nuclear Regulatory Commission (NRC) uses Compusearch Software Systems' secure and auditable two-way web portal, FedConnect®, to communicate with vendors and contractors. FedConnect® provides bi-directional communication between the vendor/contractor and the NRC throughout pre-award, award, and post-award acquisition phases. Therefore, in order to do business with the NRC, vendors and contractors must register to use FedConnect® at https://www.fedconnect.net/FedConnect. The individual registering in FedConnect® must have authority to bind the vendor/contractor. There is no charge for using FedConnect®. Assistance with FedConnect® is provided by Compusearch Software Systems, not the NRC. FedConnect® contact and assistance information is provided on the FedConnect® web site at https://www.fedconnect.net/FedConnect.

I.3 NRC Acquisition Regulation (48 CFR Chapter 20)

§2052.209-72 Contractor organizational conflicts of interest.

(d) Purpose. The primary purpose of this clause is to aid in ensuring that the contractor:

(1) Is not placed in a conflicting role because of current or planned interests (financial, contractual, organizational, or otherwise) which relate to the work under this contract; and

(2) Does not obtain an unfair competitive advantage over other parties by virtue of its performance of this contract.

(e) Scope. The restrictions described apply to performance or participation by the contractor, as defined in 48 CFR 2009.570-2 in the activities covered by this clause.

(f) Work for others.

(1) Notwithstanding any other provision of this contract, during the term of this contract, the contractor agrees to forego entering into consulting or other contractual arrangements with any firm or organization the result of which may give rise to a conflict of interest with respect to the work being performed under this contract. The contractor shall ensure that all employees under this contract abide by the provision of this clause. If the contractor has reason to believe, with respect to itself or any employee, that any proposed consultant or other contractual arrangement with any firm or organization may involve a potential conflict of interest, the contractor shall obtain the written approval of the contracting officer before the execution of such contractual arrangement.

(2) The contractor may not represent, assist, or otherwise support an NRC licensee or applicant undergoing an NRC audit, inspection, or review where the activities that are the subject of the

audit, inspection, or review are the same as or substantially similar to the services within the scope of this contract (or task order as appropriate) except where the NRC licensee or applicant requires the contractor's support to explain or defend the contractor's prior work for the utility or other entity which NRC questions.

(3) When the contractor performs work for the NRC under this contract at any NRC licensee or applicant site, the contractor shall neither solicit nor perform work in the same or similar technical area for that licensee or applicant organization for a period commencing with the award of the task order or beginning of work on the site (if not a task order contract) and ending one year after completion of all work under the associated task order, or last time at the site (if not a task order contract).

(4) When the contractor performs work for the NRC under this contract at any NRC licensee or applicant site,

(i) The contractor may not solicit work at that site for that licensee or applicant during the period of performance of the task order or the contract, as appropriate.

(ii) The contractor may not perform work at that site for that licensee or applicant during the period of performance of the task order or the contract, as appropriate, and for one year thereafter.

(iii) Notwithstanding the foregoing, the contracting officer may authorize the contractor to solicit or perform this type of work (except work in the same or similar technical area) if the contracting officer determines that the situation will not pose a potential for technical bias or unfair competitive advantage.

(g) Disclosure after award.

(1) The contractor warrants that to the best of its knowledge and belief, and except as otherwise set forth in this contract, that it does not have any organizational conflicts of interest as defined in 48 CFR 2009.570-2.

(2) The contractor agrees that if, after award, it discovers organizational conflicts of interest with respect to this contract, it shall make an immediate and full disclosure in writing to the contracting officer. This statement must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. The NRC may, however, terminate the contract if termination is in the best interest of the Government.

(3) It is recognized that the scope of work of a task-order-type contract necessarily encompasses a broad spectrum of activities. Consequently, if this is a task-order-type contract, the contractor agrees that it will disclose all proposed new work involving NRC licensees or applicants which comes within the scope of work of the underlying contract. Further, if this contract involves

work at a licensee or applicant site, the contractor agrees to exercise diligence to discover and disclose any new work at that licensee or applicant site. This disclosure must be made before the submission of a bid or proposal to the utility or other regulated entity and must be received by the NRC at least 15 days before the proposed award date in any event, unless a written justification demonstrating urgency and due diligence to discover and disclose is provided by the contractor and approved by the contracting officer. The disclosure must include the statement of work, the dollar value of the proposed contract, and any other documents that are needed to fully describe the proposed work for the regulated utility or other regulated entity. NRC may deny approval of the disclosed work only when the NRC has issued a task order which includes the technical area and, if site-specific, the site, or has plans to issue a task order which includes the technical area and, if site-specific, the site, or when the work violates paragraphs (c)(2), (c)(3) or (c)(4) of this section.

(h) Access to and use of information.

(1) If, in the performance of this contract, the contractor obtains access to information, such as NRC plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (5 U.S.C. Section 552a (1988)), or the Freedom of Information Act (5 U.S.C. Section 552 (1986)), the contractor agrees not to:

(i) Use this information for any private purpose until the information has been released to the public;

(ii) Compete for work for the Commission based on the information for a period of six months after either the completion of this contract or the release of the information to the public, whichever is first;

(iii) Submit an unsolicited proposal to the Government based on the information until one year after the release of the information to the public; or

(iv) Release the information without prior written approval by the contracting officer unless the information has previously been released to the public by the NRC.

(2) In addition, the contractor agrees that, to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. Section 552a (1988)), or the Freedom of Information Act (5 U.S.C. Section 552 (1986)), or other confidential or privileged technical, business, or financial information under this contract, the contractor shall treat the information in accordance with restrictions placed on use of the information.

(3) Subject to patent and security provisions of this contract, the contractor shall have the right to use technical data it produces under this contract for private purposes provided that all requirements of this contract have been met.

(i) Subcontracts. Except as provided in 48 CFR 2009.570-2, the contractor shall include this clause, including this paragraph, in subcontracts of any tier. The terms contract, contractor, and contracting officer, must be appropriately modified to preserve the Government's rights.

(j) Remedies. For breach of any of the above restrictions, or for intentional nondisclosure or misrepresentation of any relevant interest required to be disclosed concerning this contract or for such erroneous representations that necessarily imply bad faith, the Government may terminate the contract for default, disqualify the contractor from subsequent contractual efforts, and pursue other remedies permitted by law or this contract.

(k) Waiver. A request for waiver under this clause must be directed in writing to the contracting officer in accordance with the procedures outlined in 48 CFR 2009.570-9.

(l) Follow-on effort. The contractor shall be ineligible to participate in NRC contracts, subcontracts, or proposals therefor (solicited or unsolicited) which stem directly from the contractor's performance of work under this contract. Furthermore, unless so directed in writing by the contracting officer, the contractor may not perform any technical consulting or management support services work or evaluation activities under this contract on any of its products or services or the products or services of another firm if the contractor has been substantially involved in the development or marketing of the products or services.

(1) If the contractor under this contract, prepares a complete or essentially complete statement of work or specifications, the contractor is not eligible to perform or participate in the initial contractual effort which is based on the statement of work or specifications. The contractor may not incorporate its products or services in the statement of work or specifications unless so directed in writing by the contracting officer, in which case the restrictions in this paragraph do not apply.

(2) Nothing in this paragraph precludes the contractor from offering or selling its standard commercial items to the Government.

(End of Clause)

§2052.215-71 Contracting Officer's Representative (COR) Authority (Oct 1999)

(a) The contracting officer's authorized representative hereinafter referred to as the COR for this contract is:

Name: Trisha Carr, Trisha.Carr@nrc.gov, 301-287-0760

Alternate: Henry Davis, Henry.Davis@nrc.gov, 301-415-0713

(b) Performance of the work under this contract is subject to the technical direction of the NRC COR. The term technical direction is defined to include the following:

(1) Technical direction to the contractor which shifts work emphasis between areas of work or tasks, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work or changes to specific travel identified in the Statement of Work), fills in details, or otherwise serves to accomplish the contractual statement of work.

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.

(3) Review and, where required by the contract, approve technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

(c) Technical direction must be within the general statement of work stated in the contract. The project officer does not have the authority to and may not issue any technical direction which:

(1) Constitutes an assignment of work outside the general scope of the contract.

(2) Constitutes a change as defined in the "Changes" clause of this contract.

(3) In any way causes an increase or decrease in the total estimated contract cost, the fixed fee, if any, or the time required for contract performance.

(4) Changes any of the expressed terms, conditions, or specifications of the contract.

(5) Terminates the contract, settles any claim or dispute arising under the contract, or issues any unilateral directive whatever.

(d) All technical directions must be issued in writing by the project officer or must be confirmed by the project officer in writing within ten (10) working days after verbal issuance. A copy of the written direction must be furnished to the contracting officer. A copy of NRC Form 445, Request for Approval of Official Foreign Travel, which has received final approval from the NRC must be furnished to the contracting officer.

(e) The contractor shall proceed promptly with the performance of technical directions duly issued by the project officer in the manner prescribed by this clause and within the project officer's authority under the provisions of this clause.

(f) If, in the opinion of the contractor, any instruction or direction issued by the COR is within one of the categories defined in paragraph (c) of this section, the contractor may not proceed but shall notify the contracting officer in writing within five (5) working days after the receipt of any instruction or direction and shall request that contracting officer to modify the contract accordingly. Upon receiving the notification from the contractor, the contracting officer shall issue an appropriate contract modification or advise the contractor in writing that, in the

contracting officer's opinion, the technical direction is within the scope of this article and does not constitute a change under the "Changes" clause.

(g) Any unauthorized commitment or direction issued by the COR may result in an unnecessary delay in the contractor's performance and may even result in the contractor expending funds for unallowable costs under the contract.

(h) A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect to the instruction or direction is subject to §52.233-1 - Disputes.

(i) In addition to providing technical direction as defined in paragraph (b) of the section, the project officer shall:

(1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.

(2) Assist the contractor in the resolution of technical problems encountered during performance.

(3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this contract.

(End of Clause)

§2052.215-73 Commitment of public funds

The contracting officer is the only individual who can legally commit the NRC to the expenditure of public funds in connection with this procurement. This means that, unless provided in a contract document or specifically authorized by the contracting officer, NRC technical personnel may not issue contract modifications, give informal contractual commitments, or otherwise bind, commit, or obligate the NRC contractually. Informal contractual commitments include:

(1) Encouraging a potential contractor to incur costs before receiving a contract;

(2) Requesting or requiring a contractor to make changes under a contract without formal contract modifications;

(3) Encouraging a contractor to incur costs under a cost-reimbursable contract in excess of those costs contractually allowable; and

(4) Committing the Government to a course of action with regard to a potential contract, contract change, claim, or dispute.

(End of Clause)

2052.215-78 Travel approvals and reimbursement - Alternate 1.

(a) Total expenditure for travel may not exceed $0.00 without the prior approval of the contracting officer.

(b) All foreign travel must be approved in advance by the NRC on NRC Form 445, Request for Approval of Official Foreign Travel, and must be in compliance with FAR 52.247-63 Preference for U.S. Flag Air Carriers. The contractor shall submit NRC Form 445 to the NRC no later than 30 days prior to the commencement of travel.

(c) The contractor will be reimbursed only for travel costs incurred that are directly related to this contract and are allowable subject to the limitations prescribed in FAR 31.205-46.

(d) It is the responsibility of the contractor to notify the contracting officer in accordance with the FAR Limitations of Cost clause of this contract when, at any time, the contractor learns that travel expenses will cause the contractor to exceed the travel ceiling amount identified in paragraph (a) of this clause.

(e) Reasonable travel costs for research and related activities performed at State and nonprofit institutions, in accordance with Section 12 of Pub. L. 100-679, must be charged in accordance with the contractor's institutional policy to the degree that the limitations of Office of Management and Budget (OMB) guidance are not exceeded. Applicable guidance documents include OMB Circular A-87, Cost Principles for State and Local Governments; OMB Circular A- 22, Cost Principles for Nonprofit Organizations; and OMB Circular A-21, Cost Principles for Educational Institutions.

*To be incorporated into any resultant BPA Calls.

2052.216-73 ACCELERATED TASK ORDER PROCEDURES

(a) The NRC may require the contractor to begin work before receiving a definitized BPA Call from the contracting officer. Accordingly, when the contracting officer verbally authorizes the work, the contractor shall proceed with performance of the task order subject to the monetary limitation established for the task order by the contracting officer.

(b) When this accelerated procedure is employed by the NRC, the contractor agrees to begin promptly negotiating with the contracting officer the terms of the definitive BPA Call and agrees to submit a cost proposal with supporting cost or pricing data. If agreement on a definitized task order is not reached by the target date mutually agreed upon by the contractor and contracting officer, the contracting officer may determine a reasonable price and/or fee in accordance with Subpart 15.8 and Part 31 of the FAR, subject to contractor appeal as provided in 52.233-1, Disputes. In any event, the contractor shall proceed with completion of the BPA Call subject only to the monetary limitation established by the contracting officer and the terms and conditions of the basic contract.

(End of Clause)

2052.215-70 KEY PERSONNEL. (JAN 1993)

(a) The following individual are considered to be essential to the successful performance of the work hereunder:

LABOR CATEGORY

Program Manager: [redacted]

Deputy Program Manager: [redacted]

*The contractor agrees that personnel may not be removed from the contract work or replaced without compliance with paragraphs (b) and (c) of this section.

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

(c) Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution. The contracting officer and the project officer shall evaluate the contractor's request and the contracting officer shall promptly notify the contractor of his or her decision in writing.

(d) If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

(End of Clause)

SECTION J: LIST OF ATTACHMENTS

Attachment One (1a) – Synaptek Schedule Contract

Attachment One (1b) – Edgewater Schedule Contract

Attachment Two (2) – [redacted]

Attachment Three (3) – Target Technical Standards and Architectural Requirements

Attachment Four (4) – Standards for Maintenance and Modernization

Attachment Five (5) - CSO IT Security Requirement

Attachment Six (6) – NRC Form 441

Attachment Seven (7) –NRC Form 441A

Attachment Eight (8) – NRC Form SF-328

Attachment Nine (9) – [redacted]

Attachment Ten (10) – [redacted]