

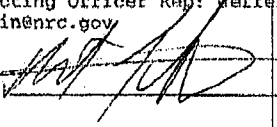
ORDER FOR SUPPLIES OR SERVICES

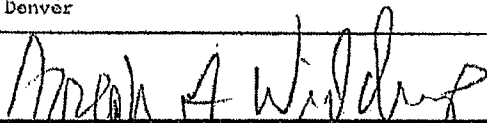
PAGE 1 OF 1 PAGES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

BPA NO.

1. DATE OF ORDER		2. CONTRACT NO. (if any) GS35P0626M		8. SHIP TO:	
3. ORDER NO. NRC-HQ-12-F-33-0001		4. REQUISITION/REFERENCE NO. OIS-12-074 11/29/11		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts, CMB3 Attn: Wanda M Brown Mail Stop: TWB-01-B10M Washington, DC 20555		6. STREET ADDRESS 11555 Rockville Pike		c. CITY Rockville	
7. TO:		d. STATE MD		e. ZIP CODE 20852	
9. NAME OF CONTRACTOR AKAMAI TECHNOLOGIES, INC.		f. SHIP VIA		10. REQUISITIONING OFFICE OIS Office of Information Services	
b. COMPANY NAME		<input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY		REFERENCE YOUR Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
c. STREET ADDRESS 11111 SUNSET HILLS RD STE 250		Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.		d. CITY RESTON e. STATE VA f. ZIP CODE 201905374	
11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input type="checkbox"/> a. SMALL <input checked="" type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) <input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)		12. F.O.B. POINT N/A		13. PLACE OF	
a. INSPECTION		b. ACCEPTANCE		14. GOVERNMENT BIL NO.	
15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)		16. DISCOUNT TERMS 30		17. SCHEDULE (See reverse for Rejections)	

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Akamai Technologies, Inc shall provide the U.S. Nuclear Regulatory Commission (NRC) with the NRC Public Web Site Content Delivery and Continuity-of Operations Service in accordance with the attached Schedule of Price and the Statement of Work (SOW). Type of Contract: Firm-Fixed-Price Akamai Contact: Lenise Gibson 703-621-4033 lgibson@akamai.com NRC Contracting Officer Rep: Jeffery Main 301-415-6849 jeffery.main@nrc.gov ACCEPTANCE: 				See CONTINUATION Page	

19. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.	
21. MAIL INVOICE TO:		a. NAME Department of Interior / NBC Email: NRCPayments@nbc.gov		17(h) TOTAL (Cont. pages)	
b. STREET ADDRESS (or P.O. Box) Attn: Fiscal Services Branch - D2770 7301 W. Mansfield Avenue		PHONE: FAX:		17(i) GRAND TOTAL	
c. CITY Denver		d. STATE CO		e. ZIP CODE 80235-2230	
22. UNITED STATES OF AMERICA BY (Signature) 		23. NAME (Typed) Joseph L. Widdup Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER		\$329,692.00	

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE
Akamai Technologies, Inc. 328.1

SUNSI REVIEW COMPLETE

APR 5 2012

OPTIONAL FORM 347 (REV. 5/2011)
PRESCRIBED BY GSA/FAR 48 CFR 53.213(f)

ADMO02

Table of Contents

SECTION B - CONTINUATION BLOCK	B-1
B.1 PERIOD OF PERFORMANCE (AUG 2011)	B-5
B.2 OBLIGATION AND CONSIDERATION.....	B-1
B.3 PRICE SCHEDULE.....	B-3
SECTION C - CONTRACT CLAUSES	C-1
C.1 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)	C-1
C.2 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)	C-1
C.3 2052.215-71 PROJECT OFFICER AUTHORITY (NOVEMBER 2006)	C-1
C.4 52.224-2 PRIVACY ACT (APR 1984)	C-3
C.5 2052.204.70 SECURITY (MAR 2004).....	C-4
C.6 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (AUG 2011)	C-5
C.7 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MAR 2006).....	C-8
C.8 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2011).....	C-8
C.9 ELECTRONIC PAYMENT (AUG 2011).....	C-9
C.10 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS (AUG 2011).....	C-9
C.11 GREEN PURCHASING (JUN 2011)	C-10
C.12 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS (AUG 2011).....	C-11
C.13 52.237-3 CONTINUITY OF SERVICES (JAN 1991).....	C-11

BILLING INSTRUCTIONS FOR FIXED-PRICE TYPE CONTRACTS (JULY 2011)

**STATEMENT OF WORK (SOW)
SOLICITATION NO. RFQ-OIS-12-074**

Table of Contents

1	Introduction.....	4
2	Background.....	4
3	Objective.....	4
4	Scope and Schedule of Work.....	5
5	General Requirements.....	12
6	Security Requirements.....	16
7	Review and Approval of Reports.....	17
	Attachment 1: Monthly Status Report Guidance.....	19
	Attachment 3: References for Creating Documentation to Validate Compliancy.....	21
	Attachment 4: Contract Security and/or Classification Requirements (NRC Form 187).....	24
	Attachment 5: Acronyms and Abbreviations.....	25
	Attachment 6: Definitions.....	26

Introduction

The U.S. Nuclear Regulatory Commission (NRC) uses the Internet to conduct business with its external stakeholders around the world and to inform the broader public of news and information available from the agency. The primary means for disseminating this information is through the NRC Public Web Site (www.nrc.gov). The agency adds and revises Web content at this site each day as part of its regulatory mission of protecting the public health and safety and the environment.

In 2004, the agency first issued a contract to deliver such content in a cost-effective, reliable manner and to provide related content delivery and Continuity-Of-Operations (COOP) services in a hosted environment. Since that time, the NRC has seen the use of the Internet by both its staff and external stakeholders grow. Increasing interest in new reactor designs, the combined operating license process, nuclear waste disposal, and the agency's regulatory processes have stimulated site traffic. Several additional factors have also added complexity to the process, including new Federal Information Security Management Act of 2002 (FISMA) documentary requirements and the need for the provisioning and maintenance of a full backup site to maintain COOP in the event the NRC origin server becomes unavailable for an extended period of time.

Background

The NRC's existing Content Delivery Network (CDN) contractor provides the agency with world-wide delivery across Akamai Technologies' distributed network, ensuring not only that our Public Site remains available should our origin server be offline, but also that the site content is routed to users world-wide across an optimized path to minimize packet loss, even in the event of a regional outage of the Internet. Another contractor-provided service shields NRC servers from international Internet Protocol (IP) traffic. The contractor backs up all site Web pages on numerous, geographically distant servers collocated at internet service providers calculated to be near the end user. In this way, only a small percentage of traffic requires end-to-end transit, minimizing the time required for page delivery.

Since the service was first acquired in 2004, much time and effort has been spent providing a finely tuned configuration of Akamai Technologies' Commercial Off-The-Shelf (COTS) delivery algorithm such that the service is tailored specifically to the NRC's delivery needs at a file and folder level without any custom software development. Akamai's secure, web-based portal provides the NRC technical team with the ability to manage minor changes to this configuration in a robust fashion with full revision tracking, quality control, and roll-back capabilities. Using the portal, the NRC technical staff can also quickly mitigate information spills world-wide in under 10 minutes with no intervention by Akamai support staff. In addition, the NRC can view near real-time graphical usage statistics in the portal. These statistics can be extensively configured and also scheduled for periodic email delivery through this portal, again with no intervention by Akamai support staff.

Objective

The purpose of this contract is to acquire maintenance and expand assistance to distribute and deliver HTTP content and provide COOP services for the NRC Public Web Site (www.nrc.gov). The Contractor shall provide the NRC with an integrated solution that includes continuous Public

Web Site caching, backup and spidering, content delivery, application scripting, monitoring, reporting tools and automatic fail-over capabilities 24 hours a day, 365 days a year.

Scope and Schedule of Work

General Description

The contractor shall provide several components, the first of which is to continue the existing level of service provided for guaranteed 99.999% uptime for Public Web content delivery and failover without interruption. Delivery shall be provided through an existing world-wide network of computer servers operated by the Contractor. The servers shall be co-located in the data centers of Internet Service Providers on 6 continents such that at least 75% of Internet users around the world shall be within one "hop" (server connection) of a server operated by the Contractor. The delivery shall encompass both temporary (cached) and long-term (backup) storage of content hosted on the Contractor's server network. The content hosted in the Contractor-provided backup storage shall be refreshed from the NRC's origin server by a Contractor-provided Web crawling service. Statistical reports, content control features, and configuration options for these services shall be provided to the NRC by means of a Web-based, secure portal. Finally, the Contractor shall provide service documentation to the NRC on the technical and security aspects of the services and supporting infrastructure. The schedule and details of these services are provided below.

Schedule of Tasks and Deliverables

Task	Description	Due Date
5.1	Deliver Public Web Content	Beginning on 2/1/2012
5.2	Provide for Continuity of Operations	Beginning on 2/1/2012
5.3	Provide Access to Web Server Statistics and Reporting Tools	Beginning on 2/1/2012
5.4	Provide project documentation	April 20, 2012 (except as stated in section 5.4.2)
5.5	Provide Professional Services	6 hours per month
5.6	Configure NRC Digital Properties for IPv4/IPv6 Dual Stack Delivery	May 30, 2012

Task 1 – Deliver Public Web Content

The Contractor shall dynamically cache and distribute the NRC public web-site throughout the world.

Size of Network

The Contractor shall provide distributed delivery of NRC web defined properties with a minimum HTTP outbound bandwidth requirement of 15 Mbps, scalable to 32Mbps.

The Contractor shall provide a distributed network that consists of a world-wide deployment to provide for a global reach and maximize performance objectives in order to accommodate unpredictable load increases (flash crowds) and Internet-wide projected growth. This network shall ensure that Distributed Denial-of-Service attacks (DDoS) are absorbed without incident and shall include the following:

1. Caching servers shall be deployed globally in a minimum of fifty countries on six continents.
2. These servers shall be deployed in a minimum of 750 different telecommunications and internet service provider networks.
3. These servers shall be deployed within the networks of at least five different network providers in the State of Maryland.
4. There shall be a minimum of 1000 of these servers deployed within the United States of America.

Servers within the United States of America shall be physically deployed in diverse physical locations throughout the country, and be distributed throughout various regions of the North American continent.

No requests for content from the NRC routed through the Contractor's network shall be sent to the NRC from a server located outside North America (although the request may be received by the Contractor from outside North America and it may be routed through intermediary servers within portions of the Contractor's network located outside North America).

Simplicity

The Contractor shall reduce the bandwidth demand and load utilization on the current NRC Headquarters infrastructure located in Rockville, Maryland, be integrated into the existing infrastructure, and not require additional equipment or dedicated links. The amount of load reduction shall be at least 15% (with total requests reduced by at least 70%) as a monthly average.

The Contractor shall dynamically direct end users to the "optimal" caching server without NRC or end user intervention.

NRC Web Content Control Utilities

The Contractor shall provide the utilities that allow the NRC full control of business rules, delivered web content, and the origin server at all times. This shall include all applications and management tools to allow for object-level control and content purging and pushing. The Contractor shall offer NRC complete control over its content on the Contractor's distributed network. Specifically, NRC requires the ability to purge outdated information from the Contractor's network. The NRC also requires the ability to "push" critical information out across the Contractor's network during periods where immediate availability of new content is critical. The NRC shall also be able to customize refresh rates for individual pages based on NRC determined assumptions on the "shelf-life" of the content presented in the page.

Growth Capacity

The Contractor's network shall be capable of facilitating future NRC growth by providing optimal path selection from edge servers making requests to the origin infrastructure to determine the fastest routes through the Internet to support secure and non-secure content delivery transactions.

Service Level Agreement

The Contractor shall provide a service level agreement of 100% for Web site availability and functionality. The site delivery solution shall be a continuous service that is available 24 hours a day, 7 days a week, 365 days a year (24/7/365).

Task 2 – Provide for Continuity of Operations

The Contractor shall provide a live, real-time, “hot-site”, fail-over solution for the NRC public web server, continuous monitoring of the NRC origin site, and protection against Distributed Denial of Service (DDoS) attacks. The Contractor shall monitor the NRC origin site with the capability to automatically and instantaneously switch to Web content stored on the Contractor's off-site network, while preventing the NRC origin site from being exposed to DDoS attacks by shielding its Internet Protocol (IP) address from public exposure.

Site Fail-Over Service

The Contractor shall provide a dynamic, real-time, automatic site fail over service that monitors data origin and immediately switches to off-site storage if the NRC source becomes unavailable. The Contractor shall provide the following as part of the fail-over service.

- Host scalable, fault-tolerant, capacity-on-demand storage service (at least 1350 GB) in at least three locations,
- Serve the most recently cached content during fail-over,
- Automatically rollback to and deliver the cached site origin content when the NRC-hosted server becomes available,
- Enable the COR to manage all site content and control during fail-over by means of file transfer protocol (FTP), and
- Provide for integration of the Contractor's service into the existing NRC infrastructure technologies and not require additional hardware or dedicated links.

Origin Site Backup and Spidering Service

The Contractor shall host a backup copy of the NRC Public Web Site. This backup copy shall be supported by the same network infrastructure as is included in the site delivery service provided to comply with Requirement 4.1. This backup copy of the NRC Public Web Site shall be maintained through a Contractor-provided Web spidering service¹ that crawls the NRC origin at a default interval of 12 hours. The NRC shall have secure, Web-based and FTP access to update or purge content from the backup site manually. The NRC's access to the backup site shall be independent of the spidering capability. The backup site shall provide at least 1,350 GB of storage space. The NRC shall have secure, Web-based access to business rules that define the priority under which content is delivered from the backup site. The Contractor shall provide

¹ See Attachment 6, “Definitions,” for an expanded definition of *Web Spider*.

technical support to assist in modifying the business rules and other configuration details to ensure the NRC business needs are met.

The contractor shall provide configuration assistance to ensure the spidering service is properly tuned and calibrated to refresh the content at the contractor-maintained backup Web site from the NRC origin site at an interval specified by the NRC. This configuration of spidering intervals shall encompass at least 500 areas of content areas at the NRC origin site which may require separate spidering refresh rules.

Prevention of Distributed Denial of Service (DDoS) Attacks

The Contractor shall prevent the NRC origin site from being exposed to DDoS attacks by shielding its Internet Protocol (IP) address from public exposure. The Contractor shall effectively act as a proxy service, absorbing excessive traffic that does not conform to the business rules defined in the NRC site configuration of the Contractor's site delivery service. The Contractor shall provide the NRC with lists of Contractor IP addresses through which the NRC origin site will receive requests for Web objects at least 24 hours in advance of any changes to that list.

Removal of Inadvertently Released Web Content

The Contractor shall provide a Web portal interface to enable the NRC to remotely request the removal of any Public Site content by Uniform Resource Identifier (URI) from all Contractor caching servers worldwide.

Service Level Agreement

The Contractor shall provide a service level of 100% for Web site availability and functionality. The site monitoring and fail-over solution shall be a continuous service that is available 24 hours a day, 7 days a week, 365 days a year (24/7/365). The Contractor shall complete the removal of inadvertently released Public Site content within 10 minutes of request through the Contractor's Web portal.

Task 3 – Provide Access to Web Server Statistics and Reporting Tools

The Contractor shall provide and support the implementation of web site statistics tracking and monitoring tools. These tools shall be web based and enable the NRC to perform customized reports to monitor desired statistics on specified web objects and pages contained in the www.nrc.gov Web site.

Site Monitoring Tools

The Contractor shall provide web site statistics tracking and monitoring tools that enable for real-time alerts for the following:

- Bandwidth Burst
- Bandwidth Drop
- Origin Server Failure
- Origin Connect Failure

- Origin DNS Failure
- SSL Transaction Failure
- Aborted Download
- Access Denied at Origin
- Object not Found

Customized Web Object Reporting

The Contractor shall provide a means for the NRC to access a customer support portal over the web from any web browser. Available services shall include monitoring, content control, reporting, configuring, self-help and alerts.

The Contractor's Web-based tool shall allow for customized reports to monitor desired statistics on specified objects. Site access (HTTP file request) and error logs and SMTP e-mail transaction logs (syslogs) shall be easily attained by NRC or be collected and compressed in a suitable format, and sent by FTP to an NRC location, designated by the COR, each calendar day.

Web Statistics Reporting

The Contractor shall provide web accessible reporting services that enable NRC staff to monitor the following:

- Average number of concurrent streams
- Number of hits
- Minutes of content viewed
- Maximum concurrent streams
- Amount of content delivered
- Number of unique viewers
- Views by bit rate
- Most viewed Web addresses
- Traffic by geography
- Traffic trends (by hour of day, day of week, etc.)
- NRC-defined statistics on specific objects and pages

Web Traffic Statistics

The Contractor shall provide a web portal tool that allows web traffic summary information on NRC defined statistics that includes the following.

- Network bandwidth utilization
- Number of hits on popular pages

- Unique visitors by time of day and day of week
- Geographic dispersion of users accessing content
- Traffic at NRC Web sites, including number of hits and megabytes delivered

Service Level Agreement

The Contractor shall provide a service level of 100% for availability and functionality for access to site statistics and reporting. The site statistics solution shall be a continuous service that is available 24 hours a day, 7 days a week, 365 days a year (24/7/365) except for scheduled system outages for which advance notice has been provided to the Government.

Task 4 - Provide Project Documentation

All data first produced by the Contractor in performing under this contract is subject to FAR Clause 52.227-14 in contract no. GS35F0626M.

Scope of Documentation

Documentation shall address all aspects of the functional, security, and project management requirements associated with this effort.

The contractor shall provide the initial **draft** of each of the following no later than April 4, 2012:

1. System Architecture
2. Configuration Management Plan
3. System Concept of Operations
4. System Security Plan
5. Contingency Plan
6. Contingency test report
7. Initial Risk Assessment
8. Current Risk and Issues List
9. Standard Operating Procedures

The COR expects to require approximately 15 business days to review the documents provided above (i.e. approximately 45 business days from contract award).

Documentation due annually:

- Information needed for the Government to revise the annual security control test plan and associated report
- Updates to the following documents to reflect any changes to the Contractor's system used to perform requirements of this contract: System Architecture, Configuration Management Plan, System Concept of Operations, Contingency Plan, Contingency

Test Report, System Security Plan, Current Risk and Issues List, and Standard Operating Procedures

Periodic reports:

Problem Reports. The Contractor shall bring problems or potential problems affecting performance to the attention of the COR in writing as soon as possible after they are identified.
Delivery Instructions

All deliverables shall be delivered to the COR no later than the date specified in this statement of work. Deliverables are to be transmitted with a cover letter, on the Contractor's letterhead, describing the contents.

Service Level Agreement

The scope of physical access to Contractor facilities required by the Government shall be limited to a single contractor facility identified by the Government. Access shall be given to the Contractor facility. Scans may be performed at any time by the Government.

Task 5 - Provide Professional Services

The Contractor shall perform up to 6 hours per month of professional services consisting of technical and administrative tasks associated with the following.

- changes to the NRC's site configuration(s) hosted by the Contractor
- diagnosing and correcting causes of local or general latency or lapses in access to NRC site(s) delivered by the Contractor
- preventing or mitigating the effects of malicious activity directed at NRC site(s) through the Contractor's service

Service Level Agreement

The Contractor shall be available by email and telephone for up to 6 hours per month of Professional Services identified above. This service incorporates those tasks not necessary for normal service management, which are included at no additional charge under the Technical Support requirement in Section 6.

Task 6 – Configure NRC Digital Properties for IPv4/IPv6 Dual Stack Delivery

The Contractor shall perform all tasks necessary for users of NRC sites delivered through the Contractor's network to access each site at either an IPv4 or IPv6 address without requiring any change to the NRC's IPv4 origin site or infrastructure. Tasks include the following.

1. Review existing hosted configurations for IPv6 feature compatibility
2. Review existing hostnames and maps
3. Modify existing configuration to enable IPv6 portal features
4. Upgrade existing hosted configuration to support IPv6, deploy to staging
5. Regression test all active features over IPv4 and IPv6 in staging

6. Deploy hosted configuration to production
7. Regression test all active features over IPv4 and IPv6 in production
8. Migrate hostname to dual-stack compliance map
9. Use same hosted configuration for additional sites, if applicable

Service Level Agreement

The Contractor shall complete all tasks identified in Section 5.6 by May 30, 2012.

General Requirements

This section provides detailed information on select requirements that may apply to multiple services described in Section 4. General requirements address such topics as staffing, documentation, place of performance, technical support, continuity of service, security, and privacy. They are incorporated by reference throughout Section 4.

Staffing Requirements and Contractor-Furnished Items

The Contractor shall provide qualified personnel, equipment, tools, materials, supervision, and other items and services necessary to successfully perform all analytical, technical, administrative, and clerical support tasks as defined in this statement of work with the exception of all Government furnished property, materials, supplies, and services specifically identified in this contract.

The Contractor shall furnish its own IT equipment, IT services, and IT access necessary to complete this effort except as specifically stated in this statement of work. The Government will furnish no other IT equipment, IT services or IT access, unless the NRC deems it necessary and beneficial to complete this effort.

Timeliness and Accuracy

Timeliness and accuracy are indicators of the level of performance. Customer satisfaction surveys from the NRC staff, periodic site visits by the COR, and customer complaints will also be compiled by the Government and reviewed in order to determine the Contractor's performance level.

Documentation Standards for Format, Grammar, and Mechanics

Requirement: Deliverable File Formats

Except where specifically stated otherwise, the Contractor shall provide all documentation in all the following formats: paper, Microsoft Word (version 2003), and Adobe PDF (version 7.0) formats.

Requirement: Draft and Final Submission

All documentation shall be submitted in draft form for review and written comment by the COR.

The Contractor shall incorporate into the final documentation any written comments received from the COR on the draft documentation.

Performance Criterion

The COR will review all draft documents submitted as part of contract deliverables for conformity to the standards referenced in this requirement. The first revision cycle for a deliverable shall be complete when the Contractor submits a revised deliverable incorporating any comments and suggestions made by the COR on their review of the initial draft.

Technical Support

Performance Criterion for Email Support

Wait time for email responses for email support requests shall not exceed 3 hours. Automated generic email responses shall not be considered to meet this criterion.

Performance Criterion for Telephone Support

Wait time (including call-back time for pager messages) for telephone support calls shall not exceed 3 hours. Automated generic telephone responses shall not be considered to meet this criterion.

Place of Performance for Project Management, Technical Support, and Other Services

The place of performance shall be at the Contractor's facility and shall be within the continental United States of America. The Contractor shall have broadband access and computers for all personnel working on these or subsequent efforts. The Contractor may have its employees work at their location or the employee's home (provided the employee's home has broadband access and the required IT equipment).

Electronic Connectivity with NRC Users and Infrastructure

All services provided under this contract shall operate physically and logically separate from the NRC's physical IT infrastructure.

All electronic connections between the services provided under this contract and the NRC user shall be established by HTTPS or SFTP.

The requirements for an NRC user to interact with the service shall be limited to the following:

- access rights granted by the NRC administrator
- personal computer with a connection to the Internet
- Microsoft Internet Explorer 6.0+ or Firefox 2.0+ (supporting 128-bit secure sockets layer connectivity)

Period of Performance

The period of performance is 2/1/12-1/31/13. Subject to FAR clause 52.217-9, the NRC may exercise the option at its discretion to extend the term of the contract by six months.

Hours of Operation

Duty Hours

The Contractor shall provide technical support twenty four (24) hours a day, seven (7) days a week, Monday through Sunday. The Contractor must, at all times, maintain an adequate work force for the uninterrupted performance of all tasks defined within this statement of work.

Contractor Performance on Federal Holidays

The Contractor is required to provide service on nationally observed Federal holidays: New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

Continuity of Services

The Contractor recognizes that the services under this contract are considered vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another Contractor, may continue them. The Contractor agrees to (1) furnish phase-in training and (2) exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

Computer Security and Privacy Requirements

Within 30 days of contract award, the Contractor shall provide documentary proof to the COR to certify the training of all employees involved in the management, use, design, development, maintenance or operation of an application or automated information system in the rules and requirements pertaining to security of the respective Federal IT systems, which they access, operate, or manage. Training shall be consistent with guidance issued by the OMB and NIST Special Publication 800-16. Within 30 days of hire, the Contractor shall provide documentary proof to the COR that each new employee has been trained. Computer security awareness refresher training is required at least annually or whenever there is a significant change in IT. Within 30 days of the completion of such refresher training, the Contractor shall provide documentary proof to the COR.

Government Observations

The COR and their designees may, from time-to-time, observe or inspect Contractor operations. However, these personnel may not interfere with Contractor performance. The Contractor shall provide reasonable assistance and information for these observations, as requested by these Government personnel.

Quality Control

The Contractor shall provide the following:

Performance Evaluation Meetings

The Contractor may be required to meet at least weekly with the COR during the first month of the contract. Meetings may be conducted by conference call or using an Internet meeting service of the contractor's choice. Meetings will be as often as necessary thereafter as determined by the COR. However, if the Contractor requests, a meeting will be held whenever a Contract Discrepancy Report (CDR) is issued. The written minutes of all performance evaluation meetings shall be prepared by the Government and signed by an authorized representative of the Contractor and the COR. Should the Contractor not concur with the minutes, the Contractor shall so state any areas of non-concurrence in writing to the COR within ten calendar days of receipt of the signed minutes. The minutes will be included in the COR's contract file.

Inclement Weather

The COR will provide the NRC policy regarding weather emergencies within seven days after award. The Contractor and COR shall coordinate a plan to communicate the closing of NRC facilities during inclement weather.

Support for Internet Protocol Version 6

The Contractor shall provide an Internet Protocol Version 6 (IPV6) compliant product or system capable of receiving, processing, transmitting, and forwarding as appropriate IPV6 packets and should interoperate with other systems and protocols in both the IPV4 and IPV6 modes of operation. Specifically, the Contractor shall provide a product or system that

1. interoperates with both IPV6 and IPV4 systems and products, and
2. if not initially compliant provide a migration path and commitment to upgrade to IPV6 for all application and product features within 90 days of the identification of noncompliance.

The Contractor shall provide IPV6 technical support for development and implementation and fielded product management. Further information on IPV6 requirements are available at <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf> **Government-Furnished Records, Files, Documents, and Work Papers.**

The Government shall furnish appropriate records (Standard Operational Procedures, regulations, manuals, texts, briefs and the other materials associated with this project.) All records, files, documents, and work papers provided by the Government and/or generated for the Government in the performance of this contract are Government property and shall be maintained and disposed by the Government. At the time of contract completion, the Contractor shall box, label contents, and turn them over to the COR

System Availability

Public access to all content delivered by means of the services provided in this contract shall be available 100% of the time, 24 hours each day, 365 days each year for the term of the contract.

Security Requirements

The contractor shall implementing sufficient Information system security, to reasonably prevent the compromise of NRC resources for all of the systems that are interconnected with a NRC network. The NRC systems that are operated by contractor and/or vendor equipment used to process or store NRC data must comply with the following requirements and shall assist NRC with the performance of annual compliance reviews.

Information system resources include, but are not limited to, hardware, application software, system software, and information (data). Information system services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

All Contractor servers, switches, routers, and other associated hardware utilized in the performance of this contract shall be

- physically and environmentally secured,
- configured and maintained in compliance with NRC policy (including all hardware and software patches), and
- fully documented in a system concept of operations and a systems architecture to be provided to the COR.

The Contractor shall

1. maintain the existing Authority to Operate (ATO) recognized by the COR and their designees ;
2. address and comply with all NIST 800-53 requirements consistent with moderate baseline security controls specified in "References for Creating Documentation to Validate Compliancy," (Attachment 3);
3. correct any deficiencies identified in the evaluation report for the ST&E provided by the Government at the conclusion of the C&A process until a full ATO that confers full certification and accreditation from the COR is obtained; and
4. provide both remote and physical access to their facilities and NRC systems on an un-scheduled basis to NRC staff performing system scans and auditing security controls.

For connections involving a public user, the public user shall not be required to provide authentication or encryption and shall be able to log in to the NRC Production Web Site anonymously.

For connections involving a NRC user, Contractor servers shall be configured for 128-bit secure sockets layer authentication.

Processing (FIPS) Standards and Special Publications (SP) 800 Series guidance

The Contractor shall provide secure data communications (encryption, authentication, data integrity checking, key exchange, and data compression) commensurate with the risks inherent with the information sensitivity.

Review and Approval of Reports

Reporting Requirements

In addition to meeting the delivery schedule in the timely submission of any draft and final reports, summaries, data and documents that are created in the performance of this contract, the Contractor shall comply with the directions of the NRC regarding the contents of the 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 will not be deemed accepted or completed until the NRC's directions are complied with. The reports, summaries, data and related documents will be considered draft until approved by the NRC. The Contractor agrees that the direction, determinations, and decisions on approval or disapproval of reports, summaries, data and related documents created under this contract remains solely within the discretion of the NRC.

Publication of Information Developed Under This Contract

Prior to any dissemination, display, publication or release of articles, reports, summaries, data or related documents developed under the contract, the Contractor shall submit for review and approval by the NRC the proposed articles, reports, summaries, data and related documents that the Contractor intends to release, disseminate or publish to other persons, the public or any other entities. The Contractor 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 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 intends to release, display, disseminate or publish to other persons, the public or any other entities. The Contractor agrees and grants a royalty free, nonexclusive, irrevocable world-wide 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, for any governmental purpose and to have or authorize others to do so.

Identification/ Marking of Sensitive and Safeguards Information

The decision, determination or direction by the NRC that information constitutes sensitive or safeguards information remains exclusively a matter within the authority of the NRC to make. In performing the contract, the Contractor shall clearly mark sensitive and safeguards information to include for example "Official Use Only" and "Safeguards 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 forms (e.g. NRC Form 461 "Safeguards Information" and NRC Form 190B "Official Use Only") in maintaining these records and documents. The Contractor will ensure that sensitive and safeguards information is handled appropriately, maintained and protected from unauthorized disclosure. The Contractor 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), and NRC Management Directive and Handbook 12.6.

Attachments

Attachment 1: Monthly Status Report Guidance

Attachment 3: References for Creating Documentation to Validate Compliancy

Attachment 4: Contract Security and/or Classification Requirements (NRC Form 187)

Attachment 5: Acronyms and Abbreviations

Attachment 6: Definitions

Attachment 1: Monthly Status Report Guidance

Task Information

NRC contract number

Accounting Control Transaction (ACT) number and reporting period

Client agency and location

Brief task description

Reporting Period Information

- A summary of progress to date and percentage of completion by task area
- Milestones reached or, if missed, and explanation provided
- A narrative review of work accomplished during the reporting period and significant events.
- Any problems, constraints, issues, or delays encountered or anticipated and recommendations for resolution. If the recommended resolution involves a contract modification, e.g., change in work requirements, level of effort (cost) or schedule delay, the Contractor shall submit a separate letter to the contracting officer identifying the required change and estimated cost impact.
- Description of any travel or unique services provided
- Efforts planned or completed by the next report

Attachment 3: References for Creating Documentation to Validate Compliancy

Draft SP 800-72, Draft NIST Special Publication 800-72, Guidelines on PDA Forensics - see [CSRC drafts](#).

Draft SP 800-70, Draft NIST Special Publication 800-70, The NIST Security Configuration Checklists Program - see [CSRC drafts](#).

Draft SP 800-68, Draft NIST Special Publication 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist - see [CSRC drafts](#).

SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004 [Adobe PDF](#) (960 KB).

Draft SP 800-66, DRAFT Special Publication 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule see [CSRC drafts](#).

Draft SP 800-65, DRAFT Special Publication 800-65: Integrating Security into the Capital Planning and Investment Control Process - see [CSRC drafts](#).

SP 800-64, Security Considerations in the Information System Development Life Cycle, October 2003 (revised file posted July 7, 2004) [Adobe PDF](#) (1,083 KB) [Zipped PDF](#) (669 KB).

SP 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004 (revised file posted September 27, 2004) [Adobe PDF](#) (217 KB).

SP 800-61, Computer Security Incident Handling Guide, January 2004 [Adobe PDF](#) (2.71 MB) [Zipped PDF](#) (1.6 MB).

SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004 [Volume I Adobe PDF](#) (444 KB) [Volume II: Appendixes Adobe PDF](#) (2,003 KB).

SP 800-59, Guideline for Identifying an Information System as a National Security System, August 2003 [Adobe PDF](#) (95.5 KB) [Zipped PDF](#) (72.9 KB).

Draft SP 800-58, DRAFT Special Publication 800-58 : Security Considerations for Voice Over IP Systems - see [CSRC drafts](#).

Draft SP 800-57, DRAFT Special Publication 800-57 Recommendation on Key Management see [CSRC drafts](#).

Draft SP 800-56, DRAFT Special Publication 800-56, Recommendation on Key Establishment Schemes - see [CSRC drafts](#).

SP 800-55, Security Metrics Guide for Information Technology Systems, July 2003 [Adobe PDF](#) (569 KB) [Zipped PDF](#) (465 KB).

Draft SP 800-53, DRAFT NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems - see [CSRC drafts](#).

Draft SP 800-52, DRAFT Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations - see [CSRC drafts](#).

SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, September 2002 [Adobe PDF](#) (204 KB) [Zipped PDF](#) (177 KB).

SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003 [Adobe PDF](#) (4,131 KB) [Zipped PDF](#) (3,565 KB).

SP 800-49, Federal S/MIME V3 Client Profile, November 2002 [Adobe PDF](#) (151 KB) [Zipped PDF](#) (112 KB).

SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002 [Adobe PDF](#) (1,027 KB) [Zipped PDF](#) (780 KB).

SP 800-47, Security Guide for Interconnecting Information Technology Systems, September 2002 [Adobe PDF](#) (729 KB) [Zipped PDF](#) (505 KB).

SP 800-46, Security for Telecommuting and Broadband Communications, September 2002 [Adobe pdf](#) (3,779 KB) [Zipped PDF](#) (2,156 KB).

SP 800-45, Guidelines on Electronic Mail Security, September 2002 [Adobe PDF](#) (1,098 KB) [Zipped PDF](#) (1,019 KB).

SP 800-44, Guidelines on Securing Public Web Servers, September 2002 [Adobe PDF](#) (2,183 KB) [Zipped PDF](#) (2,073 KB).

SP 800-43, Systems Administration Guidance for Windows 2000 Professional, November 2002 [HTML, with security templates](#).

SP 800-42, Guideline on Network Security Testing, October 2003 [Adobe PDF](#) (1,554 KB) [Zipped PDF](#) (1,104 KB).

SP 800-41, Guidelines on Firewalls and Firewall Policy, January 2002 [Adobe PDF](#) (1,180 KB)

SP 800-40, Procedures for Handling Security Patches, September 2002 [Adobe PDF](#) (3,773 KB) [Zipped PDF](#) (1,949 KB).

SP 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, May 2004 [Adobe PDF](#) (104 KB).

Draft SP 800-38B, Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode - see [CSRC drafts](#).

SP 800-38A, Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001 [Adobe PDF](#) (225 KB).

SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004 [Adobe PDF](#) (738 KB).

SP 800-36, Guide to Selecting Information Security Products, October 2003 [Adobe PDF](#) (464 KB) [Zipped PDF](#) (339 KB).

SP 800-35, Guide to Information Technology Security Services, October 2003 [Adobe PDF](#) (2,920 KB) [Zipped PDF](#) (2,426 KB).

SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002 [Adobe PDF](#) (1,937 KB) [Zipped Adobe PDF](#) (1,164 KB).

SP 800-33, Underlying Technical Models for Information Technology Security, December 2001 [Adobe PDF](#) (453 KB).

SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001 [Adobe PDF](#) (256 KB).

SP 800-31, Intrusion Detection Systems (IDS), November 2001 [Adobe PDF](#) (851 KB).

SP 800-30, Risk Management Guide for Information Technology Systems, July 2002 [Adobe PDF](#) (479 KB).

SP 800-29, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001 [Adobe PDF](#) (274 KB).

SP 800-28, Guidelines on Active Content and Mobile Code, October 2001 [Adobe PDF](#) (498 KB)

SP 800-27 Rev. A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, June 2004 [Adobe PDF](#) (291 KB).

SP 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 [Adobe PDF](#) (1,522 KB) [MS Word .doc](#) (922 KB).

SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000 [Adobe PDF](#) (130 KB) [MS Word .doc](#) (421 KB).

SP 800-24, PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, August 2000 [Adobe PDF](#) (225 KB).

SP 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000 [Adobe PDF - Complete document](#) (837 KB) [[Part 1 of 3 PDF](#) (419 KB) [Part 2 of 3 PDF](#) (160 KB) [Part 3 of 3 PDF](#) (261 KB)] [Complete zipped PDF](#) (803 KB).

SP 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, October 2000 [Revised: May 15, 2001] [Adobe PDF](#) (1,422 KB) Errata sheet for originally published version ([Adobe PDF](#)).

SP 800-21, Guideline for Implementing Cryptography in the Federal Government, November 1999 [Adobe PDF](#) (612 KB).

SP 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, Revised April 2000 [Adobe PDF](#) (1,246 KB).

SP 800-19, Mobile Agent Security, October 1999 [Adobe PDF](#) (136 KB).

SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998 [MS Word .doc](#) (540 KB) [Adobe PDF](#) (306 KB).

Letter from CIO Council Security Committee [Adobe PDF](#) (31 KB).

SP 800-17, Modes of Operation Validation System (MOVS): Requirements and Procedures, February 1998 [Adobe PDF](#) (406 KB).

SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172), April 1998 [Pt. 1 - document: [Adobe PDF](#) (845 KB), Pt. 2 - Appendix A-D: [Adobe PDF](#) (96 KB), Part 3 - Appendix E: [Adobe PDF](#) (374 KB)].

SP 800-15, Minimum Interoperability Specification for PKI Components (MISPC), Version 1, January 1998 [Adobe PDF](#) (278 KB), [MS Word .doc](#) (339 KB), [Postscript file](#) (886 KB).

SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 [Postscript file](#) (480 KB), [WordPerfect file](#) (182 KB), [Adobe PDF](#) (188 KB).

SP 800-13, Telecommunications Security Guidelines for Telecommunications Management Network, October 1995 [WordPerfect file](#) (217 KB).

SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995 [HTML format](#).

[Postscript File 1 of 5 \(602 KB\)](#)

[Postscript File 2 of 5 \(3,051 KB\)](#)

[Postscript File 3 of 5 \(1,345 KB\)](#)

[Postscript File 4 of 5 \(575 KB\)](#)

[Postscript File 5 of 5 \(1,247 KB\)](#)

[Adobe PDF \(1,685 KB\)](#)

[Word .doc Ch. 14-20 \(313 KB\)](#)

[Word .doc extra of document \(18 KB\)](#)

**Attachment 4: Contract Security and/or Classification
Requirements (NRC Form 187)**

Attachment 5: Acronyms and Abbreviations

The following acronyms and abbreviations are used throughout this document.

ANACI	Access National Agency Check with Inquiries
ASP	Application Service Provider
ATO	Authority to Operate
CO	Contracting Officer
COR	Contracting Officer Representative
COOP	Continuity Of Operations
DAA	Designated Approving Authority
DFS	Division of Facilities and Security, NRC Office of Administration
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTE	Full Time Equivalent
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol
GB	Gigabyte
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol-Secure
IP	Internet Protocol
IT	Information Technology
LBI	Limited Background Investigation
MD	Management Directive (NRC)
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
PDF	Portable Document Format, Adobe Acrobat
PSB/DFS	Personnel Security Branch, Division of Facilities and Security
SFTP	Secure File Transfer Protocol
SITSO	Senior Information Technology Security Officer, NRC
SSL	Secure Sockets Layer
ST&E	System Test and Evaluation
TB	Terabyte
XML	eXtensible Markup Language

Attachment 6: Definitions

Critical Task

A task which is vital to the successful completion of the Government's mission and if done incorrectly or behind schedule could cause the Government irreparable harm. A critical task must be completed by the Contractor with a standard of performance of 100% accuracy (except as otherwise noted herein).

Dynamically Cache

To store data temporarily based on business rules and without client intervention.

Dynamically Direct

To route or reroute a request by algorithm through an optimal path without user intervention.

Origin Server

The Internet Web Server scanned by the Contractor's indexing server for new content at periodic intervals. Only content retrieved by the Contractor's service will be visible to the public who visit the NRC Public Web Site.

NRC Public Web Site

The only NRC Web site visible to the public at <http://www.nrc.gov>. It is delivered through this service and is periodically updated by the Contractor's indexing engine when it crawls the Origin Server.

Web Spider (or Web Crawler)

A program or automated script that browses the World Wide Web in a methodical, automated manner. This process is called *web crawling* or *spidering*. Many sites, in particular search engines, use spidering as a means of providing up-to-date data. Web crawlers are mainly used to create a copy of all the visited pages for later processing by a search engine that will index the downloaded pages to provide fast searches. Crawlers can also be used for automating maintenance tasks on a website, such as checking links or validating HTML code.

SECTION B - CONTINUATION BLOCK

Schedule of Prices – NRC-HQ-12-F-33-0001

Pricing For Monthly Service

The recurring services shown below are priced on a monthly basis. The pricing for the Base Year and the Option Period are the same rates and do not escalate.

Pricing Table Summary

Base Year (2/1/12-1/31/13)

Recurring Monthly Services	Firm Fixed Price per Month
Clin 0001-Distributed Delivery Service of NRC Content (DSA Overage Rate to be applied if monthly traffic exceeds 30mps)@290/mbps	\$8,678.00 Per Month
Clin 0002-Provide for Continuity of Operations	\$13,397.00 Per Month
(a) Netstorage	\$5,400.00
(b) Failover (Site Shield)	\$5,000.00
(c) Site Snapshot	\$2,997.00
Clin 0003-Provide for Access to Web Server Stats and Premium Reporting	\$1,316.00 Per Month
Clin 0004-Provide Project Documentation	Separately Priced
Clin 0005-Professional Serviced (fixed price)	\$2,000.00 Per Month
<i>Total Monthly Price</i>	\$25,391.00
Other Services:	
Clin 0006-Configure NRC Digital Properties for IPV6 Dual	\$25,000.00
<i>Subtotal Base Year FFP</i>	<i>(\$304,632.00)</i>
<i>Total Base Year FFP (include all 12 months)</i>	\$329,692.00

Option Period 1(2/1/13-7/31/13)

Recurring Monthly Services	Firm Fixed Price per Month
Clin 1001-Distributed Delivery Service of NRC Content (DSA Overage Rate to be applied if monthly traffic exceeds 30mps)@290/mbps	\$8,678.00 Per Month
Clin 1002-Provide for Continuity of Operations	\$13,397.00 Per Month
(a) Netstorage	\$5,400.00
(b) Failover (Site Shield)	\$5,000.00
(c) Site Snapshot	\$2,997.00

Clin 1003-Provide for Access to Web Server Stats and Premium Reporting	\$1,316.00 Per Month
Clin 1004-Provide Project Documentation	Separately Priced
Clin 1005-Professional Services (fixed price)	\$2,000.00 Per Month
<i>Monthly Price FFP</i>	\$25,391.00
<i>Subtotal Option Period 1 FFP</i>	<i>(\$152,346.00)</i>
<i>Total Option Period 1 FFP</i>	\$152,346.00
<i>Total Base Period and Option Period FFP</i>	\$482,038.00

Travel is **NOT** required to complete the work as defined in the 'In Scope' section of the SOW.

B.1 PERIOD OF PERFORMANCE (AUG 2011):

The period of performance of this contact is February 1, 2012, through January 31, 2013 (one year) for the base period. The term of the contact may be extended at the option of the government for an additional six months period as follows:

Option Period: February 1, 2013 through July 31, 2013

B.2 CONSIDERATION AND OBLIGATION—FIRM FIXED PRICE (JUN 1988):

The firm fixed price of this contract is \$482,038.00 (inclusive of all option periods).

Base Period: \$329,692.00

Option Period: \$152,346.00

Total Periods: \$482,038.00

SECTION C - CONTRACT CLAUSES**C.1 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within the contract period; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed eighteen months.

C.2 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond March 18, 2013. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond March 18, 2013, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

C.3 2052.215-71 CONTRACTING OFFICER REPRESENTATIVE

(a) The contracting officer's authorized representative (hereinafter referred to as the COR) for this contract is:

Name: Jeffrey Main

Address: U.S. Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852
jeffrey.main@nrc.gov

Telephone Number: 301-415-6845

Name: Jun Lee (Alternate COR)

Address: U.S. Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852
Jun.lee@nrc.gov

Telephone Number: 301-415-1337

(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 (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

(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, approval of 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 COR 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 COR or must be confirmed by the COR 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 COR 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 as 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 the 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 thereto is subject to 52.233-1 -Disputes.

(i) In addition to providing technical direction as defined in paragraph (b) of the section, the COR 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.

(4) Assist the contractor in obtaining the badges for the contractor personnel.

(5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination.

(6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.

(7) For contracts for the design, development, maintenance or operation of Privacy Act Systems of Records, obtain from the contractor as part of closeout procedures, written certification that the contractor has returned to NRC, transferred to the successor contractor, or destroyed at the end of the contract in accordance with instructions provided by the NRC Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

C.4 52.224-2 PRIVACY ACT (APR 1984)

(a) The Contractor agrees to--

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

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to the Act; and

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

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

(c) (1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

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

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

C.5 2052.204.70 SECURITY (MAR 2004)

(a) Contract Security and/or Classification Requirements (NRC Form 187). The policies, procedures, and criteria of the NRC Security Program, NRC Management Directive (MD) 12 (including MD 12.1, "NRC Facility Security Program;" MD 12.2, "NRC Classified Information Security Program;" MD 12.3, "NRC Personnel Security Program;" MD 12.4, "NRC Telecommunications Systems Security Program;" MD 12.5, "NRC Automated Information Systems Security Program;" and MD 12.6, "NRC Sensitive Unclassified Information Security Program"), apply to performance of this contract, subcontract or other activity. This MD is incorporated into this contract by reference as though fully set forth herein. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (e.g., Safeguards), access to sensitive Information Technology (IT) systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants.

(b) It is the contractor's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for protecting National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the contracting officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, safeguards information, or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub. L. 93.579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor shall ensure that information protected from public disclosure is maintained as required by NRC regulations and policies, as cited in this contract or as otherwise provided by the NRC. The contractor will not directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security (DFS) and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

The contractor agrees to comply with the security requirements set forth in NRC Management Directive 12.1, NRC Facility Security Program which is incorporated into this contract by reference as though fully set forth herein. Attention is directed specifically to the section titled "Infractions and Violations," including "Administrative Actions" and "Reporting Infractions."

(e) Definition of National Security Information. The term National Security Information, as used in this clause, means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(f) Definition of Restricted Data. The term Restricted Data, as used in this clause, means all data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but does not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

(g) Definition of Formerly Restricted Data. The term Formerly Restricted Data, as used in this clause, means all data removed from the Restricted Data category under Section 142-d of the Atomic Energy Act of 1954, as amended.

(h) Definition of Safeguards Information. Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

(i) Security Clearance. The contractor may not permit any individual to have access to Restricted Data, Formerly Restricted Data, or other classified information, except in accordance with the Atomic Energy Act of 1954, as amended, and the Commission's regulations or requirements applicable to the particular type or category of classified information to which access is required. The contractor shall also execute a Standard Form 312, Classified Information Nondisclosure Agreement, when access to classified information is required.

(j) Criminal Liabilities. It is understood that disclosure of National Security Information, Restricted Data, and Formerly Restricted Data relating to the work or services ordered hereunder to any person not entitled to receive it, or failure to safeguard any Restricted Data, Formerly Restricted Data, or any other classified matter that may come to the contractor or any person under the contractor's control in connection with work under this contract, may subject the contractor, its agents, employees, or subcontractors to criminal liability under the laws of the United States. (See the Atomic Energy Act of 1954, as amended; 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794; and Executive Order 12958.)

(k) Subcontracts and Purchase Orders. Except as otherwise authorized in writing by the contracting officer, the contractor shall insert provisions similar to the foregoing in all subcontracts and purchase orders under this contract.

(l) In performing the contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued hereunder involving the origination or generation of classified documents, material, and equipment must provide that the subcontractor or supplier assign classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

C.6 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (AUG 2011)

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 favorable 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.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to the NRC PO who will then provide them 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 favorable 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.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, through the NRC Contracting Officer's Representative (COR) 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.

C.7 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MAR 2006)

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that the individual has been approved for unescorted access after a favorable adjudication from the Security Branch, Division of Facilities and Security (SB/DFS).

In this regard, all contractor personnel whose duties under this contract require their presence on site shall be clearly identifiable by a distinctive badge furnished by the NRC. The Project Officer shall assist the contractor in obtaining badges for the contractor personnel. All contractor personnel must present two forms of Identity Source Documents (I-9). One of the documents must be a valid picture ID issued by a state or by the Federal Government. Original I-9 documents must be presented in person for certification. A list of acceptable documents can be found at http://www.usdoj.gov/crt/recruit_employ/i9form.pdf. It is the sole responsibility of the contractor to ensure that each employee has a proper NRC-issued identification/badge at all times. All photo-identification badges must be immediately (no later than three days) delivered to SB/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must display any NRC issued badge in clear view at all times during on site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work, and to assure the protection of any Government records or data that contractor personnel may come into contact with.

C.8 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.

C.9 ELECTRONIC PAYMENT (AUG 2011)

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 the Department of the Interior at NRCPayments_NBCDenver@nbc.gov. If the contractor submits a hard copy of the invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

C.10 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS (AUG 2011)

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.

C.11 GREEN PURCHASING (JUN 2011)

(a) In furtherance of the sustainable acquisition goals of Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance" products and services provided under this contract/order shall be energy- efficient (Energy Star or Federal Energy Management Program (FEMP) designated), water-efficient, biobased, environmentally preferable (e.g., Electronic Product Environmental Assessment Tool (EPEAT) certified), non-ozone depleting, contain recycled content, or are non-toxic or less toxic alternatives, where such products and services meet agency performance requirements. <http://www.fedcenter.gov/programs/eo13514/>

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

C.12 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS (AUG 2011)

The Debt Collection Improvement Act of 1996 requires that all Federal payments except IRS tax refunds be made by Electronic Funds Transfer. It 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.

C.13 52.237-3 CONTINUITY OF SERVICES (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to (1) furnish phase-in training and (2) exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

BILLING INSTRUCTIONS FOR FIXED-PRICE TYPE CONTRACTS (JULY 2011)

INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL (SAMPLE FORMAT - COVER SHEET)

1. Official Agency Billing Office

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

2. Invoice/Voucher Information

- a. Payee's DUNS Number or DUNS+4. The Payee shall include the Payee's Data Universal Number (DUNS) or DUNS+4 number that identifies the Payee's name and address. The DUNS+4 number is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the Payee to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.
- b. Payee's Name and Address. Show the name of the Payee as it appears in the contract and its correct address. Where the Payee is authorized to assign the proceeds of this contract in accordance with the clause at FAR 52.232-23, the Payee shall require as a condition of any such assignment, that the assignee shall register separately in the Central Contractor Registration (CCR) database at <http://www.ccr.gov> and shall be paid by EFT in accordance with the terms of this contract. See Federal Acquisition Regulation 52.232-33(g) Payment by Electronic Funds Transfer - Central Contractor Registration (October 2003).
- c. Contract Number. Insert the NRC contract number (including Enterprise-wide Contract (EWC)), GSA Federal Supply Schedule (FSS), Governmentwide Agency Contract (GWAC) number, or Multiple Agency Contract (MAC) number, as applicable.
- d. Task Order Number. Insert the task/delivery order number (If Applicable). **Do not include more than one task order per invoice or the invoice may be rejected as improper.**
- e. Invoice/Voucher. The appropriate sequential number of the invoice/voucher, beginning with 001 should be designated. Contractors may also include an individual internal accounting number, if desired, in addition to the 3-digit sequential number.
- f. Date of Invoice/Voucher. Insert the date the invoice/voucher is prepared.
- g. Billing Period. Insert the beginning and ending dates (day, month, year) of the period during which deliverables were completed and for which payment is requested.
- h. Description of Deliverables. Provide a brief description of supplies or services, quantity, unit price, and total price.

- i. Work Completed. Provide a general summary description of the services performed or products submitted for the invoice period and specify the section or Contract Line Item Number (CLIN) or SubCLIN in the contract pertaining to the specified contract deliverable(s).
- j. Shipping. Insert weight and zone of shipment, if shipped by parcel post.
- k. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.
- l. Instructions. Include instructions to consignee to notify the Contracting Officer of receipt of shipment.
- m. For Indefinite Delivery contracts, the final invoice/voucher shall be marked "FINAL INVOICE" or "FINAL VOUCHER".
- n. Total Amount Billed. Insert columns for total amounts for the current and cumulative periods.
- o. Adjustments. Insert columns for any adjustments, including outstanding suspensions for deficient or defective products or nonconforming services, for the current and cumulative periods.
- p. Grand Totals.

