


**ORDER FOR SUPPLIES OR SERVICES**

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

BPA NO.

1. DATE OF ORDER <b>DEC 15 2008</b>		2. CONTRACT NO. (if any) GS35F0448N		6. SHIP TO:	
3. ORDER NO. NRC-DR3308344T002		MODIFICATION NO.		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts, CMB3 Attn: Manon Butt, Cont Spc, 301-492-3629 Mail Stop: TWB-01-B10M Washington, DC 20555		4. REQUISITION/REFERENCE NO. 33-08-344T002 11/20/2008		b. STREET ADDRESS William T. Dabbs Mail Stop T-2-C2M 11555 Rockville Pike	
7. TO:		c. CITY Rockville		d. STATE MD	e. ZIP CODE 20852
a. NAME OF CONTRACTOR KNOWLEDGE CONSULTING GROUP, INC.		f. SHIP VIA		8. TYPE OF ORDER	
b. COMPANY NAME		<input type="checkbox"/> a. PURCHASE		<input checked="" type="checkbox"/> b. DELIVERY	
c. STREET ADDRESS 11710 PLAZA AMERICA DR STE 520		REFERENCE YOUR Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.		Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
d. CITY RESTON	e. STATE VA	f. ZIP CODE 201904741		10. REQUISITIONING OFFICE CIO Computer Security Office (CSO)	
9. ACCOUNTING AND APPROPRIATION DATA This action administratively transfers \$167,695.24 in FY2008 funds previously obligated under Order NRC-DR-33-08-344. 87S-15-5D1-328 N7343 252A 31X0200.810 FFS# 10870535CC		11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. EMERGING SMALLBUSINESS <input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED		12. F.O.B. POINT Destination	
13. PLACE OF a. INSPECTION b. ACCEPTANCE		14. GOVERNMENT B/ NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) Award - 9/30/2009	
				16. DISCOUNT TERMS Net 30	

17. SCHEDULE (See reverse for Rejections) See CONTINUATION Page

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS # 007232429 Issuance of Task Order No. 002 under Order NRC-DR-33-08-344. Title: "Security Assessment Reviews."  Period of Performance: Award date through September 30, 2009, plus two option years.  See attached pages for description of the task order. Reference KCG's proposal for Task Order 2 dated 12/01/2008.  NRC Project Officer: Bill Dabbs, 301-415-0524, email Bill.Dabbs@nrc.gov    Note to NRC Accounting: Request FY08 funds in the amount of \$167,695.24, previously obligated under Delivery Order NRC-DR-33-08-344 dated 9/30/2008, to be administratively transferred to NRC-DR-33-08-344-T002 (Task Order No. 2).					

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		
21. MAIL INVOICE TO:						
a. NAME Department of Interior / NBC NRCPayments@nbc.gov						
b. STREET ADDRESS (or P.O. Box) Attn: Fiscal Services Branch - D2770 7301 W. Mansfield Avenue						
c. CITY Denver		d. STATE CO	e. ZIP CODE 80235-2230			
SEE BILLING INSTRUCTIONS ON REVERSE					\$481,991.93	17(h) TOTAL (Cont. pages)  17(i). GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature) 	23. NAME (Typed) Eleni Jernell Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER
---	---

AUTHORIZED FOR LOCAL REPRODUCTION  
PREVIOUS EDITION NOT AVAILABLE  
**TEMPLATE - ADM001**

**SUNSI REVIEW COMPLETE**

JAN 08 2009

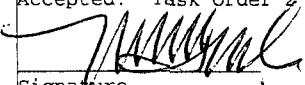
OPTIONAL FORM 347 (REV. 4/2006)  
PRESCRIBED BY GSA/FAR 48 CFR 53.213(f)  
**ADM002**

**ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION**

PAGE NO.  
2

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

DATE OF ORDER	CONTRACT NO. GS35F0448N	ORDER NO. NRC-DR3308344T002
---------------	----------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>Please indicate your acceptance of Task Order 2 by having an official authorized to bind your organization execute three copies of this document in the space provided below and return two copies to the U.S. Nuclear Regulatory Commission, Attn: Manon L. Butt, Division of Contracts, Mail Stop TWB-01-B10M, 11555 Rockville Pike, Rockville, MD 20852. Please retain the third copy for your records.</p> <p>Accepted: Task Order 2 under NRC-DR-33-08-344:</p> <p>                      Signature                      Maryann Hirsch                      Name                      President                      Title                      12/18/08                      Date</p> <p>Enclosure: Statement of Work</p>					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**TASK ORDER TERMS AND CONDITIONS**

NOT SPECIFIED IN THE CONTRACT

**A.1 NRC Acquisition Clauses - (NRCAR) 48 CFR Ch. 20**

**A.2 Other Applicable Clauses**

See Addendum for the following in full text (if checked)

52.216-18, Ordering

52.216-19, Order Limitations

52.216-22, Indefinite Quantity

52.217-6, Option for Increased Quantity

52.217-7, Option for Increased Quantity Separately Priced Line Item

52.217-8, Option to Extend Services

52.217-9, Option to Extend the Term of the Contract

**A.3 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within 15 days of the expiration date; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 20 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 two years and ten months.

**A.4 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)**

Funds are not presently available for performance under this contract beyond September 30, 2009. 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 September 30, 2009, 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.

In accordance with the task order procedures of Delivery Order NRC-DR-33-08-344, Senior Information Technology Security Officer Support Services, this definitizes Task Order No. 2, titled "Security Assessment Reviews." This effort shall be performed in accordance with the enclosed Statement of Work, the terms and conditions of Delivery Order NRC-DR-33-08-344, and GSA Schedule No. GS-35F-0448N.

Period of Performance and Cost

The period of performance for Task Order No. 2 is December 15, 2008 through September 30, 2009 for the base period. The term of this task order may be extended at the option of the Government for an additional two one-year option periods, as follows:

Option Year 1: October 1, 2009 through September 30, 2010.

Option Year 2: October 1, 2010 through September 30, 2011.

This is a time and material task order with a fixed ceiling of \$167,695.24 (base period). The total amount of this task order, if all option periods are exercised, is as follows:

Base Period: \$167,695.24.

Option Year 1: \$158,176.83

Option Year 2: \$156,119.86

Total: \$481,991.93

Price Schedule - Task Order No. 2 under NRC-DR-33-08-344:

Base Period: FY2009 12/15/2008 – 9/30/2009

NRC Labor Category	KCG GSA Labor Category	Labor Hours	Discounted Labor Rate	Total
Program Manager	Program Manager	[REDACTED]	[REDACTED]	\$9,760.00
Subject Matter Expert (SME)	Information Assurance Engineer IV	[REDACTED]	[REDACTED]	\$81,716.44
Senior Certified Information Systems Security Professional	Information Assurance Engineer III	[REDACTED]	[REDACTED]	\$76,218.80
Total Base Period		[REDACTED]		\$167,695.24

## Option Year One: FY2010 10/1/2009 – 9/30/2010

NRC Labor Category	KCG GSA Labor Category	Labor Hours	Discounted Labor Rate	Total
Program Manager	Program Manager			\$9,290.19
Subject Matter Expert (SME)	Information Assurance Engineer IV			\$77,037.94
Senior Certified Information Systems Security Professional	Information Assurance Engineer III			\$71,848.70
Total Option Year One				\$158,176.83

## Option Year Two: FY2011 10/1/2010 – 9/30/2011

NRC Labor Category	KCG GSA Labor Category	Labor Hours	Discounted Labor Rate	Total
Program Manager	Program Manager			\$9,183.94
Subject Matter Expert (SME)	Information Assurance Engineer IV			\$76,026.80
Senior Certified Information Systems Security Professional	Information Assurance Engineer III			\$70,909.12
Total Option Year Two				\$156,119.86

Total Price, Base Period plus Two Option Years

\$481,991.93

Travel, other than local travel, will not be needed on this task order. Local travel expenses will not be reimbursed.

Consideration and Obligation - Accounting and Appropriation Data

FY 2008 funding in the amount of \$167,695.24, previously obligated under Delivery Order NRC-DR-33-08-344, will be administratively transferred to fully fund the base period of this task order, NRC-DR-33-08-344-T002, up to the current ceiling. The original Appropriation Data from Delivery Order NRC-DR-33-08-344 is: B&R: 810-15-5D1-328, JCN: J1100, BOC: 252A, APP NO: 31X0200.810, FFS #10870535CC. However, the B&R number has changed to 87S-15-5D1-328, and the Job Code Number has changed to N7343.

Key Personnel

The following individuals are considered to be essential to the successful performance of work hereunder: Matt Brown, Program Manager; Hank Williams, Subject Matter Expert; and Philip LaViscount, Senior CISSP. The Contractor agrees that such personnel shall not be removed from the effort under the task order without compliance with Section A.5, Key Personnel, in basic Delivery Order NRC-DR-33-08-344.

NRC-DR-33-08-344-T002

Task Order No. 2 under NRC-DR-33-08-344

Page 6 of 6

The issuance of Task Order No. 2 does not change any terms and conditions of Delivery Order NRC-DR-33-08-344.

NRC contacts during the course of this task order are:

Technical Matters:

Bill Dabbs, Project Officer, phone 301-415-0524, CSO, Mail Stop T-2-C2M, email

[Bill.Dabbs@nrc.gov](mailto:Bill.Dabbs@nrc.gov).

Alan Sage, Technical Point of Contact, phone 301-415-7060, CSO, Mail Stop T-2-C2M, email

[Alan.Sage@nrc.gov](mailto:Alan.Sage@nrc.gov).

Contractual Matters:

Manon L. Butt, Contract Specialist, phone 301-492-3629, ADM/DC/CMB3, Mail Stop TWB-01-B10M, email [Manon.Butt@nrc.gov](mailto:Manon.Butt@nrc.gov).

## U.S. Nuclear Regulatory Commission

### Statement of Work for Task Order No. 2 under NRC-DR-33-08-344 Security Assessment Reviews

#### 1. Objective

The objective of this task order is to assist the U.S. Nuclear Regulatory Commission (NRC) in evaluating and reviewing the Certification and Accreditation (C&A) packages of NRC information systems.

#### 2. Type of Task Order

This is a time and materials task order with a fixed ceiling.

#### 3. Background

This activity will assist in ensuring NRC information systems adhere to federally mandated and NRC defined security requirements. Also, this activity will help the NRC to identify and understand the risks associated with operating these information systems.

A **Major Application (MA)** is a computerized information system or application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Because of their impact on the agency mission and the information they contain or process, Major Applications require special management oversight. (See OMB Circular A-130, Appendix III.) For example, an agency wide financial management system containing NRC's official financial records would be a Major Application. A computer program or a spreadsheet designed to track expenditures against an office budget would not be considered a Major Application. Similarly, commercial off-the-shelf software products (such as word processing software, utility software, or general purpose software) would not typically be considered Major Applications.

A **General Support System (GSS)** is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. (See OMB Circular A-130, Appendix III.) The mission objective of a GSS is to provide automated information systems (AIS) resources in support of the organizational mission. Typical GSSs are LANs, WANs, servers, and data processing centers.

A **Listed System** refers to a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to the operations of an NRC office or region, but is not an MA when viewed from an agency perspective. Most NRC systems rely on the security protections provided by the NRC LAN/WAN GSS. However, NRC offices have developed a number of additional non-major applications that are processing sensitive data such as individual privacy act information, law enforcement sensitive information, sensitive contractual and financial information, and other categories of

## U.S. Nuclear Regulatory Commission

### Statement of Work for Task Order No. 2 under NRC-DR-33-08-344 Security Assessment Reviews

sensitive information that the sponsor has determined will require additional security protections beyond the basic security provided by the NRC LAN/WAN. For those types of non-major applications that the sponsor has built in additional security protections and controls because of the added sensitivity of the information being processed, such a non-major application shall be categorized as a Listed System. The security plan for a listed system will describe those additional security protections and controls. These additional security controls could refer to the use of additional passwords, or the use of additional security technology such as virtual private networks (VPNs), digital signatures, secure Web sites, or other security solutions based on the use of public key infrastructure (PKI) technology. In addition, any system that processes classified information or unclassified Safeguards Information (SGI) that is not a GSS or a MA shall be categorized as a Listed System. An abbreviated security plan format that is compliant with National Institute of Standards and Technology (NIST) security plan guidance is available on the NRC internal web site.

The following link identifies the documents that makeup the C&A Package of an NRC information system:

[http://www.internal.nrc.gov/pmm/index.htm#pmm\\_security\\_c&a/guidances/roadmaps/iss\\_c%20a\\_deliv\\_EA44A8FB.html](http://www.internal.nrc.gov/pmm/index.htm#pmm_security_c&a/guidances/roadmaps/iss_c%20a_deliv_EA44A8FB.html). Depending upon whether the system is a GSS, MA, or Listed System, the requirements may include: Security Categorization, Privacy Impact Assessment (PIA) (if needed), E-Authentication Risk Assessment (if needed), Security Risk Assessment (SRA) Narrative, Security Risk Assessment (SRA) Asset List, Security Risk Assessment (SRA) Details, System Security Plan (SSP), Standard Test and Evaluation (ST&E) Plan, ST&E Report, Vulnerability Assessment Report (VAR), Plan of Action and Milestones (POA&M) Report, and Contingency Plan (CP).

#### **4. Scope of Work**

The contractor will develop a Security Assessment Review package for each system. The NRC expects the contractor will conduct eight Security Assessment Reviews per year over the performance of this task. At periodic points, the contractor will meet with the NRC to review progress (e.g. between subtasks 2 and 3, and subtasks 4 and 5). This package will be developed using the following specific subtasks:

- 1) Complete C&A Document Checklist Template - The object of this activity is to ensure current C&A documentation is being used for Review, Analysis, and Recommendations.
  - a. Download the documents found in the system's C&A package from ADAMS.
  - b. Ensure there is a complete inventory of the required documents.
  - c. Complete the C&A Document Checklist Template.
  - d. Ensure the C&A Document Checklist Template contains the following information for each document: name, version, ADAMS tracking number, date last modified, and status (Draft/Final).



U.S. Nuclear Regulatory Commission

Statement of Work for Task Order No. 2 under NRC-DR-33-08-344  
Security Assessment Reviews

- e. Review each technical control resolution and identify all supporting documents.
  - f. Add these supporting documents to the C&A Documentation Checklist Template and record the required information.
  - g. Deliver the C&A Document Checklist Template to the NRC Project Officer.
- 2) SSP Control Summary Template – The object of this activity is to ensure the status of the security controls has been accurately documented.
- a. Record the security control status for each control using the SSP Control Summary Template.
  - b. Determine if the controls are in-place, partially in-place, planned, risk based decision, and not applicable.
  - c. Verify that the technical resolution of each security control makes sense and does not conflict with its current status.
  - d. Deliver the SSP Control Summary Template to the NRC Project Officer.
- 3) C&A Risk Rating Crosswalk Template – The object of this activity to accurately document the risk levels found in the SRA Report, POA&M, VAR, and ST&E Report.
- a. Record the risk level of each control using the SRA Report, POA&M, VAR, and ST&E Report.
  - b. Verify that the risk rating documented in the SRA Report, POA&M, VAR, and ST&E Report corresponds to the control impact summary.
  - c. Verify all controls listed as not in place and partially in place have appropriate risk ratings.
  - d. Update the SSP Control Summary Template.
  - e. Deliver C&A Risk Rating Crosswalk Template and updated SSP Control Summary Template to the NRC Project Officer.
- 4) Draft Security Assessment Report (SAR) – The object of this activity is to draft the Security Assessment Report.
- a. Analyze each control and use that information to create the draft SAR.
  - b. Perform an analysis of the control status, control risk rating, control impact summary, and control recommendations.
  - c. Update the security risk assessment findings summary using the C&A Risk Rating Crosswalk Template.
  - d. Deliver draft SAR to the NRC Project Officer.

U.S. Nuclear Regulatory Commission

Statement of Work for Task Order No. 2 under NRC-DR-33-08-344  
Security Assessment Reviews,

- 5) Final SAR Package – The object of this activity is to finalize the SAR and produce the following draft documentation: SAR (with Executive Summary), POA&M, and Designated Approval Authority (DAA) Briefing Slides.
  - a. Update the SAR based on the review.
  - b. Develop the draft Accreditation Recommendation and DAA Accreditation Memos, the POA&M, Executive Summary, and DAA Briefing Slides.
  - c. Conduct internal review and finalize for delivery.
  - d. Develop finalized SAR.
  - e. Deliver the draft Accreditation Recommendation and DAA Accreditation Memos, the POA&M, Executive Summary, and DAA Briefing Slides to the NRC Project Officer.

Schedule

The estimated number of hours to complete the various phases of the Security Assessment Reviews for GSS, MA, and Listed Systems is shown below. There may be variations on these estimates based upon the complexity of each individual system and the maturity of the documentation.

Description	Number of Hours		
	MA	GSS	Listed
Complete C&A Document Checklist	97	75	43
Complete SSP Control Summary	130	100	57
Complete C&A Risk Rating Crosswalk	130	100	57
Draft SAR	130	100	57
Final SAR	52	40	23
POA&M	40	30	17
Accreditation Memos	32	25	14
DAA Briefing Slides	40	30	17

Information Handling and Ownership

The products and information associated with, or generated from, this project are considered sensitive information and property of the Nuclear Regulatory Commission and shall NOT be distributed, copied, transmitted, or by any other method, disclosed to the public or any individual without the express written permission of the NRC Contracting Officer.

U.S. Nuclear Regulatory Commission

Statement of Work for Task Order No. 2 under NRC-DR-33-08-344  
Security Assessment Reviews

**5. Period of Performance**

This task order shall have a base period of performance from the award date through September 30, 2009, and two (2) one year options.

**6. Travel**

Travel, other than local travel, will not be needed on this task order. Local travel expenses will not be reimbursed by the NRC.

**7. Meetings**

The Contractor's technical representative shall attend monthly status meetings at NRC Headquarters to discuss work being done under this task order.

**8. Technical Point of Contact**

The SITSOSS Technical Point of Contact is Alan Sage, Senior IT Specialist, FISMA Compliance and Oversight Team, CSO. Mr. Sage can be reached at 301-415-7060, Alan.Sage@nrc.gov.