

DELIVERY ORDER DR-33-06-317

TASK ORDER (72)

Atomic Safety and Licensing Board Panel (ASLBP)

Certification and Accreditation (C&A) Support

1.0 OBJECTIVE

The contractor shall support the Atomic Safety and Licensing Board Panel (ASLBP) in the certification and accreditation of the following:

- DDMS – Digital Data Management System – This is a Major Application with a sensitivity of: Confidentiality (M), Integrity (M), and Availability (M).

2.0 BACKGROUND

The following summarizes the systems that the contractor will be working with:

DDMS

The ASLBP conducts all licensing and other hearings as directed by the Commission, primarily through individual three-judge Atomic Safety and Licensing Boards appointed by either the Commission or the Chief Administrative Judge. In addition to adjudicating licensing and enforcement cases regarding nuclear power reactors and nuclear materials, ASLBP will be responsible for conducting the adjudicatory proceeding regarding the Department of Energy's (DOE) application for construction authorization for a high-level waste (HLW) repository at Yucca Mountain, NV. The scope and nature of this proceeding, as well as the agency's other reactor and materials licensing adjudications, dictate the essential need for efficient capture and management of the enormous volume of multimedia data that must be processed and displayed in a very short time frame.

The U.S. Nuclear Regulatory Commission (NRC) established digital information retrieval, utilization, and display capabilities in conjunction with the potential licensing proceeding for a HLW repository. The Digital Data Management System (DDMS) has been successfully developed and deployed in the NRC Two White Flint North (TWFN) complex in Rockville, MD and in a GSA-leased building in Las Vegas. It is also available via the Internet to authorized hearing participants.

Because judges, lawyers, counsel for parties, and technical support staff will use the DDMS interchangeably in both Rockville and Las Vegas in support of the Yucca Mountain proceeding as well as other proceedings, the components installed in the Las Vegas facility are basically identical to those installed in Rockville. The data and document files stored in the Rockville system must be made available to support hearings held in Las Vegas, and vice versa, driving a requirement that the databases and data files under this effort be a virtual mirror image in both locations.

The currently operational Enterprise DDMS enables the creation and use of an integrated, comprehensive digital record for adjudicatory proceedings. Using information that is pre-filed electronically by hearing participants in the Agencywide Documents Access and Management System (ADAMS)-based Electronic Hearing Docket (EHD), the DDMS records, stores, and displays the text and image of documents and other digital data presented in the hearings and permits access and retrieval of the entire documentary and video record of the proceeding in an electronic format. The system allows counsel for the parties to bring prepared materials to the evidentiary hearings electronically and to have them integrated and accessible concurrently with the record being presented in the hearing room. The record is continually accessible by the presiding officer and the parties in the proceeding. The DDMS supports hearing activities and information management during all hearing phases

3.0 PERIOD OF PERFORMANCE

The period of performance for this task order is September 10, 2009 through September 09, 2010.

4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$117,912.56** (includes **\$7,500** for NTE travel).
- (b) The amount presently obligated with respect to this task order is **\$110,000.00**. 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 is done so at the Contractor's sole risk.

5.0 SCOPE OF WORK

The contractor must ensure the system has been installed, configured, and maintained according to federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The contractor will identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The contractor shall perform the following:

Tasks	DDMS (Update)
Subtask 2 - E-Authentication Risk Assessment	N/A
Subtask 3 - Security Categorization Package <ul style="list-style-type: none"> • Security Categorization Document • Security Categorization Memo • Privacy Impact Assessment • Records Management Form 637 	N/A
Subtask 4 - Security Risk Assessment (SRA)	Shall Update the DDMS SRA
Subtask 5 - System Security Plan (SSP)	N/A
Subtask 6 - Preliminary System Testing	N/A
Subtask 7 - Standard Test and Evaluation (ST&E) Plan	Shall develop ST&E Plan
Subtask 8 - System Testing <ul style="list-style-type: none"> • ST&E Report • Vulnerability Assessment Report • Plan of Action and Milestone (POA&M) Report. 	Shall perform system testing.
Subtask 9: - Contingency Plan	Shall develop the system Contingency Plan

Tasks	DDMS (Update)
Subtask 10 – Contingency Test Report	<p>Shall work with the system owner to verify, validate, and document the results of the system’s contingency test.</p> <p>Upon completion of the Contingency Test, the contractor shall work with the system owner to update system’s Contingency Plan to reflect validated information.</p>
<p>Subtask 11 - Authority To Operate (ATO) Package</p> <ul style="list-style-type: none"> • Approval to Operate Memo • Package Includes Named Deliverables 	<p>Shall put together an ATO Package for system owner.</p> <p>The contractor shall deliver the updated ATO Package to the system owner by 1/8/2010.</p>

The contractor shall ensure that the steps, templates, and reports outlining certification and accreditation in NRC’s Project Management Methodology are utilized and followed.

The contractor shall provide the necessary security support staff to develop the associated documentation to support the tasks specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 “C&A PROCESS AND DELIVERABLES” for unclassified systems.

6.0 SCHEDULE

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

7.0 TASKS

The contractor shall support the Certification and Accreditation according to SOW Enclosure 6 and Section B “Schedule of Supplies or Services and Prices”.

Subtask 1: Integrated Security Activity Project Plan

The contractor shall develop and implement a project plan to ensure the completion of the tasks identified in this SOW occurs as expected. The contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling. 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 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 Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The Project Plan will include:

- **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.

- **Schedule and Budget**

The schedule and budget will identify what resources are needed, identify how much effort is required, and when each of the tasks specified in the WBS can be completed. 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: E-Authentication Risk Assessment

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. The focus is on remote authentication of individual people over a network, for the purpose of electronic government or commerce. The OMB M-04-04 memorandum guidance applies to systems that have remote authentication of users of Federal agency information technology systems for the purposes of conducting Government business electronically (or e-government). The guidance does not apply to internal only systems or the authentication of servers, or other machines and network devices. NRC's policy is to only require separate E-authentication Risk Assessments on systems where it is required. E-Authentication Risk Assessments shall be consistent with OMB M04-04, NIST SP 800-30, NIST SP 800-60A, and NIST SP 800-63.

Subtask 3: Security Categorization Package

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs; (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. NRC's Security Categorization Package contains the following deliverables: Security Categorization Memo, Security Categorization Document, Privacy Impact Assessment, and Records Management Form 637.

A Security Categorization Package shall be completed for each new major application/general support system, listed system, contractor system, and those owned by other Federal agencies.

Subtask 4: Security Risk Assessment

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

This Assessment is an important activity in an agency's information security program that directly supports security accreditation and is required by the FISMA and OMB Circular A-130, Appendix III. This assessment influences the development of the security controls for an information system and generates much of the information needed for the system's security plan.

The assessment shall characterize the information processed by using FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. The risk assessment shall follow NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and include the following:

- Identification of user types and associated roles and responsibilities;
- Identification of risk assessment team members and their associations;
- A description of the risk assessment approach and techniques, where the techniques include documentation review, interviews, observation, and system configuration assessments, security scans and penetration tests;
- A description of the risk scale used, including at a minimum, the potential impact as defined in FIPS 199, and likelihood as defined in NIST SP 800-30, Risk Management Guide for Information Technology

Systems;

- A list of potential system vulnerabilities;
- A list of potential threat-sources applicable to the system, including natural, human, and environmental threat-sources;
- A table of vulnerability and threat-source pairs and observations about each;
- Detailed findings for each vulnerability and threat-source pair discussing the possible outcome if the pair is exploited; existing controls to mitigate the pair; the likelihood determination as high, moderate, or low; the impact determination expressed as high, moderate, or low; the overall risk rating based upon the risk scale; and the recommended controls to mitigate the risk; and,
- A summary that includes the number of high, moderate, and low findings and provides a list of prioritized action items based upon the findings.

The assessment shall be documented in a report that follows the NRC Template for the Risk Assessment Report. The report shall be delivered in draft form and then in final form after NRC comments are incorporated.

Any residual risk is tracked in the Plan of Action and Milestones (POA&M) Report. The POA&M Report documents the results of this process. POA&Ms include documenting the risk number, a description of each risk, the type of risk (i.e., impacting the confidentiality, integrity, or availability), the level of risk (i.e., low, moderate, or high), the associated controls, and the action(s) required or actually performed to eliminate or minimize each risk. The goal is to remediate all high and moderate security findings, and track the remaining security findings using the system's POA&M Report.

Subtask 5: Systems Security Plan

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The SSP shall be developed in accordance with 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 IT Security Plan Template. The SSP identifies the necessary security controls that are required, citing the security controls that are in place, those that are planned, those that are not planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The SSP shall be documented in a report that follows the NRC Template. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The SSP shall be updated after completion of the ST&E test report to reflect validated in-place and planned controls.

Subtask 6: Preliminary Testing

The contractor shall perform a preliminary assessment of the system to ensure the system is compliant with federally mandated and NRC defined security requirements. The contractor shall identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The contractor shall obtain from the system owner a list of deviations that have been approved by the Designated Approving Authorities (DAAs), so these risks can be factored in during testing. Accepted risks are still reported, evaluated, and documented.

This subtask includes the automated and manual testing of the different system platforms to ensure they have been configured, operated, and maintained correctly. Also, the contractor must ensure the entire system is

tested including those components not identified in this SOW. This testing specifically excludes any Development/Test Environment.

The following is a list of some of the standards that must be checked:

- National Institute of Standards and Technology (NIST) Federal Information Processing (FIPS) 140-2. When checking NIST FIPS 140-2, the contractor must ensure that all cryptography used in the system has been validated, has a current FIPS 140-2 certificate, and the configuration of that cryptography complies with the security policy specified by the certificate for the cryptographic module.
- NIST 800-53 Rev 2 or later standard. The contractor must ensure the system complies with the technical, managerial, and procedural controls found in this standard.
- NRC Hardening Standards. The contractor must ensure the system meets all the NRC hardening standards. For a complete list of Hardening standards please see "<http://www.internal.nrc.gov/ois/it-security/guidance.html>".

The CSO has purchased a Center for Internet Security License for the NRC giving the organization the ability to access CIS Benchmarks; to distribute CIS Benchmark documents and tools; and to use CIS Benchmarks for commercial purposes.

Note: When a federally mandated configuration or NRC hardening standard have not been specified, the contractor will test that component using the vendor's suggested best security practices.

The contractor shall document the results and observations of this process. This shall include documenting the risk number, a description of each risk, the type of risk (i.e., impacting the confidentiality, integrity, or availability), the level of risk (i.e., low, moderate, or high), the associated controls, and the action(s) required or actually performed to eliminate or minimize each risk. The goal is for the system owner to remediate all high/moderate security findings/risks and track those risks using a Plan of Action and Milestone (POA&M) Report.

The contractor shall be responsible for coordinating and executing all applicable site access and non-disclosure agreements and authority to scan forms with parties other than the Nuclear Regulatory Commission prior to commencement of the above mentioned activities, ensuring that project schedules are not impacted.

Subtask 7: ST&E Plan

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The ST&E plan exercises the system's 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 Guide for accessing the Security Controls in Federal Information Systems
- 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
- NRC System Security Test and Evaluation Plan Template

The ST&E plan provides detailed test procedures to ensure all federally mandated and NRC defined security requirements are fully tested. These procedures contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E plan identifies all testing assumptions, constraints, and dependencies and includes 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. Also, the contractor shall ensure testing identifies any operational risks found that may affect the system's ability to

perform its mission and protect its data (stored and transmitted). Additionally, the contractor must ensure the ST&E Plan includes the entire 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 random individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. For 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 ensure security controls have been properly implemented and maintained. For 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. For example, the contractor will attempt to access the system by logging on to the system from an end user workstation (or other device) using an incorrect password to see if the system responds with an error message stating an incorrect password has been entered or denies access after exceeding the maximum threshold for logon attempts.

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.

Subtask 8: System Testing

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The system shall be independently reviewed, verified, and validated using the system's security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all system security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended. Once testing has been completed, the ST&E Report, the Vulnerability Assessment Report, and the Corrective Action Plan shall be developed to document the results of the system's testing. Finally, the ST&E Plan is updated to reflect validated information.

Subtask 9: System CP

The Contractor shall support the NRC staff in the development and documentation of a CP and test procedures within the Rational Suite Enterprise. The System CP shall be documented in a report generated from the Rational Suite Enterprise that follows the NRC Template for the System CP. The Plan shall be maintained in its hard copy form for contingency execution should the Rational Suite Enterprise or NRC Network Infrastructure be unavailable.

The CP shall be developed in accordance with federally mandated requirements, NRC defined security requirements, National Institute of Standards & Technology (NIST) Special Publication (SP) 800-34

“Contingency Planning Guide for Information Technology Systems”, NIST SP 800-37 “Guide for the Security Certification & Accreditation of Federal Information Systems”, and the NRC Contingency Plan (CP) Template.

The Contractor shall provide detailed procedures for the Notification/Activation Phase, Recovery Operations, and Return to Normal Operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system CP shall contain

- Sufficient contact information (personnel and vendor)
- Equipment (hardware and software)
- Specification information to enable reconstitution of the system from scratch, all service level agreements, memoranda of understanding
- IT standard operating procedures for the system
- Identification of any systems that this system is dependent upon along with references for the applicable contingency plans
- References to the emergency management plan and occupant evacuation plan
- References to the appropriate continuity of operations plan.

The System CP shall be documented in a report generated from the Rational Suite Enterprise that follows the NRC Template for System CP. The report shall be delivered in draft form and then in pre-Test form after NRC comments have been incorporated. The NRC CSO staff review of the draft is required to ensure compliance.

Subtask 10: Contingency Test and Report

The Contractor shall provide expert advice and support during the Contingency Planning Test to ensure the test plan documentation is compliant with the System CP that has been approved by the NRC. Testing shall follow the test procedures developed and documented by the Contractor within the Rational Suite Enterprise. The Contractor shall document the testing in a System Contingency Test Report (CP Test Report). The CP Test Report shall be developed in accordance with federally mandated requirements, NRC defined security requirements, NIST SP 800-34 “Contingency Planning Guide for Information Technology Systems”, NIST SP 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems”, and the NRC Contingency Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for NRC Contingency Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC must approve the final CP Test Report.

The Contractor shall update the system’s CP once the CP Test Report has been completed to reflect validated information. The NRC must approve the final version of the system’s CP.

Subtask 11: ATO Package

The contractor shall perform this task as identified in the table found in section 3 “Scope of Work”.

The ATO package documents the results of the system certification and provides the authorizing official with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

The ATO Package contains the following deliverables plus a corresponding CD that contains all supporting documentation: Security Categorization Document, SRA, SSP, ST&E Plan, ST&E Report, Vulnerability Assessment Report, Corrective Action Plan, and an Approval to Operate Request Memo.

All documentation must be provided to the CSO in both hard copy and electronically in MS Word. The SSP must be current (within 2 months). The SRA, ST&E Plan, ST&E Report, and VAR must be current (within 2 months).

8.0 TRAVEL

The following travel is required to support this effort:

- DDS – Shall not exceed \$7,500.00.

9.0 MEETINGS

At the request of the NRC, the contractor's technical representative shall attend monthly status meetings at NRC Headquarters to discuss work being done under this task order.