ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 | 3

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO. NRC-33-05-339

1. DATE OF ORDER: AUG 19 2005	2. CONTRACT NO. (If any): GS35F0068J
3. ORDER NO.: NRC-33-05-339-003 MODIFICATION NO.	4. REQUISITION/REFERENCE NO.: NSR-05-508

5. ISSUING OFFICE (Address correspondence to):
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn:
Mail Stop T-7-I-2
Washington, DC 20555

6. SHIP TO:
a. NAME OF CONSIGNEE: U.S. Nuclear Regulatory Commission
ATTN: PAM KRUZIC
b. STREET ADDRESS: Mail Stop: T7D31
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20555

7. TO:
a. NAME OF CONTRACTOR: PROJECT PERFORMANCE CORPORATION
b. COMPANY NAME:
c. STREET ADDRESS: 1760 OLD MEADOW RD FL 4
d. CITY: MC LEAN | e. STATE: VA | f. ZIP CODE: 221022433

f. SHIP VIA:

8. TYPE OF ORDER
[ ] a. PURCHASE — 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.
[X] b. DELIVERY — Except for billing instructions on the reverse, this delivery/task 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.

9. ACCOUNTING AND APPROPRIATION DATA
511-15-5DC-385 R1121 251A 31X0200.511 $80,000
511-15-5DC-385 R1121 251A 31X0200.511 $90,000

10. REQUISITIONING OFFICE: NSR
NSIR/PMDA

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
[X] a. SMALL [ ] b. OTHER THAN SMALL [ ] c. DISADVANTAGED [ ] g. SERVICE-DISABLED VETERAN-OWNED
[ ] d. WOMEN-OWNED [ ] e. HUBZone [ ] f. EMERGING SMALL BUSINESS

12. F.O.B. POINT: Destination

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE			
Rockville, MD	Rockville, MD			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)
	The Contractor shall provide the U.S. Nuclear Regulatory Commission with "Federal Information Security Management Act (FISMA) Support", in accordance with the attached Statement of Work, the terms and conditons of GSA Contract GS-35F-0068J, and the attached schedule. ATTACHMENTS: 1. Schedule 2. Statement of Work 3. NRC Form 187 4. Billing Instructions Period of Performance: 08/23/05 - 08/22/06 (Base Period) 08/23/06-08/22/07 (Option 1); 08/23/06-02/22/07 (Option 2) ACCEPTANCE: Peter Dierbeck 9/30/05 SIGNATURE DATE Peter Dierbeck/Director of Contracts PRINT NAME/TITLE					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		
			$385,862.88	

21. MAIL INVOICE TO:
a. NAME: U.S. Nuclear Regulatory Commission
Payment Team, Mail Stop T-7-I-2
b. STREET ADDRESS (or P.O. Box): Attn: (NRC-33-05-339-003)
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20555

17(h) TOTAL (Cont. pages)

170,000.00

17(i). GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature)

23. NAME (Typed)
Robert B. Webber
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

TEMPLATE - ADM001

ADM002

OPTIONAL FORM 347 (REV. 3/2005)
PRESCRIBED BY GSA/FAR 48 CFR 53.213(e)

SISP REVIEW COMPLETE

TASK ORDER TERMS AND CONDITIONS NOT SPECIFIED IN THE CONTRACT

***** *Full Text '205221571' Ignored* *****

****

A.1 NRC ACQUISITION CLAUSES - (NRCAR) 48 CFR CH. 20
A.2 OTHER APPLICABLE CLAUSES

[X] 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

[X] 52.217-9, Option to Extend the Term of the Contract

***** *Begin Inserted Clause (Full Text) '205221570'* *****

A.3 2052.215-70 KEY PERSONNEL (JAN 1993)

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

[redacted] [redacted]

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

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor

shall immediately notify the contracting officer and shall, subject to the con-currence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

(c) Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution. The contracting officer and the project officer shall evaluate the contractor's request and the contracting officer shall promptly notify the contractor of his or her decision in writing.

(d) If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

***** *End Inserted Clause '205221570'* *****

A.4 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.

July 12, 2005

U.S. NUCLEAR REGULATORY COMMISSION (NRC)

OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE (NSIR)

STATEMENT OF WORK

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) SUPPORT

Provide FISMA support to the Office of Nuclear Security and Incident Response at the Nuclear Regulatory Commission.

Requested Period of Performance

Base Period: August 23, 2005 – August 22, 2006 (1 year)
Option Period 1: August 23, 2006 – August 22, 2007 (1 year)
Option Period 2: August 23, 2007 – February 22, 2008 (6 months)

Enclosure 1

1. Introduction

1.1 Background

The Office of Nuclear Security and Incident Response (NSIR) develops overall agency policy and provides management direction for evaluation and assessment of technical issues involving security at nuclear facilities. NSIR is the agency safeguards and security interface with the Department of Homeland Security (DHS), the intelligence and law enforcement communities, Department of Energy (DOE), and other agencies. NSIR develops emergency preparedness policies, regulations, programs, and guidelines for both currently licensed nuclear reactors and potential new nuclear reactors. It provides technical expertise regarding emergency preparedness issues and interpretations, conducts and directs the NRC program for response to incidents, and is the agency emergency preparedness and incident response interface with the DHS, Federal Emergency Management Agency (FEMA) and other Federal agencies.

Within the NRC, the Office of Information Systems (OIS) provides authoritative assistance, consultation, and guidance in the area of computer security and compliance. The information technology (IT) security staff within OIS ensures that agency programs comply with federal guidance including but not limited to the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB), and General Accounting Office (GAO) guidance.

In support of the NSIR mission there are numerous IT systems that must conform to the NRC IT security policies.

1.2 Objective

The objective of this delivery order is to obtain skilled personnel with expertise in the FISMA security process and other related security policies that can support NSIR in conforming to the NRC IT security policies.

1.3 Scope of Work

This engagement involves a number of discrete tasks, and then ongoing support on an as-needed basis in the following areas of interest:

a) Security Policy & Procedures
b) Security Architecture
c) Security Services
d) Business Continuity & Disaster Recovery
e) Certification & Accreditation
f) Security Monitoring and Incident Response
g) Security Education & Training
h) Security Program Management

These areas of interest will be applied across the NSIR enterprise and in support all NSIR systems (approximately five listed systems, five more classified listed systems, one major system with five sub-components and other projects that might arise within the engagement).

2. TASKS

This statement of work will require one FTE for the duration of the period of performance that will act as advocate for NSIR in all security matters and support the detailed tasks described below. It is expected that the assigned FTE will have access to additional – more specialized – resources that could be used if necessary for any task.

All of the work performed under this agreement, and any output produced throughout the life of the delivery order, shall incorporate and be in accordance with all applicable NRC policies and processes.

The following subsections describe specific tasks. Each task includes a description of the task as well as an estimated level of effort.

2.1 TASK 1 PLAN ENGAGEMENT

The contractor shall create an Engagement Plan that includes a schedule, financial plan, and plan for how resources (contractor and NRC resources) will be applied within the engagement.

This is a discrete task that will be performed once at the start if the engagement. This task is estimated at 10 person-days of effort.

2.1.1 Kick-Off Engagement

The contractor shall lead a kick-off meeting that brings together task participants and sets expectations on roles and responsibilities.

2.1.2 Survey Existing Systems

The contractor shall research existing NSIR systems to identify the systems, understand the classification (e.g. major, listed) of each system. As security planning is part of the systems lifecycle, the contractor shall ensure that the modernization, maintenance and training have been considered as well as where the system is in its security lifecycle of annual assessments & updates and triennial certification & accreditation.

2.1.3 Familiarize With Existing Documentation

The contractor shall become familiar with the existing security documentation for the NSIR systems. This will include the relevant security documentation as identified in Attachment 2 as well as any security-related Plan of Action and Milestone (POAM) documents.

2.1.4 Analyze Security Policies

Contractor shall analyze relevant NRC-specific security policies including:

a) Management Directive 12.5:NRC Automated Information Security Program
b) NRC-specific Security Templates

Contractor shall have familiarity with relevant FIPS and NIST security specifications as identified in attachment 2.

2.1.5 Author and Deliver Engagement Plan

The contractor shall author and deliver an Engagement Plan that includes:

a) List of systems that will be managed from a security perspective within this engagement;
b) Dates of discrete events and deliverables;
c) Budget for the engagement that is aligned with the NSIR three-year budget, the OMB Exhibit 300 financial data as well as the NRC OIS Form 9 budget preparation; and
d) Points of contact for the NSIR systems.
e) Additional resources that will be required from the contractor beyond the one FTE due to workload or specialized needs.

2.2 TASK 2 Security Policy & Procedures

The contractor shall author standard operating procedures plus roles and responsibilities in support of security compliance. This will be done within the context of the existing security policies, procedures, roles, and responsibilities and coordinated with other offices similarly applying the policies, procedures, roles, and responsibilities. The assignment of roles will ensure an appropriate separation of duties as intended by FISMA. The resulting policies and procedures will prescribe exactly which NSIR staff members will perform what security activities when in a project's lifecycle. The procedures shall be augmented with enough information to support budgeting of the activities.

The contractor shall stay informed of changes that might affect the correctness of the security policies and procedures including changes coming from OIS and other external sources (e.g. NIST). This may involve attending meetings as the NSIR representative to stay informed on any upcoming changes to security-related policies and procedures.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. As this entails applying the existing policies and procedures to the specifics of the NSIR systems and staff, this task is estimated at 5 person-days.

2.3 TASK 3 Security Architecture

The contractor shall support NRC-wide architecture security reviews and participate in government-wide and OMB architecture development as required. This will involve attending meetings as the NSIR representative and communicating findings to the NSIR staff in the form of meeting minutes.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. It is expected that this will require only an incidental level of effort spread across the contract period of one to two percent of the contractor's time.

2.4 TASK 4 Security Services

The contractor shall support periodic security assessments and annual updates of security documentation. This may involve providing assistance to NRC staff members or other contractors updating the documents, or it may involve transitioning responsibility of the documents and their upkeep to the contractor.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. This task is expected to take approximately 2/3 of the time within this engagement.

2.4.1 Support Security Assessments

The contractor shall support project managers during annual self assessments to assist in evaluation of system management, operational, and technical security controls.

2.4.2 Reformat Incident Response System (IRS) Security Documentation

The contractor shall reformat the existing IRS security plan to conform to the current NRC security documentation specifications. IRS is currently classified as a major system. This task will involve analyzing the existing plan, complete documentation to create new documentation as well as collaborating with NSIR team members to fill any gaps of information required in the new format.

2.4.3 Classified System Security Documentation

The contractor shall update the security documentation as appropriate for selected classified systems. New systems documentation and periodic reviews will be based on changes to the systems or updates based on new direction from the OIS. There are some dozen classified systems that may need document reviews. The contractor would need security clearance up to the secret level to complete this task.

2.4.4 Author Security Plans for Safeguard Information (SGI) Machines

The contractor shall author the security plans for the PC's and laptops that access SGI information (about fifty machines). The Office of Information Systems (OIS) has prepared templates to be used in the development of the security plans. This task could also involve developing generic security documents/templates for safeguards (SGI) personal computers and laptop machines. The contractor will need SGI clearance to complete this task.

2.4.5 Author NSIR-Wide Data Sensitivity Model

The contractor shall create an NSIR-wide data sensitivity model that will be used as a resource in the security categorizing of the systems.

2.4.6 Author Reusable Boilerplate Content

Based on the analysis of the systems and the assessment of existing security documentation, the contractor shall author sections of security documentation that can be applied across all of the NSIR systems to improve productivity, promote consistency, and ensure correctness. This will include sections of the Systems Categorization document, the Risk Assessment, and the Security Plan.

2.4.7 Update Security Documentation

The contractor shall update the security documentation as appropriate for NSIR systems. Documentation may need periodic updates or updates based on changes to the systems or updates based on new direction from the OIS. Other security plans for listed systems may be required.

2.5 TASK 5 Business Continuity & Disaster Recovery

The contractor shall support business continuity and disaster recovery as an ongoing task that will be applied as necessary throughout the duration of the engagement. This task is estimated to take approximately five percent of the time in this engagement.

2.5.1 Validate Contingency Test Plans

The contractor shall review and validate contingency test plans.

2.5.2 Support Contingency Testing

The contractor shall support business continuity testing. Each project will do its own business continuity testing; the contractor will play a supporting oversight role supporting the project manager as appropriate.

2.6 TASK 6 Certification & Accreditation

The contractor shall coordinate with the appropriate NRC staff, author documents, and support the certification and accreditation of the NSIR IT systems.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. The participation in the certification & accreditation process for the systems could become time consuming; it is estimated at up to 25% of the time within this engagement.

2.6.1 Review Security Test & Evaluation Reports

The contractor shall review the Security Test & Evaluation Reports created by the independent contractor that authored the Security Test & Evaluation Plan and Security Test & Evaluation Reports.

2.6.2 Review Certification & Accreditation Documentation

The contractor shall review the existing Certification & Accreditation documentation independently and in conjunction with stakeholders within NSIR and the OIS IT Security team to ensure correct, high-quality documents.

2.6.3 Update Certification & Accreditation Documentation

The contractor shall update Certification & Accreditation documentation as appropriate so that it adheres to the current accepted format and responds to any issues identified during the review.

2.7 TASK 7 Security Monitoring and Incident Response

The security & incident monitoring program is the responsibility of OIS and other maintenance contractors. The contractor shall coordinate with OIS for periodic penetration testing results.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. It is expected that this will require only an incidental level of effort spread across the contract period of one to two percent of the contractor's time.

2.7.1 Monitoring Security Controls

The contractor shall monitor the technical aspects of the compliance with security controls. This will involve monitoring system logs and possibly participating in periodic penetration testing.

2.7.2 Monitoring Audits and Logs

The contractor shall monitor operational and administrative aspects of compliance in the form of audits and logs.

2.8 TASK 8 Security Education & Training

The contractor shall coordinate with NSIR divisions, the Human Resources (HR) department, and OIS on security-related training. Training could include awareness training, training on the security controls, FISMA training, technical training (on such security-related topics as digital signatures and PKI), and training on authoring the security portions of the OMB 300. This might involve investigation of security training needs, analysis of available security training, and possibly authoring and delivering of security training.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. If there is no need to author custom security training material, this task is estimated to take from one to two percent of the contractor's time. If custom training material is deemed necessary, this estimate will be increased.

2.9 TASK 9 Security Program Management

The contractor shall develop metrics and management reporting to support effectiveness measurement and oversight. Contractor will also work with NRC staff to define and draft a short security program statement.

This is an ongoing task that will be applied as necessary throughout the duration of the engagement. It is estimated that this task will take up to five percent of the contractor's time.

3. PERIOD OF PERFORMANCE

The period of performance for this delivery order is August 23, 2005 through August 22, 2006 (Base Period) with two optional extensions, as outlined below:

Option Period 1: August 23, 2006 – August 22, 2007 (1 year)

Option Period 2: August 23, 2007 – February 22, 2008 (6 months)

4. DELIVERY SCHEDULE

The table below remarks on potential engagement deliverables. It is expected that the initial task of engagement planning will identify a more complete set of deliverables and a schedule. The delivery schedule shall be the contractor's responsibility and followed accordingly.

Task	Deliverable	Schedule
1 (2.1.1)	Kick-off meeting	Within 3 working days after delivery order award
1 (2.1.5)	Engagement Plan	Submit 10 working days after delivery order award
2 (2.2)	Standard Operating Procedures with Roles and Responsibilities	As scheduled
3 (2.3)	Meeting Minutes with Findings and Summary	Delivered within five working days after each security architecture meeting attended
4 (2.4.2)	IRS recertification documentation (~700 pages)	Five months after engagement plan
4 (2.4.3)	Classified Security Documentation	Per classified system as appropriate
4 (2.4.4)	Process generic SGI security plan for ~ 50 pc's and laptops	Two months after engagement plan
4 (2.4.5)	NSIR Data Sensitivity Model	As scheduled in Engagement Plan
4 (2.4.6)	Reusable Boilerplate Security Documentation Content	As scheduled in Engagement Plan
4 (2.4.7)	Security Risk Assessment	Per system as appropriate
4 (2.4.7)	E-Authentication Risk Assessment .	Per system as appropriate
4 (2.4.7)	Security Categorization Document	Per system as appropriate
4 (2.4.7)	Privacy Impact Assessment	Per system as appropriate
4 (2.4.7)	System Security Plan	Per system as appropriate
5 (2.5.1)	Contingency Plan	Per system as appropriate
6 (2.6.1)	Document Review Findings	Per security document reviewed delivered within three working days after each document review
7 (2.7)	Security & Incident Monitoring Program Plan	As scheduled
7(2.7)	Security & Incident Monitoring Data	Regularly gathered as defined in the Security & Incident Monitoring Program Plan
8 (2.8)	Security Training Material	As-needed
9 (2.9)	Security Program Plan (3 pages)	As scheduled in Engagement Plan
9 (2.9)	Security Program Measurement Plan	As scheduled in Engagement Plan
9 (2.9)	Security Program Metrics	Regularly gathered as defined in the Security Program Measurement Plan

The contractor shall submit all deliverables in paper copy and in electronic format in either WP 10.0 or WinWord Version XP on 3.5" floppy diskette or CD-ROM. Deliverables will be reviewed and signed off by the Project Officer.

5. ROLE OF THE NRC

The NRC Project Officer will provide overall program direction, review and approve all plans and deliverables including documents and assessment activities within the scope of the delivery order.

5.1 PROJECT OFFICER

The designated Project Officer for this work is:

Name: Pam Kruzic

Address: U.S. Nuclear Regulatory Commission

Mail-stop: T4A57

Washington, DC 20555

Telephone Numbers: (301) 415-1170, FAX: (301) 415-6382

E-mail address: pgk2@nrc.gov

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(g) 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.

(h) 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.

(End of Clause)

6. PERSONNEL AND MANAGEMENT REQUIREMENTS

The contractor shall provide the correct number of qualified, competent, and fully trained personnel to perform the activities delineated under this delivery order. The contractor's personnel shall act in a courteous, responsive, knowledgeable, and professional manner at all times.

The contractor shall have the professional communication skills required to take the necessary actions to contact, meet with, discuss, and otherwise obtain information required to

accomplish the items described in this statement of work on his/her own initiative without supervision. This will involve regular communications – formal and informal – with senior NRC staff members.

The contractor will be required to deliver the FISMA support under the direction of a project manager. The contractor's project manager shall be responsible for overall execution of the provisions of the contract including the provision of all required technical and financial reports.

7. SAFEGUARD OF INFORMATION

In connection with the performance of the work under this delivery order, the contractor may be furnished, or may develop or acquire, proprietary data (trade secrets) or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub.L. 93-579) or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor agrees to hold the information in confidence and not to 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 delivery order. 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 delivery order.

8. MEETINGS AND TRAVEL

Minimal travel is expected during the delivery order to NRC Headquarters (Rockville, MD), 11545 Rockville Pike, Rockville, MD 20852.

9. GOVERNMENT FURNISHED EQUIPMENT

a. The following resources shall be provided by the NRC:

(1) NRC will grant the Contractor appropriate access to the NRC Rockville, MD building and the applicable databases.

(2) For the duration of the project, the NRC will provide one standard workstation with a standard NRC PC (with a CD-ROM, 3.5" floppy disk) and a Monitor at the NRC Headquarters in Rockville, MD. As appropriate this machine will also have access to removal hard drive, attached printer and Microsoft office. This workstation will have the appropriate access to required staff and data and may be in a security access controlled area. There will be an E-mail account for the contractor. The workstation will have internet connection but all internet access will be monitored by the LAN system administrator.

b. The contractor shall be responsible and accountable for all Government property provided under this contract and shall comply with the provisions of the FAR Government Property Clause under this contract and FAR Subpart 45.5, as in effect on the date of this contract. The contractor shall investigate and provide written notification to the NRC Contracting Officer (CO) and the NRC Division of Facilities and Security, Physical Security Branch of all cases of loss, damage, or destruction of Government property in its possession or control not later than 24 hours after discovery. The contractor must report stolen

Government property to the local police and a copy of the police report must be provided to the CO and to the Division of Facilities and Security, Physical Security Branch.

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

10.0 SECURITY REQUIREMENTS

The Contractor and all its personnel shall comply with the security requirement listed below.

2052.204-70 SECURITY (March 2004)

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

(End of Clause)

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 Security Branch, Division of Facilities and Security (SB/DFS). In this regard, all contractor personnel whose duties under this contract require their presence on-site shall be clearly identifiable by a distinctive badge furnished by the NRC. The Project Officer shall assist the contractor in obtaining badges for the contractor personnel. It is the sole responsibility of the contractor to ensure that each employee has a proper NRC-issued identification/badge at all times. All photo-identification badges must be immediately (no later than three days) delivered to SB/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must display any NRC issued badge in clear view at all times during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work, and to assure the protection of any Government records or data that contractor personnel may come into contact with."

SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL

The contractor shall ensure that all its employees, including any subcontractor employees and any subsequent new employees who are assigned to perform the work herein, are approved by the Government for building access. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award.

A contractor employee shall not have access to NRC facilities until he/she is approved by Security Branch, Division of Facilities and Security (SB/DFS). Temporary access may be approved based on a favorable adjudication of their security forms. Final access will be approved based on favorably adjudicated background checks by General Services Administration in accordance with the procedures found in NRC Management Directive 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. When an individual receives final access, the individual will be subject to a reinvestigation every five years.

The Government shall have and exercise full and complete control over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. Individuals performing work under this contract shall be required to complete and submit to the contractor representative an acceptable GSA Form 176 (Statement of Personal History), and two FD-258 (Fingerprint Charts). Non-U.S. citizens must provide official documentation to the DFS/SB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U. S. Citizenship and Immigration Services. Any applicant with less than two years residency in the U. S. will not be approved for building access. The contractor representative will submit the documents to the Project Officer who will give them to the SB/DFS. SB/DFS may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the GSA Form 176. Also, in the exercise of its authority, GSA may, among other things, grant or deny permanent building access approval based on the results of its investigation and adjudication guidelines. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the work sites for an extended period of time during the term of the contract. In the event that SB/DFS and GSA are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

The contractor will immediately notify the Project Officer when a contractor employee terminates. The Project Officer will immediately notify SB/DFS (via e-mail) when a contractor employee no longer requires building access and return any NRC issued badges to the SB/DFS within three days after their termination.

SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY ACCESS APPROVAL

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 over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract.

SECURITY REQUIREMENTS FOR 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. Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and will require a favorably adjudicated Limited Background Investigation (LBI).

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by Security Branch, Division of Facilities and Security (SB/DFS). Temporary access may be approved based on a favorable adjudication of their security forms and checks. Final access will be approved based on a favorably adjudicated LBI in accordance with the procedures found in NRC MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to SB/ 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 (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3 which is incorporated into this contract by reference as though fully set forth herein. Based on SB review of the 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 under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level I approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E. O. 12968.

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) 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 of 30 days) to NRC Headquarters controlled buildings; or otherwise requires issuance of an NRC badge.

SECURITY REQUIREMENTS FOR 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. Such contractor personnel shall be subject to the NRC contractor personnel requirements of MD 12.3, Part I, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Access National Agency Check with Inquiries (ANACI).

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by SB/DFS. Temporary access may be approved based on a favorable review of their security forms and checks. Final access will be approved based on a favorably adjudicated ANACI in accordance with the procedures found in MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC SB/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 (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on SB review of the 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 under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level II approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E.O. 12968.

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) 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 30 days) to NRC Headquarters controlled buildings; or otherwise requires issuance of an NRC badge.

For the purpose of this task, the contractor employee(s) shall fulfill security requirements for Level I.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for investigation is to be withdrawn or canceled, the contractor shall immediately notify the Project Officer by telephone in order that he/she will immediately contact the SB/DFS so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing to the Project Officer who will forward the confirmation via email to the SB/DFS. Additionally, SB/DFS must be immediately notified 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 access under the NRC "Personnel Security Program."

SECURITY REQUIREMENTS FOR ACCESS TO CLASSIFIED MATTER OR INFORMATION

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

The proposer/contractor must identify all individuals to work under this contract and propose the type of security clearance required for each. The NRC sponsoring office shall make the final determination of the type of security clearance required for all individuals working under this contract.

Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and 10 CFR Part 10.11, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Single Scope Background Investigation(SSBI) for "Q" clearances or a favorably adjudicated Limited Background Investigation (LBI) for "L" clearances.

A contractor employee shall not have access to classified information until he/she is granted a security clearance by the Security Branch, Division of Facilities and Security (SB/DFS), based on a favorably adjudicated investigation. In the event the contractor employee's investigation cannot be favorably adjudicated, their interim approval could possibly be revoked and the individual could be subsequently removed from the contract. The individual will be subject to a reinvestigation every five years for "Q" clearances and every ten years for "L" clearances.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project

Officer to SB/DFS for review and submission to the Office of Personnel Management for investigation. The individual may not work under this contract until SB has granted them the appropriate security clearance, read, understand, and sign the SF 312, "Classified Information Nondisclosure Agreement." The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on SB review of the applicant's investigation, the individual may be denied his/her security clearance in accordance with the due process procedures set forth in MD 12.3 Exhibit 1, E. O. 12968, and 10 CFR Part 10.11.

In accordance with NRCAR 2052.204-70 cleared contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) 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 classified information; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires NRC photo identification or card-key badges.

ATTACHMENT LIST

Number	Title
1.	NRC Form 187 - Contract Security and/or Classification Requirements
2.	List of Relevant Security Documents

Attachment 2 – Relevant Security Documents

The contractor shall have familiarity with relevant security specifications including:

a) Security Risk Assessment
b) E-Authentication Risk Assessment
c) Security Categorization Document
d) Privacy Impact Assessment
e) System Security Plan
f) Security Test & Evaluation Plan
g) Security Test & Evaluation Report
h) Contingency Plan
i) Contingency Test Report

The contractor shall have familiarity with relevant security specifications including:

a) FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
b) FIPS 200 Minimum Security Controls for Federal Information Systems
c) NIST SP 800-30 Risk Management Guide for Information Technology Systems, July 2002
d) NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
e) NIST SP 800-60, Volume II: Guide for Mapping Types of Information and Information Systems to Security Categories
f) NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems
g) NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems
h) NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems
i) NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems
j) NIST SP 800-53 Recommended Security Controls for Federal Information Systems
k) NIST SP 800-64 Security Considerations in the Information System Development Life Cycle
l) Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources
m) DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM)
n) Additional issuances from the Committee on National Security Systems relevant to classified systems
o) Federal Information Security Management Act 2002
p) NRC Management Directive 12.5 (to be furnished upon contract award)

NRC FORM 187
(1-2000)
NRCMD 12

U.S. NUCLEAR REGULATORY COMMISSION

CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

AUTHORITY
The policies, procedures, and criteria of the NRC Security Program, NRCMD 12, apply to performance of this contract, subcontract or other activity.

COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE

1. CONTRACTOR NAME AND ADDRESS	A. CONTRACT NUMBER FOR COMMERCIAL CONTRACTS OR JOB CODE FOR DOE PROJECTS (Prime contract number must be shown for all subcontracts.)		2. TYPE OF SUBMISSION
	B. PROJECTED START DATE	C. PROJECTED COMPLETION DATE	☑ A. ORIGINAL ☐ B. REVISED (Supersedes all previous submissions) ☐ C. OTHER (Specify)
	08/01/2005	10/15/2007	

3. FOR FOLLOW-ON CONTRACT, ENTER PRECEDING CONTRACT NUMBER AND PROJECTED COMPLETION DATE

A. DOES NOT APPLY	B. CONTRACT NUMBER	DATE
☑		

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

Federal Information Security Management Act (FISMA) Support

5. PERFORMANCE WILL REQUIRE A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION ☑ YES (If "YES," answer 1-7 below) ☐ NO (If "NO," proceed to 5.C.)	NOT APPLICABLE	NATIONAL SECURITY		RESTRICTED DATA	
		SECRET	CONFIDENTIAL	SECRET	CONFIDENTIAL
1. ACCESS TO FOREIGN INTELLIGENCE INFORMATION	☑	☐	☐	☐	☐
2. RECEIPT, STORAGE, OR OTHER SAFEGUARDING OF CLASSIFIED MATTER. (See 5.B.)	☑	☐	☐	☐	☐
3. GENERATION OF CLASSIFIED MATTER.	☐	☑	☑	☐	☐
4. ACCESS TO CRYPTOGRAPHIC MATERIAL OR OTHER CLASSIFIED COMSEC INFORMATION.	☐	☑	☑	☐	☐
5. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION PROCESSED BY ANOTHER AGENCY.	☐	☑	☑	☐	☐
6. CLASSIFIED USE OF AN INFORMATION TECHNOLOGY PROCESSING SYSTEM.	☐	☑	☑	☐	☐
7. OTHER (Specify) safeguards	☑	☐	☐	☐	☐

B. IS FACILITY CLEARANCE REQUIRED? ☒ YES ☐ NO

C. ☐ UNESCORTED ACCESS IS REQUIRED TO PROTECTED AND VITAL AREAS OF NUCLEAR POWER PLANTS.

D. ☑ ACCESS IS REQUIRED TO UNCLASSIFIED SAFEGUARDS INFORMATION.

E. ☑ ACCESS IS REQUIRED TO SENSITIVE IT SYSTEMS AND DATA.

F. ☑ UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING.

FOR PROCEDURES AND REQUIREMENTS ON PROVIDING TEMPORARY AND FINAL APPROVAL FOR UNESCORTED ACCESS, REFER TO NRCMD 12.

c. INFORMATION PERTAINING TO THESE REQUIREMENTS OR THIS PROJECT, EVEN THOUGH SUCH INFORMATION IS CONSIDERED UNCLASSIFIED, SHALL NOT BE RELEASED FOR DISSEMINATION EXCEPT AS APPROVED BY:

NAME AND TITLE	SIGNATURE	DATE
Pamela Kruzic	Kruzic	12 July 05

7. CLASSIFICATION GUIDANCE

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

N/A

8. CLASSIFIED REVIEW OF CONTRACTOR / SUBCONTRACTOR REPORT(S) AND OTHER DOCUMENTS WILL BE CONDUCTED BY:

☑ AUTHORIZED CLASSIFIER (Name and Title) ☐ DIVISION OF FACILITIES AND SECURITY

A Lynn Sivious

9. REQUIRED DISTRIBUTION OF NRC FORM 187 *Check appropriate box(es)*

☑ SPONSORING NRC OFFICE OR DIVISION (Item 10A) ☑ DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT

☑ DIVISION OF FACILITIES AND SECURITY (Item 10B) ☑ CONTRACTOR (Item 1)

☐ SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

10. APPROVALS

SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

NAME (Print or type)	SIGNATURE	DATE
A. DIRECTOR, OFFICE OR DIVISION Miriam Cohen	SIGNATURE	DATE 7/12/05
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY for K. O. Greene	SIGNATURE Calvin Byrd	DATE 7-28-05
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT (Not applicable to DOE agreements) / Barbara Mecham for Mary Lynn Scott	SIGNATURE Robert F. Webber	DATE 7/28/05

REMARKS