ADAMS ML12244A508

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

NRC Strategic Acquisition System (STAQS)

Date: September 12, 2012

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

   STAQS is NRC's proposed Strategic Acquisition system. The chosen solution is a Commercial off the Shelf (COTS) application that will be integrated into the Agency's FAIMIS (Financial Accounting and Integrated Management Information System) Core Financial System (CFS).

2. What agency function does it support?

   STAQS will enforce standard processes and procedures involved in acquisition activities, establish automated end-to-end workflow, and through integration with the agency's core financial system allow for the reconciliation and consistency of reporting of agency spending. The acquisition system will assure transparency in process flow; increase staff accountability; reduce redundancy; ensure compliance with Federal acquisition regulations/requirements; streamline individual touch points; and allow for "real time" reporting of all agency procurement transactions and result in enhanced visibility and standardization of the agency's entire acquisition workload.

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

   There are no modules or subsystems envisioned in the system at this time.

4. What legal authority authorizes the purchase or development of this system?

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

5. What is the purpose of the system and the data to be collected?

To create procurement documents such as contracts, solicitations, etc; to 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.

6. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
Ron Deavers	FAIMIS Acquisition Technical and Project Engineering Branch	301-415-7301
Business Project Manager	**Office/Division/Branch**	**Telephone**
James Corbett	Division of Contracts	301-415-3600
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Ray Crouse	Systems Development Branch	301-415-5276
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Cynthia Carpenter	Office of Administration	301-492-3500

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. **X** New System ___ Modify Existing System ____ Other (Explain)

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

N/A

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

N/A

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 maintain information about individuals?

Yes

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).

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

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific)?

NRC Acquisition Officials: Division of Contracts (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 or EIN number.

c. Is information being collected from the subject individual?

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

Vendor information (including name, address, Social Security Number (SSN) / Employer Identification Number (EIN)) is not collected directly from the vendor. Information about vendors, including information pertaining to individual vendors, is pulled from the Central Contractor Registration (CCR) database. As detailed elsewhere in the STAQS PIA document, 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.

(1) If yes, what information is being collected?

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 – vendor information is not collected from individuals. Vendor information, including that on individual vendors is pulled from CCR.

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

N/A

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

N/A

e. Is the information being collected from existing NRC files, databases, or systems?

Yes, but not for vendor information, including that on individual vendors, is pulled from CCR, and not from existing NRC files.

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

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

f. Is the information being collected from external sources (any source outside of the NRC)?

Yes

(1) If yes, identify the source 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 information not collected directly from the subject individual 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 (DU-N-S) number.

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 registrant's 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

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. Will information not about individuals be maintained in this system?

Yes

(1) If yes, identify the type of information (be specific).

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. 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 data in this system.

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 data both relevant and necessary for the purpose for which the system is designed?

   Yes

3. Who will ensure the proper use of the data in this system?

   System Administrators and agency contract specialists will ensure proper use of data in the system.

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 that 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?
      N/A

   b. How will aggregated data be validated for relevance and accuracy?
      N/A

   c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?
      N/A

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier? (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, Inter-agency agreement, planning action, purchase order number, and contractor/vendor ID. Additional queries can be performed by the system administrator using any field of data in system.

   The STAQS implementation user interface does not retrieve data by data fields that store an individual's name or personal identifier. The system will retrieve data based on the user who is logged into the system in a manner similar to an email inbox – in the form of a list of all the work items assigned to the user of the system. However, a

user cannot "see" work items assigned to another user.

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

   No

   a. If yes, explain.

      N/A

      (1) What controls will be used to prevent unauthorized monitoring?

         N/A

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

   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 - including 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. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

   Agency wide acquisition officials (e.g., Contracting Officer, Contract Specialist, Project Officer, Program Manager, and Technical Assistants) will have access to data in the system.

   (1) For what purpose?

Offices will have access to information in the system to fulfill Contract management responsibilities.

(2) Will access be limited?

Yes. Access is limited by roles and responsibilities.

2. Will other NRC systems share data with or have access to the data in the system?

Yes

(1) If yes, identify the system(s).

FAIMIS CFS, CRISP Data warehouse. CRISP Data warehouse is a database in OIS/ICOD's shared 3-tier MSSQL environment. CRISP is not part of FAIMIS.

(2) How will the data be transmitted or disclosed?

Service Oriented Architecture based data exchange.

3. Will external agencies/organizations/public have access to the data in the 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?

N/A

(2) Will access be limited?

External agencies / organizations / public have no access to data in the system. All access to data is password protected and restricted to Agency wide (NRC) acquisition officials.

(3) What data will be accessible and for what purpose/use?

Data in the system will not be accessible to external agencies / organizations / public. Required data/information from agency acquisition / procurement records will be provided to various Federal Web Sites such as Federal Procurement Data System (FPDS), FedConnect, Grants.gov etc.

(4) How will the data be transmitted or disclosed?

NRC may send information to external Federal websites such as Federal Procurement Data System (FPDS), FedConnect, and

Grants.gov. However, external agencies / organizations / public have no access to data in the system.

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in NUREG-0910, or the General Records Schedules at http://www.archives.gov/records-mgmt/grs ?

   Yes

   a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?

      GRS 3-3.a (1) (a) – Disposition: Destroy 6 years and 3 months after final payment.
      GRS 3-3.a (1) (b) – Disposition: Destroy after 3 years after final payment.

   b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

   N/A

3. Would these records be of value to another organization or entity at some point in time? Please explain.

   N/A

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

   N/A

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

   N/A

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

   N/A

7. Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?

   N/A

F. TECHNICAL ACCESS AND SECURITY

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

   Passwords will be used as security controls to limit access to the system. Access authorization will limited to roles and responsibilities.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

   System data will be password protected and audit trails will be maintained. Access authorization limited to roles and responsibilities will prevent misuse of system data by users in the system.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

   Yes

   (1) If yes, where?

   Details of access authorization in the STAQS application are laid out in the STAQS System Security Plan. It is still under development by the Implementation Contractor and will be submitted to review by the Agency's Chief Security Officer when it is ready.

4. 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.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

   User groups with the ability to access the system include - System

Administrators, project manager, and contractor technical staff.

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

   Yes

   a. If yes, what will be collected?

      Audit trails will collect information including – User ID, Data and Time created / updated.

7. Will contractors be involved with the design, development, or maintenance of the system?

   Yes

   If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

   - *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
   - *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

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

   Data in the system will be password protected and audit trails will be maintained in the system.

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

   Yes

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

      Certification and Accreditation for the system is still in process.

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

System Name: NRC Strategic Acquisition System (STAQS)

Submitting Office: Office of Administration

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

_X_ Privacy Act is applicable.

Comments:
This system does contain PII (name, address, and SSN if vendor is an individual). Covered under NRC's Privacy Act system of records, NRC-5 - Contracts Records Files. This system is replacing Automated Acquisition Management System (AAMS).

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Act Program Analyst	September 25, 2012

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

_X_ No OMB clearance is needed.

___ OMB clearance is needed.

___ Currently has OMB Clearance. Clearance No._____

Comments:
The new NRC Strategic Acquisition System assists the Division of Contracts in the development and implementation of agency-wide contracting policies and acquisition procedures. The system's information will be collected directly from the GSA system that collects information from vendors. NRC is not directly asking for information from vendors. No OMB clearance is needed for this system.

Reviewer's Name	Title	Date
Tremaine Donnell	Team Leader, Information Collections Team	September 24, 2012

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:
The records in the STAQS are covered under NARA approved GRS 3, Routine Procurement Files, as follows:

Item 3.a.(1)(a). Transactions that exceed the simplified acquisition threshold and all construction contracts exceeding $2,000.
Disposition: Destroy 6 years and 3 months after final payment; and
Item 3.a.(1)(b). Transactions at or below the simplified acquisition threshold and all construction contracts at or below $2,000.
Disposition: Destroy 3 years after final payment.

No modifications to the retention schedule are needed; however, adherence to the retention schedule is mandatory under 44 U.S.C. 3303a(d). Retention functionality or a manual process must be developed to meet this requirement. A recommended approach is to develop minimal record related fields in the system to enable retention. This may be accomplished by including a termination date for the records in order to delete or destroy the information as required.

Reviewer's Name	Title	Date
Mary Haynes	Records Management Analyst	September 20, 2012

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date **09/26/2012**

Russell A. Nichols, Chief
Information Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Cynthia Carpenter, Director, Office of Administration**	
Name of System: **NRC Strategic Acquisition System (STAQS)**	
Date IRSD received PIA for review: **September 14, 2012**	Date IRSD completed PIA review: **September 25, 2012**
Noted Issues: Currently covered under NRC's Privacy Act system of records, NRC-5, "Contracts Records Files." This system is replacing Automated Acquisition Management System (AAMS).	
Russell A. Nichols, Chief Information Services Branch Information and Records Services Division Office of Information Services	Signature/Date: **/RA/ 09/26/2012**
Copies of this PIA will be provided to: *Susan Daniel, Director(Acting)* *Business Process Improvement and Applications Division* *Office of Information Services* *Paul Ricketts,* *Senior IT Security Officer (SITSO)* *FISMA Compliance and Oversight Team* *Computer Security Office*	