Federal Trade Commission
Privacy Impact Assessment

AcquTrak

February 2017

PIA Template Version 1.3 – May 2016

Table of Contents

1 System Overview 1
2 Data Type, Sources, and Use 2
3 Data Access and Sharing 4
4 Notice and Consent 5
5 Data Accuracy and Security 7
6 Data Retention and Disposal 9
7 Website Privacy Evaluation 9
8 Privacy Risks and Evaluation 9
9 Approval and Signature Page 12

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) Financial Management Office (FMO) and Office of the Chief Information Office (OCIO) use AcquTrak, an acquisition collaboration and source selection tool, to manage the large amounts of documentation received and processed as part of the contract acquisition process.

AcquTrak is a third party web-based software application owned by Noblis. AcquTrak serves as a repository for acquisition-related information including Request for Proposals (RFP) and any amendments to an RFP. The system also is used to maintain any inquiries from interested vendors as well as the accompanying responses provided by the FTC. Vendor proposals and revisions, the Acquisition Plan and Source Selection Plans, and the FTC's evaluation and review documentation also are maintained in the system.

FMO and OCIO will maintain all documentation associated with the receipt and evaluation of proposals and award of task orders, BPAs, or other contract actions within the AcquTrak system for FTC acquisitions matters in which the system will be used to manage the procurement process. This includes audit information, such as the date and time the document was created, as well as the author(s) of the document. As the documents undergo review, each modification, the date and time that it occurred, and the name of the modifier is added to the system audit trail.

For the purposes of this PIA, AcquTrak users will be FTC staff in FMO and OCIO whose responsibilities include reviewing and evaluating proposals and recommending or authorizing awards or other contract actions, as described earlier.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

Collection of this information is permitted by and consistent with the FTC's inherent authority under the FTC Act, 15 U.S.C. 41 et seq., to enter into contracts, and the provisions of the Federal Acquisition Regulation (FAR), 48 CFR ch. 1, specifying the procedures to be followed by Federal agencies when procuring goods or services and, where applicable, specifying the records or information to be provided to or collected by the Government in connection with the acquisitions process under applicable law, regulation or Government-wide policy (e.g., representations and certifications). Taxpayer identification numbers are collected from all individuals and entities doing business with the Government as required by 31 U.S.C. 7701.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Public key from PIV badge
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☒ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

The information maintained in AcquTrak is generally only Business Contact Information, defined as an individual vendor's name, work email, work phone number, and work address. This information usually is public in nature and easily available on company business cards. Along with their proposals, vendors may submit resumes, which may include the individual's education history, employment history and applicable certifications, and military history or status. Typically, the resumes contain only the individual's business address, although it is possible that personal home addresses may be included as well. In general, the personal information contained in AcquTrak will be limited to Business Contact Information, except in the limited circumstances where the FTC requests additional information from the vendor and/or the vendor chooses to submit extra information in response to the FTC's Request for Quote (RFQ). The amount of PII maintained within the AcquTrak system is minimal and typically public in nature.

In order to request access to the AcquTrak system, FTC Contracting Officers (CO) provide the following data elements to Noblis via mail: names of authorized FTC employees serving as bid evaluators, their work phone numbers, e-mail addresses, and roles/access rights. Once they have been granted access, authorized FTC staff use the AcquTrak web application to register their user accounts by providing their names, email addresses, and phone number, as well as their Personal Identity Verification (PIV) card for account validation.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

Source selection information will be maintained in the system. This refers to cost estimates and price quotes provided by the vendors, as well as technical and management details provided in response to the FTC's Request For Quote (RFQ).

When an FTC evaluator reviews a set of vendor documents in AcquTrak, the evaluator's progress and evaluation records will be stored in the system. This includes the evaluator's comments on each offeror's proposal based on their assigned role on the technical evaluation team.

Additional audit information captured by the system includes log files associated with the creation and access of files, including the date and time a document was created, reviewed, or modified by a user. This includes the name of the author or individual who modified the document.

2.3 What is the purpose for collection of the information listed above?

The purpose of collection of information in AcquTrak is to facilitate the FTC's ability to manage large amounts of documentation received and processed as part of the contract acquisition process. This information collection allows the agency to evaluate offers, select vendors, and complete acquisition activities. Evaluation records are maintained to enable FTC acquisition managers to track progress and evaluation comments. The audit information collected by the system enables technical and security staff to analyze and monitor access to the system.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
Vendors	The FTC posts requests for contract services on the General Service Administration (GSA) eBuy[2] website, and in response, vendors submit proposals to the FTC via eBuy. The submission materials will generally include company information, service details, and quotes or estimates for services offered.
FTC Staff	When vendors submit proposals on eBuy in response to an FTC RFP, FTC contracting officers access the website to download the information and transfer the proposals to Noblis via encrypted email. Noblis is responsible for uploading the proposals into AcquTrak. While reviewing and evaluating vendor bids, FTC staff will enter their comments and notes directly into the AcquTrak system.

[2] eBuy is an electronic system owned by the General Services Administration (GSA) to allow government buyers to request information, find sources, and prepare RFQs and Requests for Proposal (RFPs) online, for products and services and large quantity purchases.

	FTC COs provide the PII described in Section 2.1 in order to request access to the AcquTrak system.
Noblis Staff	Noblis staff receive vendor proposals from FTC COs for uploading into the AcquTrak system. Noblis staff do not make any changes or edits to the information and directly upload all information to AcquTrak. Noblis staff receive PII from FTC COs, as described above, to create user accounts for these individuals, issue login credentials, and grant access privileges to the AcquTrak system.
AcquTrak	The system captures in log files information related to record management, including the timestamp of new records or changes, user name (author or modifier).

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
FTC Staff	FTC users have read-only privileges to submission data. FTC users have the ability to enter and edit evaluation records to which they are granted access. Data is accessed for the purpose of reviewing and evaluating proposals. Evaluation comments and documentation may be shared with other authorized FTC users based on access privileges.
Noblis Staff	Noblis AcquTrak system administrators, developers and support staff access AcquTrak to upload proposals to the system. Noblis staff do not edit or change the data in any way before directly uploading to AcquTrak. Noblis staff also create user accounts for FTC employees and set up evaluation groups with specific permissions and privileges. In addition, administrators may be required to verify and create or update registrations. System administrators access submission data in order to load, index the data, and export or delete data as requested by the FTC. Developers, Local Domain Administrators, and Local Domain Servers have manager rights to the database, while Software Support staff only have editing rights.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

☐ Not Applicable.

Yes, authorized Noblis staff have access to the data within AcquTrak. Noblis has been contracted by the agency to administer the AcquTrak application and related professional support services to maintain the application throughout the FTC's CIO BPA acquisition process. As part of the contracted professional services, approved Noblis staff will have typical administrative access and privileges to view, load, validate, and back up data, as well as perform other maintenance functions with respect to the data. Noblis staff are responsible for configuring access privileges in accordance with the FTC CO's specifications. All FTC contractors are required to complete the FTC's IT security and privacy training before obtaining access to the FTC network and systems.

The FTC CO is responsible for identifying data rights within the system to include the right to share information with additional third parties. This may occur under limited circumstances when a third party or vendor wishes to protest the results of a bid or evaluation. In such cases, the FTC can produce the necessary files from AcquTrak to furnish to the necessary parties.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

☐ Not Applicable.

Noblis maintains an incident response plan as part of their company privacy policy, which provides training on what constitutes an incident (with specific and relevant examples) and the appropriate steps to respond to suspected or confirmed incidents. In addition, Noblis staff are responsible for notifying designated FTC officials and coordinating in the event an incident occurs concerning FTC-owned information.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☐ Privacy Act Statement (☐ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☒ Login banner
- ☒ Other (*explain*):___Noblis Privacy Policy_____

☐ Notice is not provided (explain):

The AcquTrak system is not accessible to the general public. When FTC employees use the online form to register on the AcquTrak website, they are presented with the following notice:

> Information submitted will be used for account creation and maintenance activities. Your information will be retained only until the time your account is closed. You may contact our support group at any time with questions or needs. If you choose to continue, your information will be collected, retained, and used for the purposes of participating in this source selection. It will be destroyed at the end of this source selection.

Once the user has logged into the system, an additional notice is provided which notifies the user about authorized use, monitoring, and data usage:

> WARNING: The use of this system is restricted to authorized users only. These systems and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel.

In addition, a link to Noblis' privacy policies is displayed on the bottom of each AcquTrak web page.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

All information provided by vendors in response to an agency solicitation for proposals or quotes is provided voluntarily. However, vendors who decline to provide the required information will be considered non-compliant as part of the initial source selection process, and their proposal will not be loaded into the system. Once submitted, the system does not provide vendors with any option to consent or decline to the use of their information other than required or authorized uses.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Individual members of the public (including vendors) do not have access to data in AcquTrak and therefore cannot access information within the system. Vendors provide information directly to the FTC, and that information is uploaded to Acqutrak without any edits or changes by Noblis staff. If a vendor wishes to view the information maintained about them in the AcquTrak system, they may contact the FTC CO to request a copy of their file, which would be identical to the information they originally provided in response to a bid.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

All information provided in response to an RFQ is voluntary and the vendor has the responsibility for ensuring accuracy of its information at the time of the submission. Once submission data is loaded into AcquTrak, it cannot be altered. To remain an impartial party and avoid any appearance of impropriety, Noblis staff do not make any alterations or changes to the data submitted to them by the FTC. Any requests to correct or change information provided by the vendor must be processed through the FTC's CO. The vendor must contact the FTC CO and identify any inaccuracies or erroneous information that had previously been provided to the agency. The vendor can then submit the corrected information, to the extent, if any, permitted by applicable law, regulation or policy, which would be entered into AcquTrak as an amendment to the existing record. The older, inaccurate information would continue to be maintained in the system as information cannot be altered or deleted once it has been uploaded to the system. The existing record is appended with the updated information.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Information and documentation provided to the FTC in response to an RFQ is voluntarily provided by the vendor and, as noted earlier, the vendor is responsible for ensuring that its information (including any PII that may be requested) is accurate, complete, and up to date at the time of the submission. The FTC CO and/or designated staff can review the documents submitted by the vendor to determine if the information is sufficient and meets the agency's standards for completeness and accuracy; however, there is no mechanism within the AcquTrak system itself to check for accuracy or thoroughness of the data.

In order to remain objective and support an ethical acquisition, Noblis has a policy not to alter any proposal submission data. AcquTrak system administrators follow an Acquisition Setup Checklist, which outlines steps to validate that the integrity of the data was preserved at setup. Once this information is loaded into the AcquTrak database, users have read-only privileges, to avoid inadvertent or intentional alteration of the information and loss of integrity.

All staff involved with maintaining and/or having access to the system are expected to adhere to written FTC policies regarding the nature and sensitivity of the information contained on the system pursuant to the non-disclosure agreement signed as a condition of employment.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Information maintained within the AcquTrak system is safeguarded in several ways. FTC staff access the system securely via the AcquTrak website by logging in with unique user IDs and passwords.

They must also use their PIV cards to authenticate their identities; PIV cards are unique to each user and act as an additional technical access control mechanism.

Additional controls and safeguards are in place for protection of data within the system. All evaluation information and comments on solicitations are maintained on secure servers. User accounts are role based, with the policy of least privilege extending down to the document level. Accounts are created and approved at the direction of the FTC CO. Data within AcquTrak is encrypted both at rest and in transmission. (Although the system will generally not contain any sensitive PII, the source selection information in the system may be sensitive.) AcquTrak access requires two-factor authentication, and the browser based application is only accessible through an encrypted web browser (TLS). AcquTrak automatically runs a system wide scan to identify any inactive user accounts which have not been used for at least 30 days; Noblis staff then disable these accounts, and users must contact them to request access be reinstated. The AcquTrak system administrators, Information System Security Officer (ISSO) and Information System Security Manager (ISSM) function with FTC Contracting Officers to ensure the proper use of data.

All system users (including Noblis staff) must sign the FTC Rules of Behavior as a condition of accessing any data in the system. FTC staff sign an additional Technical Evaluation Team (TET) Rules of Behavior that sets forth the minimum expectations and process to ensure the integrity of PII. As a matter of policy, Noblis staff accessing AcquTrak do not alter source selection information provided by vendors or FTC. AcquTrak system administrators follow an Acquisition Setup Checklist, which outlines the steps to validate that the integrity of the data is preserved when uploaded to the system.

5.3 Has the system/project undergone the appropriate security risk assessment and received authority to operate?

The AcquTrak system has undergone the appropriate Assessment & Authorization (A&A), including a risk assessment, and was granted an Authorization to Operate (ATO) by the FTC.

5.4 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

Noblis' AcquTrak policies, procedures, and rules or behavior prohibit the use of any sensitive data for testing, training, research; therefore PII is not used in testing, training or research. Dummy account names, company names, etc. are used for this purpose.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

User account information, such as passwords and user profiles, will be retained in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2, item 030, System Access Records, for six years after a password is changed or the user account is terminated.

Contract acquisition information, such as solicitation, evaluation, and source selection records will be retained for six years after final payment as required by NARA GRS 1.1, item 010, Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.

All data is securely disposed of in accordance with OMB, NARA, and NIST regulations and guidelines and with FTC policies and procedures. If the contract with Noblis should end prior to the vendor's ability to apply the GRS, the vendor agrees to transfer the data to the FTC for further management.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

☐ Not Applicable

AcquTrak is a web-based application. Session cookies are used to authenticate and maintain session identification for logging user (FTC, FMO, and OCIO) activity. No persistent cookies are used.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	*Mitigation Strategy*
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	System administrators strictly manage access control and limit the use and access of all data for the purposes for which it was collected. A system log is maintained in AcquTrak that reflects who accessed the data at any given time, and whether the data was tampered with or edited. Additionally, there is little PII of sensitivity, if any, in the system. Most of the PII is Business Contact Information, and

	data minimization is effectuated by only collecting data that is necessary for the purpose for which the system was designed.
Unauthorized individuals may have access to PII.	Only the FTC CO has the authority to determine which FTC employees should have access to the AcquTrak system in order to carry out their duties. The FTC CO shares the names and contact information for these individuals with Noblis staff, who create access accounts for them. Each FTC user has unique user ID and password, and FTC policy prohibits the sharing of login credentials.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Noblis, in accord with the FTC CO's designation, limits access to the information in AcquTrak to those authorized FTC employees who have a business purpose for accessing the data. The FTC coordinates with Noblis to ensure that appropriate safeguards are in place to protect the information from internal misuse or external threats. The AcquTrak application is not accessible to the general public, uses multifactor authentication, and requires unique usernames and passwords to access.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Not applicable. Records in the system will be retrieved by company or business name only, not by individual name or other personally assigned identifier. Accordingly, the records are not subject to the Privacy Act and, therefore, no SORN applies or is required.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The FTC and its contractors follow applicable Federal IT security requirements and FTC policy and procedures to ensure that all information in the agency's IT systems are secured appropriately. The FTC has conducted a risk assessment to identify appropriate security controls to protect against risks, and those controls have been implemented. Monitoring, testing, and evaluations occur on a regular basis to ensure that controls continue to work properly and that information is properly safeguarded. The FTC's Chief Information Security Officer (CISO) is the point of contact for any security questions related to this system.

The FTC will maintain PII and other information within AcquTrak in accordance with FTC regulations, policies, and procedures and with FTC records retention schedule N1-122-09-1 approved by the National Archives and Records Administration (NARA).

9 Approval and Signature Page

Prepared By:

_____ **Date: _____**
Kristina Brandriff
Vendor and Program Management Office (VPMO)

Reviewed By:

_____ **Date: _____**
Katherine Race Brin
Chief Privacy Officer (CPO)

_____ **Date: _____**
Alexander C. Tang, Attorney
Office of the General Counsel (OGC)

_____ **Date: _____**
Jeffrey M. Smith
Chief Information Security Officer (CISO)

_____ **Date: _____**
Jeffrey D. Nakrin
Director, Records and Filing Office

Approved By:

_____ **Date: _____**
Raghav Vajjhala
Chief Information Officer (CIO)