

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

1. REQUISITION NO. OIS-08-336 PAGE 1 OF 30

CONTRACT NO. GS35F0153M 3. AWARD/EFFECTIVE DATE **JUN 23 2008** 4. ORDER NO. NRC-DR-33-08-307 5. SOLICITATION NUMBER OIS-08-307 6. SOLICITATION ISSUE DATE

FOR SOLICITATION INFORMATION CALL: a. NAME MICHAEL TURNER b. TELEPHONE NO. (No Collect Calls) (301) 415-6535 8. OFFER DUE DATE/LOCAL TIME

ISSUED BY U.S. Nuclear Regulatory Commission Division of Contracts ATTN: Michael Turner Two White Flint North - MS T-7-I-2 Washington, DC 20555 CODE 10. THIS ACQUISITION IS  UNRESTRICTED OR  SET ASIDE: % FOR:  SMALL BUSINESS  EMERGING SMALL BUSINESS  HUBZONE SMALL BUSINESS  SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS  8(A) NAICS: SIZE STANDARD:

1. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED  SEE SCHEDULE 12. DISCOUNT TERMS Net 30 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)  13b. RATING N/A 14. METHOD OF SOLICITATION  RFQ  IFB  RFP

5. DELIVER TO U.S. Nuclear Regulatory Commission OIS/ICOD/DBB ATTN: Roy Choudhury Mail Stop, T-5-D-14 Washington DC 20555 CODE 16. ADMINISTERED BY U.S. Nuclear Regulatory Commission Div of Contracts Two White Flint North - MS T-7-I-2 Washington, DC 20555 CODE

7a. CONTRACTOR/OFFEROR CODE 781797712 FACILITY CODE EMERGENT, LLC 8133 LEESBURG PIKE STE 400 VIENNA VA 221822622 TELEPHONE NO. (301) 466-1900 18a. PAYMENT WILL BE MADE BY Department of Interior/NBC NRCPayments@nbc.gov ATTN: Fiscal Services Branch - D2770 7301 W. Mansfield Avenue Denver, CO 80235-2230 CODE

17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED  SEE ADDENDUM

| 19. ITEM NO. | 20. See CONTINUATION Page SCHEDULE OF SUPPLIES/SERVICES   | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|--------------|---|--------------|----------|----------------|------------|
|              | <p>The Contractor shall provide the U.S. Nuclear Regulatory Commission with Managed Public Key Infrastructure support services in accordance with GSA Schedule Contract No. GS-35F-0153M, the GSA contracts of teaming contractors XTech, Inc. (GS-35F-0165S) and (DLT Solutions (GS-35F-4543G) as referenced by letter from Emergent LLC, dated 05/13/2008 which is hereby incorporated by reference and made a part of the order, and the attached statement of work.</p> <p>This order shall be effective June 23, 2008, through June 22, 2009 for the total estimated amount (ceiling) of \$1,838,947.00. There are four one-year option periods as follows: Option Year 1 \$5,204,168.75; Option Year 2 \$4,236,372.57; Option Year 3 \$3,862,090.44; and Option Year 4 \$5,271,987.19. The total estimated amount (ceiling) of this order including option periods is \$20,443,565.95.</p> <p>Individual task orders will be issued under this order. Funding will be obligated under the individual task orders. (See Section B.2, Consideration and Obligation-Task Orders)</p> <p>(Use Reverse and/or Attach Additional Sheets as Necessary)</p> |              |          |                |            |

5. ACCOUNTING AND APPROPRIATION DATA 26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$1,838,947.00

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

28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 2 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED 29. AWARD OF CONTRACT: REF. OFFER DATED YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR 31a. UNITED STATES OF AMERICA SIGNATURE OF CONTRACTING OFFICER Michael A. Turner 30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT) Greg Christensen, President 30c. DATE SIGNED 6-23-08 31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) Michael A. Turner, Contracting Officer 31c. DATE SIGNED 6/23/08

AUTHORIZED FOR LOCAL REPRODUCTION PREVIOUS EDITION IS NOT USABLE STANDARD FORM 1449 (REV. 8/2005) Prescribed by GSA - FAR (48 CFR) 53.212

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

NOV 03 2008

ADM002

**Table of Contents**

**SECTION A.....A-1**

- A.1 SF 1449 SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS .....A-1
- A.2 COMPLIANCE WITH THE US IMMIGRATION LAWS AND REGULATIONS .....A-1
- A.3 SEAT BELTS .....A-1
- A.4 WHISTLERBLOWER PROTECTION FOR NRC CONTRACTOR AND  
SUBCONTRACTOR EMPLOYEES (JULY 2006) .....A-1
- A.5 OPTION PERIODS – TASK ORDER/DELIVERY ORDER UNDER A GSA FEDERAL  
SUPPLY SCHEDULE CONTRACT (MARCH 2007) .....A-1

**SECTION B - CONTINUATION BLOCK .....B-1**

- B.1 SUPPLIES OR SERVICES AND PRICES/COSTS .....B-1
- B.2 CONSIDERATION AND OBLIGATION – TASK ORDERS .....B-1
- B.3 STATEMENT OF WORK .....B-1

**SECTION C - CONTRACT CLAUSES .....C.1**

- C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998).....C-1
- C.2 52.224-70 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR.....C-1
- C.3 52.217-19 OPTION TO EXTEND THE TERM OF THE CONTRACT.....C-1
- C.4 52.216-18 ORDERING .....C-1
- C.5 52.216-19 ORDER LIMITATIONS (OCT 1995) .....C-1
- C.6 52.216-22 INDEFINITE QUANTITY (OCT 1995) .....C-1
- C.7 52.204-6 DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER .....C.1
- C.8 52.204-7 CENTRAL CONTRACTOR REGISTRATION (JULY 2006) .....C-1

**SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS.....D-1**

## **SECTION A - CONTINUATION**

### **A.2 COMPLIANCE WITH US. IMMIGRATION LAWS AND REGULATIONS**

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States Immigration and Naturalization (INS) laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Alien Registration Receipt Card Form 1-151 or must present other evidence from the Immigration and Naturalization Services that employment will not affect his/her immigration status. The INS Office of Business Liaison (OBL) provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on the INS website, <http://www.ins.usdoj.gov/graphics/services/employerinfo/index.htm#obl>.

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

### **A.3 SEAT BELTS**

Contractors, subcontractors, and grantees, are encouraged to adopt and enforce on-the-job seat belt policies and programs for their employees when operating company-owned, rented, or personally owned vehicles.

### **A.4 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (JULY 2006)**

- a. The U.S. Nuclear Regulatory Commission (NRC) contractor and its subcontractor are subject to the Whistleblower Employee Protection public law provisions as codified at 42 U.S.C. 5851. NRC contractor(s) and subcontractor(s) shall comply with the requirements of this Whistleblower Employee Protection law, and the implementing regulations of the NRC and the Department of Labor (DOL). See, for example, DOL Procedures on Handling Complaints at 29 C.F.R. Part 24 concerning the employer obligations, prohibited acts, DOL procedures and the requirement for prominent posting of notice of Employee Rights at Appendix A to Part 24.
- b. Under this Whistleblower Employee Protection law, as implemented by regulations, NRC contractor and subcontractor employees are protected from discharge, reprisal, threats, intimidation, coercion, blacklisting or other employment discrimination practices with respect to compensation, terms, conditions or privileges of their employment because the contractor or subcontractor employee(s) has provided notice to the employer, refused to engage in unlawful practices, assisted in proceedings or testified on activities concerning alleged violations of the Atomic Energy Act of 1954 (as amended) and the Energy Reorganization Act of 1974 (as amended).
- c. The contractor shall insert this or the substance of this clause in any subcontracts involving work performed under this contract.

### **A.5 OPTION PERIODS - TASK ORDER/DELIVERY ORDER UNDER A GSA FEDERAL SUPPLY SCHEDULE CONTRACT (MARCH 2007)**

- a. The Period of Performance (POP) for this requirement may extend beyond the Offeror's current POP on their GSA Schedule. Offerors may submit proposals for the entire POP as long as their current GSA Schedule covers the requested POP, or their GSA Schedule contains GSA's "Evergreen Clause" (Option to Extend the Term of the Contract), which covers the requested PoP if/when the option(s) are exercised. Offerors are encouraged to submit accurate/realistic pricing for the requirement's entire POP, even if the proposed GSA Schedule does not include pricing for the applicable option years, etc.

b. For proposal evaluation purposes, the NRC assumes that applicable Evergreen Clause Option(s) will be exercised and the NRC will apply price analysis, as applicable. It is in the best interest of the Offeror to explain major deviations in escalation, proposed in any Evergreen Clause option years. Resulting GSA task/delivery order option years subject to the Evergreen Clause will be initially priced utilizing the same rates proposed under the last GSA-priced year of the subject GSA Schedule. Upon GSA's exercise of the GSA Schedule option year(s) applicable to the Evergreen Clause, the NRC will modify the awarded task/delivery order to incorporate either the proposed pricing for the option years or the GSA-approved pricing (whichever is lower).

c. It is incumbent upon the Offeror to provide sufficient documentation (GSA-signed schedule, schedule modifications, etc.) that shows both the effective dates, pricing and terms/conditions of the current GSA Schedule, as well as Evergreen Clause terms/conditions (as applicable). Failure to provide this documentation may result in the Offeror's proposal being found unacceptable.

# SECTION B - CONTINUATION BLOCK

## B.1 SUPPLIES OR SERVICES AND PRICES/COSTS

Base Year - (June 23, 2008 – June 22, 2009)

| MPKI CERTIFICATES, HARDWARE, SOFTWARE                                |  |           |            |            |                       |
|--|--|-----------|------------|------------|-----------------------|
| CLIN   | DESCRIPTION  | EST. QTY. | UNIT       | UNIT PRICE | EST. AMOUNT           |
| 001  | Onsite Full <u>Public</u> Managed PKI 1000 User Pack<br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 8,000 ea.)<br><br>Digital Certificates SSP Software (est. 3,000 ea.)  |           | Ea.        |            | \$ 242,000.00         |
| 002  | Onsite Full <u>Public</u> Managed PKI 1000 User Pack - (Additional Per User)<br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est.100 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 650 ea.)<br><br>Digital Certificates FBCA<br>Rudimentary (Level 1) (est. 200 ea.) |           | Ea.        | \$         | \$ 20,900.00          |
| 003  | Onsite Full <u>Private</u> Managed PKI 1000 User Pack<br>Authentication Service Bureau (est. 9,000 ea.)<br>(Identity Verification)   |           | Ea.        |            | \$ 317,520.00         |
| 004  | Onsite Full <u>Private</u> Managed PKI 1000 User Pack – (Additional Per User)<br>Authentication Service Bureau<br>(Identity Verification) (est. 550 ea.)   |           | Ea.        | \$         | \$ 14,135.00          |
| 005  | Oberthur PIV End Point Dual Interface Smart Card<br>Smart Card (PIV-2 Compliant)<br>(Units of 1000 priced @ \$6.69 ea.)  |           | Ea.        | \$         | \$ 82,620.00          |
| 006  | SCR331 Smart Card Reader<br>Smart Card Reader (USB plug-in)<br>(Units of 1000 priced @ \$21.45 ea.)  |           | Ea.        | \$         | \$ 202,014.00         |
| 007  | ShipExtra<br>Card and Reader Distribution to Users<br>(Units of 1000 priced @ \$12.42 ea.)   |           | Ea.        | \$         | \$ 198,288.00         |
| 008  | VeriSign Card Mgt. System for PIV-CMS 1000 User Pack<br>Certificate Management System License Fee (CMS)  |           | Ea.        |            | \$ 525,000.00         |
| 009  | TRAVEL – Estimated-Not-To-Exceed (Cost – Reimbursement)  |           | Lot        | N/A        | \$ 30,000.00          |
| <b>Subtotal</b>  |  |           |            |            | <b>\$1,632,477.00</b> |
| MPKI SUPPORT SERVICES  |  |           |            |            |                       |
| CLIN   | LABOR CATEGORY   | EST. HRS. | LABOR RATE |            | EST. AMOUNT           |
| 010  | Sr. Engineer   |           |            |            | \$ 5,775.00           |
|  | Principle Engineer   |           |            |            | \$ 67,375.00          |
|  | Sr. Principal*   |           |            |            | \$ 133,320.00         |
| <b>Subtotal</b> *Includes estimated 300 hours for Project Management |  |           |            |            | <b>\$ 206,470.00</b>  |
| <b>TOTAL ESTIMATED AMOUNT - BASE YEAR</b>                            |  |           |            |            | <b>\$1,838,947.00</b> |

**B.1 SUPPLIES OR SERVICES AND PRICES/COSTS - CONTINUED**

**Option Year 1 - (June 23, 2009 – June 22, 2010)**

| MPKI CERTIFICATES, HARDWARE, SOFTWARE                                |   |           |            |            |                       |
|--|---|-----------|------------|------------|-----------------------|
| CLIN   | DESCRIPTION   | EST. QTY. | UNIT       | UNIT PRICE | EST. AMOUNT           |
| 011  | Onsite Full <u>Public</u> Managed PKI 1000 User Pack<br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 33,000 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 1,000 ea.)<br><br>Digital Certificates SSP Software (est. 5,000 ea.)   |           | Ea.        |            | \$ 858,000.00         |
| 012  | Onsite Full <u>Public</u> Managed PKI 1000 User Pack - (Additional Per User)<br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 710 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 800 ea.)<br><br>Digital Certificates FBCA<br>Rudimentary (Level 1) (est. 400 ea.)<br><br>Digital Certificates SSP Software (est. 500 ea.) |           | Ea.        | \$         | \$ 53,020.00          |
| 013  | Onsite Full <u>Private</u> Managed PKI 1000 User Pack<br>Authentication Service Bureau<br>(Identity Verification)   |           | Ea.        |            | \$1,040,000.00        |
| 014  | Onsite Full <u>Private</u> Managed PKI 1000 User Pack – (Additional Per User )<br>Authentication Service Bureau<br>(Identity Verification)  |           | Ea.        | \$         | \$ 21,202.50          |
| 015  | Oberthur PIV End Point Dual Interface Smart Card<br>Smart Card (PIV-2 Compliant)<br>(Units of 1000 priced @ \$7.56 ea.)   |           | Ea.        | \$         | \$ 261,222.00         |
| 016  | SCR331 Smart Card Reader<br>Smart Card Reader (USB plug-in)<br>(Units of 1000 priced @ \$22.50 ea.)   |           | Ea.        | \$         | \$ 638,713.40         |
| 017  | ShipExtra<br>Card and Reader Distribution to Users<br>(Units of 1000 priced @ \$14.15 ea.)  |           | Ea.        | \$         | \$ 626,932.80         |
| 018  | VeriSign Card Mgt. System for PIV-CMS 1000 User Pack<br>Certificate Management System License Fee (CMS)   |           | Ea.        |            | \$1,200,000.00        |
| 019  | TRAVEL - Estimated-Not-To-Exceed (Cost - Reimbursement)   |           | Lot        | N/A        | \$ 30,000.00          |
| <b>Subtotal</b>  |   |           |            |            | <b>\$4,729,090.70</b> |
| MPKI SUPPORT SERVICES  |   |           |            |            |                       |
| CLIN   | LABOR CATEGORY  | EST. HRS. | LABOR RATE |            | EST. AMOUNT           |
| 020  | Sr. Engineer  |           |            |            | \$ 13,384.13          |
|  | Principle Engineer  |           |            |            | \$ 178,352.86         |
|  | Sr. Principal*  |           |            |            | \$ 283,341.06         |
| <b>Subtotal</b> *Includes estimated 563 hours for Project Management |   |           |            |            | <b>\$ 475,078.05</b>  |
| <b>TOTAL ESTIMATED AMOUNT - OPTION YEAR 1</b>                        |   |           |            |            | <b>\$5,204,168.75</b> |

**B.1 SUPPLIES OR SERVICES AND PRICES/COSTS - CONTINUED**

**Option Year 2 - (June 23, 2010 – June 22, 2011)**

| <b>MPKI CERTIFICATES, HARDWARE, SOFTWARE</b>         |  |                  |                   |                   |                       |
|--|--|------------------|-------------------|-------------------|-----------------------|
| <b>CLIN</b>  | <b>DESCRIPTION</b>   | <b>EST. QTY.</b> | <b>UNIT</b>       | <b>UNIT PRICE</b> | <b>EST. AMOUNT</b>    |
| 021  | <b>Onsite Full Public Managed PKI 1000 User Pack</b><br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 48,000 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 2,000 ea.)<br><br>Digital Certificates SSP Software (est. 6,000 ea.)                                  |                  | Ea.               |                   | \$1,260,000.00        |
| 022  | <b>Onsite Full Public Managed PKI 1000 User Pack - (Additional Per User)</b><br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 710 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 50 ea.)<br><br>Digital Certificates FBCA<br>Rudimentary (Level 1) (est. 600 ea.) |                  | Ea.               | \$                | \$ 30,600.00          |
| 023  | <b>Onsite Full Private Managed PKI 1000 User Pack</b><br>Authentication Service Bureau<br>(Identity Verification)  |                  | Ea.               |                   | \$ 576,000.00         |
| 024  | <b>Onsite Full Private Managed PKI 1000 User Pack - (Additional Per User)</b><br>Authentication Service Bureau<br>(Identity Verification)  |                  | Ea.               | \$                | \$ 20,585.70          |
| 025  | <b>Oberthur PIV End Point Dual Interface Smart Card</b><br>Smart Card (PIV-2 Compliant)<br>(Units of 1000 priced @ \$7.94 ea.)   |                  | Ea.               | \$                | \$ 187,384.20         |
| 026  | <b>SCR331 Smart Card Reader</b><br>Smart Card Reader (USB plug-in)<br>(Units of 1000 priced @ \$24.00 ea.)   |                  | Ea.               | \$                | \$ 458,172.74         |
| 027  | <b>ShipExtra</b><br>Card and Reader Distribution to Users<br>(Units of 1000 priced @ \$15.00 ea.)  |                  | Ea.               | \$                | \$ 449,722.08         |
| 028  | <b>VeriSign Card Mgt. System for PIV-CMS 1000 User Pack</b><br>Certificate Management System License<br>Fee (CMS)  |                  | Ea.               |                   | \$ 637,500.00         |
| 029  | <b>TRAVEL - Estimated-Not-To-Exceed (Cost - Reimbursement)</b>   |                  | Lot               | N/A               | \$ 30,000.00          |
| <b>Subtotal</b>                                      |  |                  |                   |                   | <b>\$3,649,964.72</b> |
| <b>MPKI SUPPORT SERVICES</b>                         |  |                  |                   |                   |                       |
| <b>CLIN</b>  | <b>LABOR CATEGORY</b>  | <b>EST. HRS.</b> | <b>LABOR RATE</b> |                   | <b>EST. AMOUNT</b>    |
| 030  | Sr. Engineer   |                  |                   |                   | \$ 16,419.02          |
|  | Principle Engineer   |                  |                   |                   | \$ 218,515.40         |
|  | Sr. Principal*   |                  |                   |                   | \$ 351,473.43         |
| <b>Subtotal</b>                                      |  |                  |                   |                   | <b>\$ 586,407.85</b>  |
| *Includes estimated 602 hours for Project Management |  |                  |                   |                   |                       |
| <b>TOTAL ESTIMATED AMOUNT - OPTION YEAR 2</b>        |  |                  |                   |                   | <b>\$4,236,372.57</b> |

**B.1 SUPPLIES OR SERVICES AND PRICES/COSTS - CONTINUED**

**Option Year 3 - (June 23, 2011 – June 22, 2012)**

| <b>MPKI CERTIFICATES, HARDWARE, SOFTWARE</b>                         |  |                  |                   |                   |                       |
|--|--|------------------|-------------------|-------------------|-----------------------|
| <b>CLIN</b>  | <b>DESCRIPTION</b>   | <b>EST. QTY.</b> | <b>UNIT</b>       | <b>UNIT PRICE</b> | <b>EST. AMOUNT</b>    |
| 031  | <b>Onsite Full <u>Public</u> Managed PKI 1000 User Pack</b><br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 56,000 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 2,000 ea.)<br><br>Digital Certificates <b>SSP Software</b> (est. 6,000 ea.)  |                  | Ea.               |                   | \$1,739,000.00        |
| 032  | <b>Onsite Full <u>Public</u> Managed PKI 1000 User Pack - (Additional Per User)</b><br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 17 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 358 ea.)<br><br>Digital Certificates FBCA<br>Rudimentary (Level 1) (est. 800 ea.)<br><br>Digital Certificates <b>SSP Software</b> (est. 500 ea.) |                  | Ea.               | \$                | \$ 38,525.00          |
| 033  | <b>Onsite Full <u>Private</u> Managed PKI 1000 User Pack</b><br>Authentication Service Bureau<br>(Identity Verification)   |                  | Ea.               |                   | \$ 384,000.00         |
| 034  | <b>Onsite Full <u>Private</u> Managed PKI 1000 User Pack – (Additional Per User )</b><br>Authentication Service Bureau<br>(Identity Verification)  |                  | Ea.               | \$                | \$ 17,733.00          |
| 035  | <b>Oberthur PIV End Point Dual Interface Smart Card</b><br>Smart Card (PIV-2 Compliant)<br>(Units of 1000 priced @ <b>\$8.33</b> ea.)  |                  | Ea.               | \$                | \$ 124,215.60         |
| 036  | <b>SCR331 Smart Card Reader</b><br>Smart Card Reader (USB plug-in)<br>(Units of 1000 priced @ <b>\$24.75</b> ea.)  |                  | Ea.               | \$                | \$ 303,719.32         |
| 037  | <b>ShipExtra</b><br>Card and Reader Distribution to Users<br>(Units of 1000 priced @ <b>\$15.89</b> ea.)   |                  | Ea.               | \$                | \$ 298,117.44         |
| 038  | <b>VeriSign Card Mgt. System for PIV-CMS 1000 User Pack</b><br>Certificate Management System License<br>Fee (CMS)  |                  | Ea.               |                   | \$ 500,000.00         |
| 039  | <b>TRAVEL – Estimated-Not-To-Exceed (Cost – Reimbursement)</b>   |                  | Lot               | N/A               | \$ 30,000.00          |
| <b>Subtotal</b>  |  |                  |                   |                   | <b>\$3,168,310.36</b> |
| <b>MPKI SUPPORT SERVICES</b>   |  |                  |                   |                   |                       |
| <b>CLIN</b>  | <b>LABOR CATEGORY</b>  | <b>EST. HRS.</b> | <b>LABOR RATE</b> |                   | <b>EST. AMOUNT</b>    |
| 040  | Sr. Engineer   |                  |                   |                   | \$ 19,878.08          |
|  | Principle Engineer   |                  |                   |                   | \$ 265,041.00         |
|  | Sr. Principal*   |                  |                   |                   | \$ 438,861.00         |
| <b>Subtotal</b> *Includes estimated 630 hours for Project Management |  |                  |                   |                   | <b>\$ 753,780.08</b>  |
| <b>TOTAL ESTIMATED AMOUNT - OPTION YEAR 3</b>                        |  |                  |                   |                   | <b>\$3,862,090.44</b> |



**B.1 SUPPLIES OR SERVICES AND PRICES/COSTS - CONTINUED**

**Option Year 4 - (June 23, 2012 – June 22, 2013)**

| <b>MPKI CERTIFICATES, HARDWARE, SOFTWARE</b>                         |   |                  |                   |                    |                       |
|--|---|------------------|-------------------|--------------------|-----------------------|
| <b>CLIN</b>  | <b>DESCRIPTION</b>  | <b>EST. QTY.</b> | <b>UNIT</b>       | <b>UNIT PRICE</b>  | <b>EST. AMOUNT</b>    |
| 041  | <b>Onsite Full <u>Public</u> Managed PKI 1000 User Pack</b><br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 64,000 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 2,000 ea.)<br><br>Digital Certificates FBCA<br>Rudimentary (Level 1) (est. 1,000 ea.)<br><br>Digital Certificates SSP Software (est. 7,000 ea.) |                  | Ea.               |                    | \$1,574,500.00        |
| 042  | <b>Onsite Full <u>Public</u> Managed PKI 1000 User Pack - (Additional Per User)</b><br>Digital Certificates FBCA<br>Medium Hardware (Level 4) (est. 1419 ea.)<br><br>Digital Certificates FBCA<br>Medium Software (Level 3) (est. 711 ea.)  |                  | Ea.               |                    | \$ 26,555.00          |
| 043  | <b>Onsite Full <u>Private</u> Managed PKI 1000 User Pack</b><br>Authentication Service Bureau<br>(Identity Verification)  |                  | Ea.               |                    | \$704,000.00          |
| 044  | <b>Onsite Full <u>Private</u> Managed PKI 1000 User Pack - (Additional Per User)</b><br>Authentication Service Bureau<br>(Identity Verification)  |                  | Ea.               |                    | \$ 17,835.80          |
| 045  | <b>Oberthur PIV End Point Dual Interface Smart Card</b><br>Smart Card (PIV-2 Compliant)<br>(Units of 1000 priced @ \$8.74 ea.)  |                  | Ea.               |                    | \$ 225,460.80         |
| 046  | <b>SCR331 Smart Card Reader</b><br>Smart Card Reader (USB plug-in)<br>(Units of 1000 priced @ \$24.75 ea.)  |                  | Ea.               |                    | \$ 551,273.76         |
| 047  | <b>ShipExtra</b><br>Card and Reader Distribution to Users<br>(Units of 1000 priced @ \$16.85 ea.)   |                  | Ea.               |                    | \$ 541,105.92         |
| 048  | <b>VeriSign Card Mgt. System for PIV-CMS 1000 User Pack</b><br>Certificate Management System License<br>Fee (CMS)   |                  | Ea.               |                    | \$ 550,000.00         |
| 049  | <b>TRAVEL – Estimated-Not-To-Exceed (Cost – Reimbursement)</b>  |                  | Lot               | N/A                | \$ 30,000.00          |
| <b>Subtotal</b>  |   |                  |                   |                    | <b>\$4,385,231.28</b> |
| <b>MPKI SUPPORT SERVICES</b>   |   |                  |                   |                    |                       |
| <b>CLIN</b>  | <b>LABOR CATEGORY</b>   | <b>EST. HRS.</b> | <b>LABOR RATE</b> | <b>EST. AMOUNT</b> |                       |
| 050  | Sr. Engineer  |                  |                   | \$ 23,400.00       |                       |
|  | Principle Engineer  |                  |                   | \$ 310,907.10      |                       |
|  | Sr. Principal*  |                  |                   | \$ 552,448.81      |                       |
| <b>Subtotal</b> *Includes estimated 300 hours for project Management |   |                  |                   |                    | <b>\$ 886,755.91</b>  |
| <b>TOTAL ESTIMATED AMOUNT - BASE YEAR</b>                            |   |                  |                   |                    | <b>\$5,271,987.19</b> |

**TOTAL ESTIMATED AMOUNT - BASE YEAR & OPTION YEARS 1- 4: \$20,443,565.95**

## **B.2 CONSIDERATION AND OBLIGATION- TASK ORDERS (AUG 1989)**

- a. The total estimated amount of this delivery order (ceiling) for the products/services ordered, delivered, and accepted under this order is **\$1,838,947.00**. The Contracting Officer may unilaterally increase this amount as necessary for orders to be placed with the contractor during the contract period provided such orders are within any maximum ordering limitation prescribed under this purchase order.
- b. The Contracting Officer will obligate funds on each task order issued.
- c. A total estimated cost as well as any fee, if any, will be negotiated for each task order and will be incorporated as a ceiling in the resultant task order. The Contractor shall comply with the provisions of 52.232-20 - Limitation of Cost for fully funded task orders and 52.232-22 - Limitation of Funds for incrementally funded task orders, issued hereunder.

## **B.3 STATEMENT OF WORK**

### **B.3.1 Background**

- a. The U.S. Nuclear Regulatory Commission (NRC) has operated a Managed PKI service from VeriSign, Inc. since 1999. This service includes backend Certification Authority (CA) systems and services operated by VeriSign in Mountain View, California and backup sites. It also includes registration, certificate management, and key escrow software provided by VeriSign, but operated by the NRC on government furnished equipment located in a server vault in the NRC data center. The General Services Administration (GSA) has certified the Shared Service Provider (SSP) program for federal agencies. The NRC needs to expand its MPKI service to add new software for compliance with federal PKI policies, and new certificate classes for additional e-authentication assurance levels. The design and integration needed to prepare for the new certificates and services is being performed under the Phase 1 contract already in place. The following two paragraphs describe the work in progress under the Phase 1 contract.
- b. The NRC has an operational VeriSign MPKI 6.0 Certification Authority (CA) for internal staff certificate issuance. Documentation includes a custom Certificate Policy (CP) Addendum to the VeriSign Trust Network (VTN) CP and a custom Certification Practices Statement (CPS). The CA, policies, and procedures are compliant with Federal Bridge Certification Authority (FBCA) policy at the Medium assurance level. These policies are under review as part of Phase 1. NRC also has a legacy VeriSign MPKI CA with 500 subscribers that is approaching end-of-support for the product. Work is in progress to migrate some of these subscribers to a new VeriSign MPKI platform.
- c. The VeriSign MPKI for internal staff is in the process of converting to the VeriSign federally approved SSP product. Other work in progress includes implementing FBCA Medium assurance certificates for external partners. However, recent changes to NRC regulatory and security programs may require certificates for external partners at multiple assurance levels. For this reason, migration of the legacy MPKI may not be complete until additional certificate types are made available.
- d. The NRC Infrastructure Systems Support Contract (ISSC) system management contractor is the primary IT support contractor for the development and maintenance of the NRC IT infrastructure. The ISSC contractor is responsible for the daily operation and maintenance of the MPKI, its local server components, and the internal subscriber certificate life-cycle processes.

### **B.3.2 Purpose**

The NRC seeks VeriSign Inc. (VeriSign) software licenses and digital certificate user licenses to allow the NRC to issue certificates to the necessary stakeholders. For certificates that are required to be on a hardware

security token, purchase of a smart card and smart card reader is included. The NRC also requires an off-site identity proofing service to assist with issuing secure digital certificates and hardware tokens to users located throughout the United States. The NRC requires the contractor to assemble and process enrollment packages, and to reliably ship hardware tokens to approved users. This procurement represents Phase 2 of a two-phase plan. The Phase 1 contract enabled VeriSign to design and implement new infrastructure and processes to expand the MPKI service offerings to meet new NRC requirements. This Phase 2 procurement provides the software licenses and the hardware tokens required for individual users of MPKI. The NRC also seeks professional services labor hours for future tasks as new agency requirements for MPKI are identified and defined.

### **B.3.3 Work Requirements**

- a. The contractor shall provide an off-site hardware distribution service to ship smart cards and readers to properly vetted and approved applicants in the U.S. upon instructions from the NRC. The distribution service shall provide first class postage or equivalent for all recipients in the U.S. Each smart card and reader should be shipped to its respective user within 2 business days of the user receiving final approval for smart card issuance.
- b. For Authentication Service Bureau, the contractor shall provide an off-site service to print enrollment forms (two to four 8½ x 11 sheets), provide postage-paid return envelopes addressed to the Authentication Service Bureau described below, assemble enrollment packages, and mail them to approved applicants in the U.S. upon instructions from the NRC. The distribution service shall provide first class postage or equivalent for all recipients in the U.S. Each enrollment packet should be shipped to its respective user within 2 business days of the user receiving approval for enrollment.

#### **B.3.3.1 Detailed Description of Fixed Price Priced Items for MPKI**

The contractor shall provide digital certificate user licenses, software licenses, hardware and support services identified below as needed via the issuance of task orders.

**B.3.3.1a Digital Certificates FBCA Medium Hardware (level 4), “Digital Certificates FBCA Medium Software (level 3),” and “Digital Certificates FBCA Rudimentary (level 1).”** The contractor shall provide digital certificates at the indicated assurance level from an issuing authority that is cross-certified with the Federal Bridge Certification Authority (FBCA).

**B.3.3.1b Digital Certificates SSP Software (NRC Staff).** The contractor shall provide digital certificates from an issuing authority that falls under the Federal Government Root Authority and is compliant with the Federal PKI Common Policy Framework and the federal Shared Service Provider (SSP) program.

**B.3.3.1c Smart Card (PIV-2 compliant).** The contractor shall supply smart cards that are certified as meeting Federal Information Processing Standard (FIPS) 201-1 and related guidance from the National Institute of Standards and Technology (NIST). The smart cards shall be delivered to the NRC and to the smart card distribution service according to the allocation of users. The smart cards shall be delivered in a manner to ensure timely enrollment of identified users.

**B.3.3.1d Smart Card Reader (USB plug-in).** The contractor shall supply a portable smart card reader with Universal Serial Bus (USB) personal computer connector that is capable of reading the wired contact interfaces of the supplied smart card and requires minimal or no installation of software on the user's personal computer. The smart card readers shall be delivered together with the smart cards in the same quantities.

**B.3.3.1e Authentication Service Bureau.** The contractor shall provide an off-site identity validation service to verify digital certificate applicant paperwork signed by notaries public against state motor vehicle records and NRC-defined agency and licensee telephone contact information. The vendor shall manage the flow of applications, notarized paperwork, and identity validation services to enable the successful enrollment of the

end-users. The NRC will provide an initial communication to users directing them to the enrollment web site. This may be a single mass communication.

**B.3.3.1f Certificate Management System license fee (CMS).** The contractor shall provide integrated MPKI system software (Certificate Management System) to manage the required issuer and approver roles, and audit information. The contractor shall ensure that the component is compliant with Federal PKI Policy, FIPS 201, and other appropriate federal government standards and definitions of a Card Management System (CMS), including Federal Information Security Management Act (FISMA) requirements for privacy and security.

The contractor shall provide maintenance, patches, and upgrades needed to keep the digital certificates and software in compliance with federal PKI policies and FISMA security standards. In addition the vendor may be required to assist with certification & accreditation (C & A) efforts for the NRC MPKI systems.

### **B.3.3.2 Support Services for MPKI**

In addition, the contractor may be asked to perform tasks to expand, enhance, and compliment the MPKI program to help meet emerging and changing federal PKI standards, policies, and guidelines, and new NRC requirements, as directed by the NRC. The following is a high-level list of the types of tasks that the contractor may be called upon to execute. This list is only for use in developing a staffing plan. The NRC will not be obligated to order any particular task(s) on this list.

- a. Design solutions to provide digital certificates for other applications;
- b. Implement an external partner digital certificate cryptographic token life cycle at the FBCA High assurance level;
- c. Migrate existing MPKI certificate systems to new automated workflow processes and systems;
- d. Integrate the NRC Internal Staff MPKI certificate system with GSA Managed Service Office services;
- e. Provide backup support at Federal PKI Policy Authority Certificate Policy Working Group meetings as needed to ensure NRC representation;
- f. Develop practices and procedures for collecting and maintaining PKI transaction records for applications that rely on PKI to comply with NRC and National Archives and Records Administration (NARA) records management requirements;
- g. Assist NRC system owners to convert their applications from user ID and password to digital certificate authentication;
- h. Provide training to system owners and administrators on MPKI operations, including but not limited to application authentication integration, real-time certificate validation, and identity management integration;
- i. Migrate the MPKI Internal Staff Digital Certificates to SSP; and
- j. Implement Digital Certificates at FBCA Medium Hardware.

### **B.3.4 Contractor Qualifications**

- a. The Contractor shall provide qualified, competent, and fully trained personnel to perform the support activities delineated under this contract. The contractor shall provide staff with the appropriate skills who meet or exceed the qualifications described below:
- b. Subject matter expert in federal PKI policy, practice, and procedures. Experienced with developing certificate policy, certification practice statement, registration practice statement, cross-certification application and matrix, subscriber agreement, technical reference manual, and PKI procedure documents. Requires excellent writing, documentation, and oral presentation skills.
- c. Technical Expertise in MPKI hardware, software, design, solution development, installation, configuration, troubleshooting, maintenance, capacity planning, disaster recovery planning, and training. Experienced with developing federally-compliant subscriber registration systems and training materials for registration agents. Requires excellent system administration, troubleshooting, interpersonal communication, and teaching skills.

d. Knowledge and experience in information security and MPKI technology. Able to create and recommend remediation for components of security policies. Provides specific recommendations for a clients business or technical issues. Deeper technical problem/resolution skills; mid-level infrastructure or security design capabilities; mid-level systems administration; knowledge of web application architectures and products; basic experience with scripting or coding. Mid-level security knowledge should include: PKI systems and integration; Internet attack anatomy; perimeter protection strategies; security policy structure. Mid-level methods knowledge of systems integration and security architectures.

e. Possesses specific knowledge and experience in information security and PKI technology. Provides specific recommendations for client business or technical issues. Deep technical problem / resolution skills; Basic infrastructure or security design capabilities for environments that include up to 10 security devices, processes or applications; basic systems administration (UNIX, Windows, or mainframe); basic network administration (thorough protocol experience); basic security knowledge of Internet attack anatomy; perimeter protection strategies; security policy structure; PKI technologies; basic methods knowledge of system integration.

f. Business expert in project management with technical background in MPKI systems and services. Proficient with Microsoft Project software and familiar with enterprise project functionality and integrated project plans. Requires good oral and written communication skills. The ability to apply proven project management methodologies to task orders that include project management requirements. Project Management Institute (PMI) certification is preferred.

### **B.3.5 NRC Furnished Items**

The NRC will provide the contractor with state nuclear regulatory agency and licensee telephone contact information to be used by the vendor's Authentication Service Bureau to verify digital certificate applicant paperwork signed by notaries public.

### **B.3.6 Travel**

For estimating purposes, it is anticipated that a total of 4 trips per year will be required to NRC regional offices located in Philadelphia (PA), Atlanta (GA), Chicago (IL), and Dallas/Fort Worth (TX) to perform facilitation services. If travel is requested and approved by Government, the contractor would be reimbursed for reasonable expenses in accordance with Federal Travel Regulations.

### **B.3.7 Project Management**

Professional services may specify a project management requirement and staffing. The contractor shall apply proven project management methodologies to task orders that include project management requirements. The project manager shall also incorporate elements of the NRC Project Management Methodology into the project plan if required in the task order statement of work.

### **B.3.8 Deliverables**

Contract deliverables and delivery dates will be determined on a task order basis.

### **B.3.9 Acceptance Criteria**

Acceptance Criteria will be determined on a task order basis.

### **B.3.10 Quality Assurance**

a. The NRC is very concerned that the support supplied by the Contractor shall be of the highest possible quality. To ensure the highest possible quality, the Contractor shall address quality as an implied component of all tasks and services requested delivered throughout the life of the contract.

b. NRC's goal is to provide 100% customer satisfaction to its end-users, its licensees, and the general public accessing NRC systems. All Contractor activities shall be in compliance with the NRC's quality assurance goal of providing 100% customer satisfaction. The Contractor shall provide support that enables this level of quality to be attained by developing and maintaining service goals that include, at a minimum, customer satisfaction. Workmanship performance for all Contractor efforts shall comply with current government and industry standards.

c. The Contractor shall be responsible for the implementation of a quality assurance program through which all products and services must pass prior to delivery to the Government. The Contractor shall establish quality assurance methods and procedures which demonstrate a commitment to ensuring the ability to deliver to the Government the best quality products and services, and in developing improvements in performance, productivity and management of this contract.

### **B.3.11. Technical Progress Report (JAN 1993)**

For professional services task orders, the contractor shall provide a monthly Technical Progress Report to the project officer and the contracting officer. The report is due within 15 calendar days after the end of the report period and must identify the title of the project, the contract number, appropriate financial tracking code specified by the NRC Project Officer, project manager and/or principal investigator, the contract period of performance, and the period covered by the report. Each report must include the following for each discrete task/task order:

- a. A listing of the efforts completed during the period, and milestones reached or, if missed, an explanation provided;
- b. Any problems 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.
- c. A summary of progress to date; and
- d. Plans for the next reporting period.

### **B.3.12 Period of Performance**

The ordering period for this contract shall commence on June 23, 2008, and will expire one June 22, 2009. Any orders issued during this period shall be completed within the time specified in the order, unless otherwise specified herein. (See 52.216-18 - Ordering.) The term of this contract may be extended at the option of the Government for an additional 4 one-year periods.

### **B.3.13 Project Officer Authority**

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

Name: Roy Choudhury  
Address: U.S. Nuclear Regulatory Commission  
OIS/ICOD/DDB - Mail Stop: T-5D-14  
Washington, DC, 20555  
Telephone Number: (301) 415-7226

b. Performance of the work under this contract is subject to the technical direction of the NRC project officer. 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 project officer does not have the authority to and may not issue any technical direction which:

(1) Constitutes an assignment of work outside the general scope of the contract.

(2) Constitutes a change as defined in the "Changes" clause of this contract.

(3) In any way causes an increase or decrease in the total estimated contract cost, the fixed fee, if any, or the time required for contract performance.

(4) Changes any of the expressed terms, conditions, or specifications of the contract.

(5) Terminates the contract, settles any claim or dispute arising under the contract, or issues any unilateral directive whatever.

d. All technical directions must be issued in writing by the project officer or must be confirmed by the project officer in writing within ten (10) working days after verbal issuance. A copy of the written direction must be furnished to the contracting officer. A copy of NRC Form 445, Request for Approval of Official Foreign Travel, which has received final approval from the NRC must be furnished to the contracting officer.

e. The contractor shall proceed promptly with the performance of technical directions duly issued by the project officer in the manner prescribed by this clause and within the project officer's authority under the provisions of this clause.

f. If, in the opinion of the contractor, any instruction or direction issued by the project officer 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 project officer 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 project officer shall:

(1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.

- (2) Assist the contractor in the resolution of technical problems encountered during performance.
- (3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this contract.
- (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.

**B.3.14 2052.215-70 Key Personnel (JAN 1993)**

a. The following individuals are considered to be essential to the successful performance of the work hereunder:

Frazier D. Evans, Principal Engineer  
Shawn Wilson, Senior, Sr. Principal

The contractor agrees that personnel may not be removed from the contract work or replaced without compliance with paragraphs (b) and (c) of this section.

- b. If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.
- c. Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution. The contracting officer and the project officer shall evaluate the contractor's request and the contracting officer shall promptly notify the contractor of his or her decision in writing.
- d. If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the



contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage

### **B.3.15 Security Requirements**

Performance of duties under the professional services task ordering portion of this contract may require unescorted access to NRC computer and network systems and an NRC IT-1 security access approval. The corresponding task order statement of work will specify whether unescorted access or IT-1 security approval is needed for that task. The following security requirements must be adhered to during the life of the contract:

- a. Issuing of credentials must comply with NIST SP 800-53 for operational, management, and technical controls.
- b. All system modifications must comply with NRC security policies and procedures, as well as federal laws, guidance, and standards to ensure FISMA compliance.
- c. The contractor shall ensure that its employees, in performance of the contract, receive IT security training in their role (e.g. system administrators must received training in the IT security of the operating system being used).
- d. The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any protections either designed or developed by the contractor under this contract or otherwise provided by the government. The SSP and other information system security documentation for the contract are considered Sensitive Unclassified Information. The contractor agrees to abide by NRC regulations for handling sensitive unclassified information governed by the NRC's Sensitive Unclassified Non-Safeguards Information program (SUNSI), NRC's Management Directive (MD) 12.2, "NRC Classified Information Security Program" and NRC's MD 12.5, "NRC Automated Information Security Program."
- e. The contractors shall only use NRC provided e-mail accounts to send and receive information considered sensitive.
- f. Separation of duties for the systems must be enforced by the system through assigned access authorizations.
- g. The information system shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
- h. The most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.
- i. The contractor shall only use licensed software and in-house developed authorized code (including government and contractor developed) on the on the system and for processing government information. Public domain, shareware, or freeware shall only be installed after prior written approval is obtained from the NRC DAA. The contractor shall provide proof of licensing upon request of the contracting officer, the COTR, the SITSOs, or the DAAs.
- j. All development and testing of the systems shall be performed on a network separate and isolated from the NRC operational network that is protected at the prescribed sensitivity level.
- k. All system computers must be properly configured and hardened, and comply with all NRC security policies and procedures for the prescribed sensitivity of the system.
- l. An independent tester will be required to perform the security test, evaluation, and contingency testing on the system. The contractor shall support OIS in its efforts to certify and accredit the systems under FISMA by assisting with the completion of required security deliverables that include Memorandum of Understandings, Interconnection Security Agreements, Security Categorization, E-Authentication Risk Assessment, Security Risk Assessment, System Security Plan, Contingency Plan, Security Test and Evaluation Plan, Security Test and Evaluation Execution Report, Contingency Scenario Execution Report, Corrective Actions Plan and Certification Letter.
- m. The contractor shall support the NRC in its effort to conduct security tests and evaluation, and contingency tests as needed, to ensure system certification and for continuous monitoring activities. The contractor will provide assistance to the NRC and/or security contractor responsible for developing and performing the test.

- n. User accounts that have system-level or administrative privileges must have a unique password from all other accounts held by that user, and general user tasks must be performed from a general user account, not from the administrative account.
- o. The contractor shall not hardcode any passwords into the software unless the password only appears on the server side (e.g. using server-side technology such as ASP, PHP, or JSP).
- p. All sensitive data being transmitted over a network by the system shall use FIPS 140-2 validated encryption. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.
- q. All media produced must include appropriate markings to indicate the sensitivity of the information contained on the media and the media must be controlled according to that sensitivity.

### **B.3.16 2052.204.70 Security**

- 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 (Safeguards, Official Use Only, and Proprietary information), 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, proprietary data (trade secrets) or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, other (Official Use Only) 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 of 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.

### **B.3.17 Security Requirements for Information Technology Level I or Level II Access Approval (July 2007)**

The proposer/contractor must identify all individuals and propose the level of Information Technology (IT) approval for each, using the following guidance. The NRC sponsoring office shall make the final determination of the level, if any, of IT approval required for all individuals working under this contract. The Government shall have and exercise full and complete control and discretion over granting, denying, withholding, or terminating IT access approvals for individuals performing work under this contract.

The contractor shall conduct a preliminary security interview or review for each IT level I or II access approval contractor applicant and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of IT security access for which the candidate has been proposed. The contractor will pre-screen its applicants for the following:

- (a) felony arrest in the last seven years;
- (b) alcohol related arrest within the last five years;
- (c) record of any military courts-martial convictions in the past ten 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 years;
- (e) delinquency on any federal debts or bankruptcy in the last seven years.

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

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

### **SECURITY REQUIREMENTS FOR IT LEVEL I**

Performance under this contract will involve prime contractor personnel, subcontractors or others 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.

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by FSB/DFS. Temporary IT access may be approved based on a favorable review or adjudication of their security forms and checks. Final IT access may be approved based on a favorably review or adjudication. 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 requiring IT access without the approval of FSB/DFS. Where temporary access authorization has been revoked or denied, the contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. When an individual receives final IT access, the individual will be subject to a reinvestigation every ten years.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two copies of the contractor's signed pre-screening record and two FD-258 fingerprint charts, through the PO to FSB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible. Based on FSB/DFS review of the contractor applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) and SF-86 which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g., bidders) who 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 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.

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by FSB/DFS. Temporary access may be approved based on a favorable review of their security forms and checks. Final IT access may be approved based on a favorably adjudication. 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 requiring IT access without the approval of FSB/DFS. Where temporary access authorization has been revoked or denied, the contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. When an individual receives final IT access, the individual will be subject to a review or reinvestigation every ten years.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two copies of the contractor's signed pre-screening record and two FD-258 fingerprint charts, through the PO to FSB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible. Based on FSB/DFS review of the contractor applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments); SF-86, and contractor's record of the pre-screening which furnishes the basis for providing security requirements to prime contractors, subcontractors or others

(e.g. bidders) who 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 PO by telephone in order that he/she will immediately contact FSB/DFS so that the access review may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed by the contractor in writing to the PO who will forward the confirmation via email to FSB/DFS. Additionally, FSB/DFS must be immediately notified in writing when an individual no longer requires access to NRC sensitive automated information technology systems or data, including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for IT access.

#### **B.3.18 Badge Requirements for Unescorted Building Access to NRC Facilities**

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 Personnel Security Branch, Division of Facilities and Security (PSB/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 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](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 PSB/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."

#### **B.3.19 Appropriate Use of Government Furnished Information Technology (IT) Equipment and/or IT Services/Access (MARCH 2002)**

As part of contract performance the NRC may provide the contractor with information technology (IT) equipment and IT services or IT access as identified in the solicitation or subsequently as identified in the contract or delivery order. Government furnished IT equipment, or IT services, or IT access may include but is not limited to computers, copiers, facsimile machines, printers, pagers, software, phones, Internet access and use, and email access and use. The contractor (including the contractor's employees, consultants and subcontractors) shall use the government furnished IT equipment, and / or IT provided services, and/ or IT access solely to perform the necessary efforts required under the contract. The contractor (including the contractor's employees, consultants and subcontractors) are prohibited from engaging or using the government IT equipment and government provided IT services or IT access for any personal use, misuse, abuses or any other unauthorized usage. The contractor is responsible for monitoring its employees, consultants and subcontractors to ensure that government furnished IT equipment and/ or IT services, and/ or IT access are not being used for personal use, misused or abused. The government reserves the right to withdraw or suspend the use of its government furnished IT equipment, IT services and/ or IT access arising from contractor personal usage, or misuse or abuse; and/ or to disallow any payments associated with contractor (including the contractor's employees, consultants and subcontractors) personal usage, misuses or

abuses of IT equipment, IT services and/ or IT access; and/ or to terminate for cause the contract or delivery order arising from violation of this provision.

### **B.3.20 2052.216-72 Task Order Procedures (OCT 1999)**

a. Task order request for proposal. When a requirement within the scope of work for this contract is identified, the contracting officer shall transmit to the contractor a Task Order Request for Proposal (TORFP) which may include the following, as appropriate:

- (1) Scope of work/meetings/travel and deliverables;
- (2) Reporting requirements;
- (3) Period of performance - place of performance;
- (4) Applicable special provisions;
- (5) Technical skills required; and
- (6) Estimated level of effort.

b. Task order technical proposal. By the date specified in the TORFP, the contractor shall deliver to the contracting officer a written or verbal (as specified in the TORFP technical proposal submittal instructions) technical proposal that provides the technical information required by the TORFP.

c. Cost proposal. The contractor's cost proposal for each task order must be fully supported by cost and pricing data adequate to establish the reasonableness of the proposed amounts. When the contractor's estimated cost for the proposed task order exceeds \$100,000 and the period of performance exceeds six months, the contractor may be required to submit a Contractor Spending Plan (CSP) as part of its cost proposal. The TORP indicates if a CSP is required.

d. Task order award. The contractor shall perform all work described in definitized task orders issued by the contracting officer. Definitized task orders include the following:

- (1) Statement of work/meetings/travel and deliverables;
- (2) Reporting requirements;
- (3) Period of performance;
- (4) Key personnel;
- (5) Applicable special provisions; and
- (6) Total task order amount including any fixed fee.

### **B.3.21 Accelerated Task Order Procedures (JAN 1993)**

a. The NRC may require the contractor to begin work before receiving a definitized task order from the contracting officer. Accordingly, when the contracting officer verbally authorizes the work, the contractor shall proceed with performance of the task order subject to the monetary limitation established for the task order by the contracting officer.

b. When this accelerated procedure is employed by the NRC, the contractor agrees to begin promptly negotiating with the contracting officer the terms of the definitive task order and agrees to submit a cost proposal with supporting cost or pricing data. If agreement on a definitized task order is not reached by the target date mutually agreed upon by the contractor and contracting officer, the contracting officer may determine a reasonable price and/or fee in accordance with Subpart 15.8 and Part 31 of the FAR, subject to contractor appeal as provided in 52.233-1, Disputes. In any event, the contractor shall proceed with completion of the task order, subject only to the monetary limitation established by the contracting officer and the terms and conditions of the basic contract.

**B.3.22 2052.215-78 Travel Approvals and Reimbursement Alternate 1 (OCT 1999)**

a. Total expenditure for travel may not exceed \$30,000.00 without the prior approval of the contracting officer.

b. All foreign travel must be approved in advance by the NRC on NRC Form 445, Request for Approval of Official Foreign Travel, and must be in compliance with FAR 52.247-63 Preference for U.S. Flag Air Carriers. The contractor shall submit NRC Form 445 to the NRC no later than 30 days prior to the commencement of travel.

c. The contractor will be reimbursed only for those travel costs incurred that are directly related to this contract and which are allowable subject to the limitations prescribed in FAR 31.205-46.

d. It is the responsibility of the contractor to notify the contracting officer in accordance with the FAR Limitations of Cost clause of this contract when, at any time, the contractor learns that travel expenses will cause the contractor to exceed the travel ceiling amount identified in paragraph (a) of this clause.

e. Reasonable travel costs for research and related activities performed at State and nonprofit institutions, in accordance with Section 12 of Pub. L. 100-679, shall be charged in accordance with the contractor's institutional policy to the degree that the limitations of Office of Management and Budget (OMB) guidance are not exceeded. Applicable guidance documents include OMB Circular A-87, Cost Principles for State and Local Governments; OMB Circular A-122, Cost Principles for Nonprofit Organizations; and OMB Circular A-21, Cost Principles for Educational Institutions.



## SECTION C - CONTRACT CLAUSES

### C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

<http://www.arnet.gov/far>

|           |   |          |
|-----------|---|----------|
| 52.232-20 | LIMITATION OF COSTS   | APR 1984 |
| 52.232-22 | LIMITATION OF FUNDS   | APR 1984 |
| 52.232-7  | PAYMENTS UNDER TIME-AND MATERIALS<br>AND LABOR-HOUR CONTRACTS | FEB 2007 |

### C.2 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR

Funds are not presently available for performance under this contract beyond the expiration date. 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 the expiration date, 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 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT

- a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 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 5 years.

### C.4 52.216-18 ORDERING

- a. Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from the date of award through the expiration date.
- b. All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.
- c. If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

### **C.5 52.216-19 ORDER LIMITATIONS (OCT 1995)**

a. Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than \$156,900.00, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

b. Maximum order. The Contractor is not obligated to honor--

(1) Any order for a single item in excess of the estimated quantities of \$1,838,947.00;

(2) Any order for a combination of items in excess of the estimated quantities of \$1,838,947.00;

(3) A series of orders from the same ordering office within 2 days that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) above.

c. If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) above.

d. Notwithstanding paragraphs b and c above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 2 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

### **C.6 52.216-22 INDEFINITE QUANTITY (OCT 1995)**

a. This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

b. Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

c. Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

d. Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 6 months from the expiration date of this contract.

### **C.7 52.204-6 DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER**

a. The offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "DUNS" or "DUNS+4" followed by the DUNS number or "DUNS+4" that identifies the offeror's name and address exactly as stated in the offer. The DUNS number is a nine-digit number assigned by Dun and Bradstreet, Inc. The DUNS+4 is the DUNS number plus a 4-character suffix that may be assigned at the

discretion of the offeror to establish additional CCR records for identifying alternative Electronic Funds Transfer (EFT) accounts (see Subpart 32.11) for the same parent concern.

b. If the offeror does not have a DUNS number, it should contact Dun and Bradstreet directly to obtain one.

(1) An offeror may obtain a DUNS number--

(i) If located within the United States, by calling Dun and Bradstreet at 1-866-705-5711 or via the Internet at <http://www.dnb.com>; or

(ii) If located outside the United States, by contacting the local Dun and Bradstreet office.

(2) The offeror should be prepared to provide the following information:

(i) Company legal business name.

(ii) Tradestyle, doing business, or other name by which your entity is commonly recognized.

(iii) Company physical street address, city, state and Zip Code.

(iv) Company mailing address, city, state and Zip Code (if separate from physical).

(v) Company telephone number.

(vi) Date the company was started.

(vii) Number of employees at your location.

(viii) Chief executive officer/key manager.

(ix) Line of business (industry).

(x) Company Headquarters name and address (reporting relationship within your entity).

## **C.8. 52.204-7 CENTRAL CONTRACTOR REGISTRATION**

a. Definitions. As used in this clause--

Central Contractor Registration (CCR) database means the primary Government repository for Contractor information required for the conduct of business with the Government.

Data Universal Numbering System (DUNS) number means the 9-digit number assigned by Dun and Bradstreet, Inc. (D&B) to identify unique business entities.

Data Universal Numbering System +4 (DUNS+4) number means the DUNS number assigned by D&B plus a 4-character suffix that may be assigned by a business concern. (D&B has no affiliation with this 4-character suffix.) This 4-character suffix may be assigned at the discretion of the business concern to establish additional CCR records for identifying alternative Electronic Funds Transfer (EFT) accounts (see the FAR at Subpart 32.11) for the same parent concern.

Registered in the CCR database means that--

(1) The Contractor has entered all mandatory information, including the DUNS number or the DUNS+4 number, into the CCR database; and

(2) The Government has validated all mandatory data fields and has marked the record "Active".

b. (1) By submission of an offer, the offeror acknowledges the requirement that a prospective awardee shall be registered in the CCR database prior to award, during performance, and through final payment of any contract, basic agreement, basic ordering agreement, or blanket purchasing agreement resulting from this solicitation.

(2) The offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "DUNS" or "DUNS +4" followed by the DUNS or DUNS +4 number that identifies the offeror's name and address exactly as stated in the offer. The DUNS number will be used by the Contracting Officer to verify that the offeror is registered in the CCR database.

c. If the offeror does not have a DUNS number, it should contact Dun and Bradstreet directly to obtain one.

(1) An offeror may obtain a DUNS number--

(i) If located within the United States, by calling Dun and Bradstreet at 1-866-705-5711 or via the Internet at <http://www.dnb.com>; or

(ii) If located outside the United States, by contacting the local Dun and Bradstreet office.

(2) The offeror should be prepared to provide the following information:

(i) Company legal business.

(ii) Tradestyle, doing business, or other name by which your entity is commonly recognized.

(iii) Company Physical Street Address, City, State, and Zip Code.

(iv) Company Mailing Address, City, State and Zip Code (if separate from physical).

(v) Company Telephone Number.

(vi) Date the company was started.

(vii) Number of employees at your location.

(viii) Chief executive officer/key manager.

(ix) Line of business (industry).

(x) Company Headquarters name and address (reporting relationship within your entity).

d. If the Offeror does not become registered in the CCR database in the time prescribed by the Contracting Officer, the Contracting Officer will proceed to award to the next otherwise successful registered Offeror.

e. Processing time, which normally takes 48 hours, should be taken into consideration when registering. Offerors who are not registered should consider applying for registration immediately upon receipt of this solicitation.

f. The Contractor is responsible for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or

incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

g. (1)(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in Subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the CCR database; (B) comply with the requirements of Subpart 42.12 of the FAR; and (C) agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (g)(1)(i) of this clause, or fails to perform the agreement at paragraph (g)(1)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(2) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see FAR Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

h. Offerors and Contractors may obtain information on registration and annual confirmation requirements via the internet at <http://www.ccr.gov> or by calling 1-888-227-2423, or 269-961-5757.

**SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS**

NUMBER

TITLE

Attachment No. 1

Billing Instructions

Attachment No. 2

NRC Form 187