

U.S. Nuclear Regulatory Commission
Privacy Impact Assessment
for the
Automated Acquisition Management System (AAMS)

Date: February 26, 2007

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

The AAMS is a procurement document writing system. It is a highly-configurable web-based commercial-off-the-shelf (COTS) product acquired from Distributed Solutions, Inc.(DSI). The AAMS is a suite of products targeted at the federal procurement professional.

2. What agency function does it support?

Supports the Division of Contracts (DC) function to develop and implement agency-wide contracting policies and procedures; direct and coordinate contracting, simplified acquisition, grant and financial assistance activities; provide advice and assistance to NRC program officials regarding procurement regulations, requirements, and methods for meeting program objectives consistent with such regulations; provide oversight for regional procurement activities; and develop and administer agency guidance for contracting activities with the Department of Energy laboratories and other government agencies for a wide variety of goods and services on a competitive and non-competitive basis.

3. Describe any modules or subsystems, where relevant, and their functions.

ProTrac - procurement process tracking and management
ProFund – fund tracking and management
ProDoc – procurement document generation
Web RegSearch – regulatory reference database for procurement actions

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Mona Selden	ADM/DC/PPT	415-7907
Business Project Manager	Office/Division/Branch	Telephone

Mary Lynn Scott	ADM/DC/DO	415-6172
Technical Project Manager	Office/Division/Branch	Telephone
Mary Denney	ADM/DO/PMDA	415-6598
Executive Sponsor	Office/Division/Branch	Telephone
Timothy F. Hagan	ADM/DO	415-6222

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. New System Modify Existing System Other (Explain)

Updating Security Documentation.

b. If modifying an existing system, has a PIA been prepared before?

Yes.

(1) If yes, provide the date approved and ADAMS accession number.

Approved 4/26/2004 - ADAMS ML070720307

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system collect information about individuals?

Yes.

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

Federal contractors (vendors) and Federal employees (NRC acquisition officials)

b. What information is being maintained in the system about individuals (describe in detail)?

NRC Acquisition Officials: DC point of contact name, position title, work phone number, User id; project officer name.

Vendor (if vendor is an individual): name, address, social security number.

- c. Is the information being collected from the subject individuals?

The information about the DC point of contact is entered into the AAMS by that individual.

- (1) If yes, what information is being collected from the individuals?

Name, user id, work phone number, position title.

- d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

No.

- (1) If yes, does the information collection have OMB approval?

(a) If yes, indicate the OMB approval number:

- e. Is the information being collected from internal files, databases, or systems?

The name of the NRC project officer is pulled from the "Request for Procurement Action (RFPA)."

- (1) If yes, identify the files/databases/systems and the information being collected.

- f. Is the information being collected from an external sources(s)?

Yes.

- (1) If yes, what is the source(s) and what type of information is being collected?

Vendor information (name, address, TIN/SSN) comes from the *Central Contractor Registration (CCR) (www.ccr.gov).

*CCR is the primary vendor database for the U.S. Federal Government. The CCR collects, validates, stores and disseminates data in support of agency acquisition missions.

Both current and potential government vendors are required to register in CCR in order to do be awarded contracts by the government. Vendors are required to complete a one-time registration to provide basic information relevant to procurement and financial transactions. Vendors must update or renew their registration annually to maintain an active status. CCR electronically shares the secure and encrypted data with the federal agencies' finance offices to facilitate paperless payments through electronic funds transfer (EFT).

- g. How will this information be verified as current, accurate, and complete?

CCR pre-populates the following data fields from Dun & Bradstreet (D&B): Legal Business Name, Doing Business Name (DBA), Physical Address, Postal Code/ Zip+4. It is data that is originally entered by the registrant when they applied for a Data Universal Numbering System (D-U-N-S).

When information needs to be changed or updated the registrant can modify the information. After the registrant makes the desired changes, D&B confirms the changes made with the registrants record. The registrant then goes to www.ccr.gov and clicks on Update/Renew, checks the data, and accepts the modified information if it is correct.

- h. How will the information be collected (e.g. form, data transfer)?

Data transfer.

- i. What legal authority authorizes the collection of this information?

Federal Acquisition Regulation (FAR) Parts 4, 9, 12, 13, 15, 36 and 42.

- j. What is the purpose for collecting this information?

To create procurement documents such as contracts, solicitations, etc. Prepare required reporting of data/information from agency acquisition/procurement records to the Federal Procurement Data System-Next Generation (FPDS-NG). To provide information to other Federal agencies for audits and reviews.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

- a. What type of information will be maintained in this system (describe in detail)?

Vendor (business) name, address, tax identification number (TIN); action type, title, status; NRC contractor number; award costs (estimate, commitment, obligated, etc); award date; estimated completion date; NRC program office; DUNS number; agency ID, agency code, etc.

- b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Information about the vendor (name, address, TIN) will be retrieved from the Central Contractor Registration database (external source) through data transfer.

The remaining data will be entered from internal agency generated information.

- c. What is the purpose for collecting this information?

To create procurement documents such as contracts, solicitations, etc. Prepare required reporting of data/information from agency acquisition/procurement records to the Federal Procurement Data System-Next Generation (FPDS-NG). To provide information to other Federal agencies for audits and reviews.

C. USES OF SYSTEM AND INFORMATION

(These questions will identify the use of the information and the accuracy of the data being used.)

1. Describe all uses made of the information.

The data is used for required agency reporting and to provide information to other Federal agencies for audits and reviews. Information is also used to respond to internal requests relating to management, budget, workload, document generation, etc.

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the information?

System administrator and agency contract specialists.

4. Are the data elements described in detail and documented?

Yes.

- a. If yes, what is the name of the document that contains this information and where is it located?

Data elements are described in Federal Acquisition Regulation (FAR) Parts 4, 9, 12, 13, 15, 36 and 42.

- 5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

- a. If yes, how will aggregated data be maintained, filed, and utilized?
- b. How will aggregated data be validated for relevance and accuracy?
- c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

- 6. How will the information be *retrieved* from the system (be specific)?

Data will be retrieved by requesting one of the standard reports. Also data can be retrieved from the "Look-Up tab" by action type, assist number, solicitation number, BPA number, contract number, delivery order number, funding action, interagency agreement, planning action, purchase order number, and contractor/vendor name. Additional queries can be performed by the system administrator using any field of data in system.

- 7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No.

- a. If yes, explain.
 - (1) What controls will be used to prevent unauthorized monitoring?

- 8. Describe the report(s) that will be produced from this system.

Reports and queries are controlled by user access levels and include:

Action Detail
Unlinked Funding Actions
Upcoming Milestones
FPDS-NG Report

Small Business Statistics

Milestone Report - which include Projected Planning and Milestone Plan Summary Report

Other Reports - which include Action Summary, Action Status, Acquisition Management Report, Pre Award Summary, Competition in Contracting, List of Active Contracts, Direct 8A Summary and Standard Address

ESA Reports - which include ADMIN Report, Desktop Access Report, User Account Status Report and Workgroup Report

a. What are the reports used for?

Manage NRC commercial acquisitions and required agency reporting.

b. Who has access to these reports?

Acquisition officials and system administrators based on roles and responsibilities.

D. RECORDS RETENTION AND DISPOSAL

(These questions are intended to establish whether the information contained in this system has been scheduled, or if a determination has been made that a general record schedule can be applied to the information contained in this system. Reference NUREG-0910, "NRC Comprehensive Records Disposition Schedule.")

1. Has a retention schedule for this system been approved by the National Archives and Records Administration (NARA)?

a. If yes, list the disposition schedule.

2. Is there a General Records Schedule (GRS) that applies to information in this system?

Yes.

a. If yes, list the disposition schedule.

Records for transactions of more than \$100,000 are destroyed 6 years and 3 months after final payment, in accordance with GRS 3-3.a(1)(a). Transactions of \$100,000 or less are destroyed after 3 years after final payment in accordance with GRS 3-3.a(1)(b).

3. If unscheduled, what are your retention requirements for the information maintained in this system? How long must the material be maintained to meet your programmatic needs?

E. ACCESS TO DATA

1. INTERNAL ACCESS

- a. What organizations (offices) will have access to the information in the system?

Agencywide acquisition officials (e.g., Contracting Officer, Contract Specialist, Project Officer, Program Manager, Technical Assistants).

- (1) For what purpose?

Contract management responsibilities.

- (2) Will access be limited?

Yes. Access is limited by roles and responsibilities.

- b. Will other systems share or have access to information in the system?

No.

- c. How will information be transmitted or disclosed?

- d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

The data will be password protected and audit trails will be maintained.

- e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes.

- (1) If yes, where?

The access criteria, procedures, controls and responsibilities are documented by the contractor.

2. EXTERNAL ACCESS

- a. Will external agencies/organizations/public share or have access to the information in this system?

No. Information from the system is provided to external agencies, but no external agency has electronic or password access to this system.

(1) If yes, who.

- b. What information will be shared/disclosed and for what purpose?

- c. How will this information be transmitted/disclosed?

F. TECHNICAL ACCESS AND SECURITY

- 1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

Passwords. Access authorization will limited to roles and responsibilities.

- 2. Will the system be accessed or operated at more than one location (site)?

Yes.

- a. If yes, how will consistent use be maintained at all sites?

Access will be limited to need to perform specific duties.

- 3. Which user group(s) (e.g., system administrators, project manager, etc.) have access to the system?

System administrators, project manager, contractor technical staff.

- 4. Will a record of their access to the system be captured?

Yes.

- a. If yes, what will be collected?

Audit trails collect user id and date/time created/updated.

- 5. Will contractors have access to the system?

Yes.

- a. If yes, for what purpose?

Contractors will have access to the data for input purposes and to generate reports.

- Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:

- 52.224-1 Privacy Act Notification.

- 52.224-2 Privacy Act.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

The data will be password protected and audit trails will be maintained in this system.

7. Are the data secured in accordance with FISMA requirements?

Yes.

- a. If yes, when was Certification and Accreditation last completed?

April 23, 2004. Memo signed by Charlotte Turner on May 4, 2004.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/IRSD/RFPSB Staff)

System Name: Automated Acquisition Management System (AAMS)

Submitting Office: Office of Administration (ADM)

A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

Privacy Act is applicable. Currently covered under System of Records, NRC- . Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

Comments:

Currently covered under NRC's Privacy Act system of records, NRC-5, "Contracts Records Files." No modification to the system notice is required.

This system does contain PII (name, address, and SSN if vendor is an individual).

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	June 13, 2007

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. _____

Comments:

The AAMS procurement document writing system assists the Division of Contracts (DC) in the development and implementation of agency-wide contracting policies and procedures. The system's information will be collected from less than 10 individuals who are not Federal

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: Timothy F. Hagan, Director, Office of Administration	
Name of System: Automated Acquisition Management System (AAMS)	
Date RFPSB received PIA for review: May 30, 2007	Date RFPSB completed PIA review: June 19, 2007
<p>Noted Issues:</p> <p>Covered under NRC's Privacy Act system of records, NRC-5, "Contracts Records Files." No modification to the system notice is required.</p> <p>Records for transactions of more than \$100,000 are destroyed 6 years and 3 months after final payment, in accordance with GRS 3-3.a(1)(a). Records of transactions of \$100,000 or less are destroyed after 3 years after final payment in accordance with GRS 3-3.a(1)(b).</p>	
Margaret A. Janney, Chief Records and FOIA/Privacy Services Branch Office of Information Services	Signature/Date: /RA/ 06/19/2007
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>James C. Corbett, Director Business Process Improvement and Applications Division Office of Information Services</i></p> <p><i>Kathy L. Lyons-Burke, CISSP Senior IT Security Officer (SITSO)/Chief Information Security Officer (CISO) Office of Information Services</i></p>	