



**DELIVERY ORDER DR-33-06-317  
TASK ORDER T026  
MAJOR/MODERATE C&A: REACTOR PROGRAM SYSTEM (RPS)**

**1.0 OBJECTIVE**

The Contractor shall support the OIS in certification and accreditation of major information systems such that NRC is in compliance and maintains certification and accreditation currency with NIST and FISMA Guidance. The Contractor shall at a minimum develop associated certification and accreditation documentation consistent with the security support task referenced in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317, entitled, "C&A PROCESS AND DELIVERABLES" such that an Authorization to Operate (ATO) which confers full accreditation shall be granted the system. The Contractor shall perform these security support tasks specified for a MODERATE security baseline system.

The Contractor shall develop, at a minimum, the following information system security certification documentation: a security test and evaluation plan and associated report, a contingency test plan and report, and a plan of action and milestones to correct any identified deficiencies.

**2.0 SCOPE OF WORK**

The Contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that the Reactor Program System (RPS) obtains an Authorization to Operate (ATO) and no system crosses fiscal year boundaries with an Interim Authorization to Operate (IATO).

**System Name:** Reactor Program System (RPS)

**Sponsor Office:** Office of Nuclear Reactor Regulation (NRR)

**System Owner:** Jim Dyer, Director, NRR

**System Description:** The Reactor Program System (RPS) is an NRC Privacy Act System of Records, it provides the NRC with the capability for planning, scheduling, conducting, reporting, and analyzing inspection activities at U.S. nuclear power reactor facilities, and is used as a tool on policy and inspection guidance and assesses the effectiveness and uniformity of the implementation of those programs. Used to plan and schedule licensing and other reactor regulatory activities, it is a critical part of the NRC's license fee collection process. It includes inspection and licensing information, plant performance indicators, inspection follow-up items, safety issue data, NRC staff data, facility characteristics and other reactor regulatory data.

**Status:** RPS is operational.

The Contractor shall provide security analyst staff and the development of the associated documentation associated with the security support tasks specified below for unclassified MODERATE security baseline systems for the system category "Major Application", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 - C&A PROCESS AND DELIVERABLES.

The term "Major Application" (MA) means 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, MA's 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 an MA. A computer program or a spreadsheet designed to track

expenditures against an office budget would not be considered an MA. Similarly, commercial off-the-shelf software products (such as word processing software, electronic mail software, utility software, or general purpose software) would not typically be considered MA's.

### 3.0 PERIOD OF PERFORMANCE

The period of performance of this task order is January 26, 2007 through July 26, 2007.

### 4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is \$48,598.51.
- (b) The amount presently obligated with respect to this task order is \$48,598.51. The Contractor shall not be obligated to incur costs above this ceiling/obligated amount unless and until the Contracting Officer shall increase the amount obligated. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

### 5.0 TRAVEL

No travel is required.

### 6.0 SCHEDULE

The Contractor shall provide final draft security documentation and reports for each system consistent with the NRC-approved integrated project plan (Subtask 1).

### 7.0 SPECIFIC TASKS

The Contractor shall support the NRC C&A of the Reactor Program System and application service provider facility as described below:

#### **Subtask 1: Integrated Security Activity Project Plan.**

Develop and implement a project plan to ensure completion of the RPS certification and accreditation tasks within the period of performance. The Contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling for the program. These deliverables shall be developed at the individual project level (i.e., each system for which a certification and accreditation effort will be undertaken) and aggregate to the program level. The Microsoft Project Plan shall incorporate all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Microsoft Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The project plan will include:

- A Level 5 **Work Breakdown Structure (WBS)**. The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured.

Each work package shall be assigned a start and finish date, a budget value, and can be integrated with higher-level schedules.

- A **schedule and budget** for accomplishing the work identifying what resources are needed and how much effort will be required in what time frame to complete each of the tasks in the WBS. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS, and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

## **Subtask 2: Systems Security Controls and Security Requirements Test Plan Development Support.**

The Contractor shall support the NRC staff in the development and documentation of a test plan within the Rational Suite Enterprise that exercises the systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations such that confirmation that the system and associated controls are operating as intended and in accordance with NIST SP 800-53A, NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC System Security Test and Evaluation Plan Template. The Contractor shall provide detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E Plan shall identify all testing assumptions, constraints, and dependencies and include a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing of all system security functional and assurance requirements where the requirements are not stated as being fulfilled by another system. The following test methods shall be used:

### **Analysis**

The "analysis" verification method shall be used to appraise a process, procedure, or document to ensure properly documented actions (e.g. risk assessments, audit logs, organization level policies, etc.) are in compliance with established requirements. An example of "analysis" as an evaluation technique would be to review documented physical security policies and procedures to ensure compliance with established requirements. This verification method is often called a documentation review.

### **Demonstration**

The Contractor will observe randomly individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. (Example: Observe visitors upon computer room entry in order to verify that all visitation procedures are followed.)

### **Interview**

The Contractor will interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.

### **Inspection**

The Contractor will review and analyze visitor logs to verify all information requested has been entered on the log. (Example: The Contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.)

### **Technical Test**

The Technical Test verification method shall be used to verify that each implemented control is functioning as intended with the Contractor attempting to access a system by logging on to that system from his workstation (or other device) using an incorrect password to see if the system responds with an error message stating incorrect password or denies access after exceeding the maximum threshold for logon attempts and is directed to call the system administrator to gain access.

Testing requirements that are stated as being fulfilled by another system (provider) shall be accomplished by verifying that the provider system security plan in-place controls meet the requirement.