Privacy Threshold Analysis Template
(To be used to determine whether a privacy impact assessment is required in accordance with the E-Government Act of 2002.)

Date submitted for review: February 24, 2021

Name of Project/System: Strategic Acquisition System (STAQS)

Sponsoring Office: Office of Administration (ADM)

Project manager name and phone number:

Leah Kube (301) 415 0669

1. Describe (in detail) the project/system and its purpose:

The Strategic Acquisition System (STAQS) is U.S. Nuclear Regulatory Commission (NRC's) automated acquisition system and is owned by the Office of Administration (ADM). STAQS is Unison's PRISM software which supports the agency's acquisition activities and management functions. STAQS interfaces with the agency's core Financial Accounting and Integrated Management Information System to process commitments and obligations. The system also interfaces with the General Services Administration (GSA's) Integrated Award Environment (IAE) systems, Unison's FedConnect system, and Health and Human Services (HHS) Grants.gov.

STAQS is Commercial off the Shelf application offered by Unison as a Software as a Service (SaaS) cloud service, implemented and hosted within the Amazon Web Services (AWS) East/West Infrastructure as a Service. The STAQS Unison SaaS infrastructure is composed of virtual servers that reside in AWS East and West. The boundary is the Virtual Private Gateway that leads to the STAQS virtual private clouds (VPC), one VPC encompassing the web servers and one VPC encompassing the database servers. There are four environments in AWS East and one environment in AWS West. The production environments, Quality Assurance, User Acceptance Testing and Post-production environments are located in AWS East. The disaster recovery environment is located in AWS West.

2. What agency function does it support:

STAQS supports the following agency's functions –

- Provides automated life-cycle procurement execution activities including advanced planning, requisitioning, contract solicitation, awards (including interagency agreements), close outs, and funding opportunities (including evaluation)
- Supports commitments and obligations (creates/modifies/closes requisitions and awards) operations
- Provides end-to-end contract functionality and automatically posts opportunities and other contract related announcements on beta.sam.gov (previously FedBizOpps) managed by GSA; STAQS also submits award data required for Federal Procurement Data System Next Generation
- Standardizes processes and procedures involved in acquisition activities and integrates with the agency's core financial system
- Provides end-to-end assistance agreements functionality (prepare, issue, administer and closeout functions for assistance/cooperative agreements)
- Facilitates end-to-end reporting by capturing critical data for internal and external reporting requirements; allows for real time reporting of all agency procurement transactions
- Ensures compliance with Federal acquisition regulations/requirements.

3. Status:

____ New development effort.

__X__ Existing system.

- **Date system first developed**: The STAQS system is currently operational. The STAQS was given its authority to operate in September 2013.

- **Date Privacy Threshold Analysis (PTA) last updated**: January 7, 2020.

- **Provide the Agencywide Documents Access and Management System (ADAMS) accession number**:

  STAQS Privacy Threshold Analysis ML20007C460.

- **Provide a general description of the update**:

  The STAQS system is in the operations and maintenance phase which includes the ongoing day-to-day use (production), and routine maintenance or enhancements such as routine patching, software upgrades such as applying service packs and implementing change requests to support the agency's acquisition management business needs.

4. **Do you have a U.S. Nuclear Regulatory Commission (NRC) Enterprise Architecture (EA)/Inventory number?**

   Yes.

   1. **If yes, please provide EA/Inventory number.**

      EA# - 20120005.

   2. **If no, please contact EA Service Desk to get EA/Inventory number.**

5. **Could the project/system relate in any way to individuals?**

   ____ No

   _X_ Yes

   - Provide a general description of the way the project could relate to an individual.
   - Federal contractors (Vendors) and Federal employees (NRC Acquisition Officials) business contact information only.

6. **Does this project collect, process, or retain information on: (Check all that apply)**

   _X_ NRC employees?

   ____ Other Federal employees?

   _X_ Contractors working on behalf of NRC?

   ____ Members of the public or "other individuals"?

   ____ System does not contain any such information.

7. **Does this project use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs, such as the "last four.")**

   _X_ No

   ____ Yes

   - **Why is the SSN collected or used? Provide the function of the SSN and the legal authority to do so.**

     N/A.

   - **Is the SSN full or partial SSN?**

     N/A.

8. What information about an individual could be collected, generated or retained? Provide a detailed description of the information that might be collected, generated, or retained such as names, addresses, phone numbers, etc.

STAQS does not collect, generate or retain any Personally Identifiable Information (PII).

STAQS databases include the following information.

NRC Acquisition Officials - Name, Position, and Title, Business Work Telephone Number, Business User ID, and Name of project officer.

Vendor - Name, Business Address, and Dun & Bradstreet Number (DUNS).

The information about the NRC Acquisition Officials is entered into the STAQS system by the individual.

STAQS does not directly collect vendor information (including name, address, and DUNS). This information is imported into STAQS from the System of Award Management (SAM), which is a subsystem of the GSA IAE. The SAM database is the primary vendor database for the U.S. Federal Government. Its use is federally mandated by GSA. SAM is used by anyone interested in conducting business with the Federal Government, including:

- Entities who need to register to do business with the government, look for opportunities or assistance programs, or report subcontract information;
- Government contracting and grants officials responsible for activities with contracts, grants, past performance reporting and suspension and debarment activities;
- Public users searching for government business information.

The SAM database collects, validates, stores, and disseminates vendors' data in support of agency's acquisition missions.

NOTE: **NRC does not have the "sensitive" account in SAM necessary to pull the Tax Identification Number (TIN) or SSN or any other PII into STAQS when adding or updating a vendor. The STAQS Information System Security Officer has verified that none of the STAQS databases include any kind of PII information such as SSN, TIN, etc.**

9. Does the system share personally identifiable information with any other NRC systems?

_X_ No

____ Yes

- Identify the systems:

  N/A.

10. Does this system relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?

____ No

__X__ Yes

STAQS relies on the NRC WAN for Operations. The NRC application users use their Personal Identity Verification (PIV) cards to access the STAQS application in the Unison contracting SaaS AWS cloud environment using a web browser via an NRC workstation or Citrix broadband remote desktop. Communication between the NRC network and the STAQS web application on the Unison AWS environment is protected via Transport Layer Security 1.2 encryption over HTTPS. The NRC users use the Office of the Chief Information Officer (OCIO) Information Technology Infrastructure (ITI) Identity, Credential, and Access Management (ICAM) Gateway / Security Assertion Markup Language (SAML) Single Sign-on (SSO) authentication to access the STAQS application.

The STAQS users' access is enforced by requiring the user to be connected to the NRC Network. The STAQS user profile contains the user's NRC LAN ID and network domain (SSO via SAML assertion). Additionally, the account associated with the user ID is configured for specific roles & privileges assigned by the STAQS application administrator. If an attempt is made to create an account with a user ID that already exists in the system, the STAQS application presents an error and prompt the Administrator to create a different user ID.

- **If yes, is there a log kept of communication traffic?**

  Yes.

- **If yes, what type of data is recorded in the log? List the data elements in the log.**

  The OCIO Security Operations Center maintains logs of all communications traffic. LAN ID and date/time stamp.

11. Can the system be accessed remotely?

____ No

__X__ Yes

- **If yes, how?**

In regard to the front-end application, STAQS supports multi-factor authentication in the form of NRC ITI ICAM provided single-sign-on from PIV credentials using SAML assertions. Network based two factor authentications to network resources are provided by the NRC ITI ICAM, as the STAQS application users (non-privileged users) access the system through the NRC LAN network.

STAQS in the Unison hosting environment implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access. Unison implements multifactor authentication through the use of an RSA system. The first factor is the user account credentials (something the user knows), and the second factor is the RSA server, which provides the user with the one-time pseudo random number generator (something that you have). The RSA server providing the one-time passcode / token resides on a separate server on a separate network in a separate facility (within Unison Shared Services at Ashburn, VA).

12. Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or the National Archives and Records Administration's (NARA's) General Records Schedules (GRS)?

__X__ Yes

- **If yes, please provide the schedule number, approved disposition, and describe how this is accomplished.**

GRS 1.1-010. Agency's Acquisition Management Data:

Disposition: Temporary: Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

Suggested retention based on the statement that this system is in Operation & Maintenance (O&M):

GRS 3.1-020 Information Technology Operations and Maintenance Record:

Temporary. Destroy 3 years after agreement control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

____ No

- **If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov.**

13. What FISMA system is this part of?

STAQS is NRC's independent Federal Information Security Modernization Act (FISMA) reportable system operating in the Unison FedRAMP authorization boundary.

14. Is there an Authority to Operate record (ATO)?

____ Unknown

____ No

- **If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.**

____ In progress

__X__ Yes: **Indicate the impact levels approved by the Computer Security Organization for the following:**

ATO the Strategic Acquisition System (STAQS) - ML13200A096

ADM STAQS Unison Contracting SaaS Authorization (ML20288A560)

Confidentiality:	____	Low	__X__	Moderate	____	High	____	Undefined
Integrity:	____	Low	__X__	Moderate	____	High	____	Undefined
Availability:	____	Low	__X__	Moderate	____	High	____	Undefined

PRIVACY THRESHOLD ANALYSIS REVIEW

(To be completed by: Cyber Security Branch, Governance and Enterprise Management Services Division, Office of the Chief Information Officer)

System Name: Strategic Acquisition System (STAQS)

Date reviewed: March 25, 2021

Name of the reviewer: Sally A. Hardy, Privacy Officer

__X__ No, this is NOT a privacy sensitive system – the system contains no personally identifiable information.

____ Yes, this IS a privacy sensitive system. A privacy impact assessment is required.

COMMENTS:

STAQS only includes business related information.

I concur with this analysis:

Signed by Nalabandian, Garo
on 03/25/21

Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer