Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)

Privacy Impact Assessment
for
NTC Connect

Issued by:
Adam Siple, Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: April 4, 2023

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) National Tracing Center (NTC) is the United States' only crime gun tracing facility. NTC's mission is to conduct firearms tracing to provide investigative leads for federal, state, local and foreign law enforcement agencies. NTC is only authorized to trace a firearm for a law enforcement agency involved in a bona fide criminal investigation. The firearm must have been used, or be suspected to have been used, in a crime. This gun trace data is essential to law enforcement efforts to combat violent crime and firearms trafficking.

NTC oversees the NTC Connect Program, which stores firearm descriptive and disposition data. The NTC Connect system provides several cloud databases hosted on Amazon Web Services (AWS) that allow ATF trace personnel access to participating Industry Members (IM)[1] Acquisition & Disposition records (A&D records[2]) uploaded into the system. These records will remain the property of the participating federally licensed firearms manufacturers, importers, and dealers. As the records contained in NTC Connect are owned by private companies, the records and the identification of the companies do not fall under the federal requirements for transparency and are not subject to release under Freedom of Information Act (FOIA). IMs who voluntarily participate in the NTC Connect Program (and can depart the program at will) upload their A&D records online for one or more of the Federal Firearms Licenses (FFLs[3]) they possess.

IMs are the firearm manufacturers, importers, distributors, and wholesalers who utilize the NTC Connect system to store a copy of their A&D records. Presently over 30 IMs with over 70 Federal Firearms Licenses participate in the NTC Connect program. Each IM is required to maintain a separate FFL for each of their physical locations where firearm business activities are conducted (i.e., manufacturing, importation, buy, sell, trade). Each physical location in possession of an FFL is required to maintain A&D records to track all firearms that are received or manufactured ("acquired"), and each firearm that has been either sold, transferred, or destroyed ("dispositioned"). IMs utilize the A&D Records to document the following information for each firearm in their inventory: date of acquisition, name and address or FFL number from whom the firearm was acquired, manufacturer

---

[1] Industry Members (IM) are manufacturers, importers, distributors, and wholesalers who utilize the NTC Connect system to upload a copy of their Acquisition & Disposition (A&D) Records. IMs must possess at least one Federal Firearms License (FFL) for each physical location from where they conduct firearms activities (i.e., manufacture, import, buy, sell, trade).

[2] The firearms Acquisition and Disposition (A&D) Record documents where each firearm is acquired and disposed of by the FFL holder. Records must include the following information: the manufacturer or importer, model, serial number, type of firearm, caliber or gauge, date received, name and address or name and FFL of the person or company from whom the firearm is received, date of disposition, name of person or company to whom it went, address or FFL Number of the person or company to whom it was transferred.

[3] FFL refers to an individual or company licensed to engage in the business of manufacturing, importing and/or dealing in firearms. Persons must be licensed by ATF to engage in the business of firearms. There are 3 primary types of FFL: dealers, manufacturers, and importers. Each FFL must maintain its own A&D Records.

and/or importer, model, serial number, type, caliber/gauge, date of disposition, and name and address or FFL number to whom the firearm was disposed. ATF does not use or disseminate information from NTC Connect for any purpose other than to respond to a corresponding law enforcement firearms trace request[4].

The electronic A&D record data provided by participating IMs will be accessible to ATF NTC tracing personnel, including both Federal and contract employees, in performance of their law enforcement firearms tracing function pursuant to applicable laws and regulations. Both ATF and contractor tracing staff utilize the data provided by the IMs to complete trace requests submitted by Federal, state, and local law enforcement agencies, as well as non-US law enforcement in furtherance of criminal investigations. Conducting these traces online rather than through manual contacts (i.e., phone, fax, e-mail) saves the IMs and ATF time and releases personnel for other functions.
Outside of obtaining, maintaining, and using electronic A&D information relevant to the tracing process, there will be no creation, collection, disclosure, or disposition of information by authorized ATF employees and contract staff.

For IMs who choose to use NTC Connect, there are four mandatory fields for all entries: weapon serial number, manufacturer and/or importer, type, and caliber. However, since the user interface presents these fields as free-form text boxes, IMs could add other, unsolicited information that could consist of personally identifiable information (PII). Examples would be when a firearm is sold to a company employee, or a firearm was repaired by the manufacturer and returned to a member of the public.

The A&D record data provided by IMs documents the transfer of firearms from one licensee to another (e.g., licensed manufacturer to licensed distributor, licensed distributor to licensed dealer). ATF does not enter information into NTC Connect, does not access information without a corresponding law enforcement firearms trace request, and does not use or disseminate information in NTC Connect for any purpose other than to respond to a corresponding trace request. NTC Connect provides the IMs with the option to create a report to show when trace actions have been conducted on their data.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

IMs are required to maintain A&D records for each of their physical locations which conduct firearms activities. Those who participate in the NTC Connect Program maintain their records electronically and upload a copy of the A&D Records to the NTC Connect System. IMs who voluntarily participate in the NTC Connect Program only have access to their company data. A&D records track all the

[4] Most firearms tracing requests are electronically submitted by law enforcement representatives into FTA: Electronic Tracing (E-Trace), which also have the ability to monitor the progress of traces and retrieve completed trace results conducted. E-Trace is covered in detail in the FTA portfolio PIA. All ATF PIAs can be found at: https://www.justice.gov/opcl/doj-privacy-impact-assessments.

firearms that a licensee has received or made ("acquired"), and each of those firearms that the licensee has either sold, transferred, or destroyed ("dispositioned"). Industry members utilize the A&D records to document the following information for each firearm in their inventory: date of acquisition, name and address or FFL number of the industry member from whom the firearm was acquired, manufacturer or importer, model, serial number, type, caliber or gauge, date of disposition, and name and address or FFL number to whom the firearm was disposed.

ATF developed the NTC Connect System as an online service to provide IMs with an online database for maintaining a copy of their firearm A&D records in order to provide disposition information to the ATF NTC for tracing[5] recovered firearms more quickly and efficiently.

ATF does not enter information into NTC Connect and does not access information without a corresponding trace request from a law enforcement agency. ATF does not use or disseminate information in NTC Connect for any purpose other than to respond to a corresponding trace request from a law enforcement agency. All IM access to NTC Connect is via an approved internet protocol (IP) address. Prior to gaining access to the system, the external users coordinate with the NTC Connect System Administrator to have the IP address(s) associated with their businesses configured into the system. The AWS Access Control List will reject access attempts from IP addresses not configured in the system.

IMs control the inputting of data into NTC Connect and are able to pull back or remove records for correction and resubmission, due to errors, and are able to delete their own records if they have been uploaded within a 60-day period. This 60-day period is a configurable setting that can be changed if needed. After this period, IMs can request that an NTC Connect system administrator remove the record(s). IM records are shared with NTC Connect until the company is out of business (OOB). When an IM closes an FFL, they have 30 days to submit official OOB records to the ATF National Tracing Center, Out-of-Business Records Center. Once the official records are received for the closed FFL, the records in NTC Connect are removed and deleted. IMs can request to be removed from the NTC Connect Program via a written request provided 30 days prior to the date they plan to cease using the application.

NTC Connect provides an alternative to the otherwise manual processes through which ATF conducts firearm tracing. IMs who maintain electronic A&D records may opt to participate in NTC Connect as it provides a secure internet-based user interface, through which authorized NTC personnel can readily search by serial number against a copy of a licensee's electronic A&D records and retrieve corresponding disposition data, if applicable. Having the FFL data accessible to ATF reduces the labor needed to preform searches for both the ATF and the IMs.

Contract personnel, procured by the NTC, administer the system, and provide helpdesk-like services to resolve technical issues within the system. ATF and NTC personnel do not provide helpdesk-like system administration functionality.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the

[5] As noted above, firearms tracing requests are processed in ATF system "Electronic Tracing (eTrace)" which is a web-based application developed to provide web-based firearm trace submission and analysis capabilities to ATF, and domestic and foreign law enforcement agencies.

information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	28 U.S.C. § 599A. Bureau of Alcohol, Tobacco, Firearms, and Explosives 28 CFR Subpart W - Bureau of Alcohol, Tobacco, Firearms, and Explosives 18 U.S.C. Chapter 44 – Firearms Gun Control Act of 1968 (GCA) - Pub. L. 90-618, 82 Stat. 1213
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A & C	(A) ATF employees, contractors. (C) Names of FFL POCs. Retail purchaser data could be uploaded by licensees
Date of birth or age	X	C	Data uploaded from FFL could include retail purchaser of firearm's DOBs
Place of birth			
Gender	X	C	Data uploaded from FFL could include retail purchaser of firearm's gender
Race, ethnicity, or citizenship	X	C	Data uploaded from FFL could include retail purchaser of firearm's race
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license	X	C	Retail purchaser information is not normally contained in the system, however there may be exceptions for firearms that have sold to an employee. IMs could then include retail purchaser of firearms' Driver's License information.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C	Retail purchaser information is not normally contained in system, however there are exceptions for firearms that have been returned for repair or sold to an employee. This address data could be uploaded by IMs in a freeform text box.
Personal e-mail address	X	C	Retail purchaser information is not normally contained in system, however there are exceptions for firearms that have been returned for repair or sold to an employee. Retail purchaser e-mail address data could be entered into a freeform text box.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Personal phone number	X	C	Retail purchaser information is not normally contained in system, however there are exceptions for firearms that have been returned for repair or sold to an employee. Phone numbers could then be entered into a freeform text box.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Proprietary or business information	X	C	Address: licensee addresses, and professional titles. Email: licensee email addresses Phone: licensee business landline and mobile numbers
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A & C	(A) ATF employees, & contractors (C) Members of the public (citizen, USPERs) who are IMs
- **User passwords/codes**	X	A & C	(A) ATF employees, & contractors (C) Members of the public (citizen, USPERs) who are IMs
- **IP address**	X	A & C	(A) ATF employees, & contractors (C) Members of the public (citizen, USPERs) who are IMs
- **Date/time of access**	X	A & C	(A) ATF employees, & contractors (C) Members of the public (citizen, USPERs) who are IMs
- **Queries run**			
- **Contents of files**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	C	IMs enter information into free-form text boxes and could potentially submit other information not accounted for in this table.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component		Other DOJ Components		Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): NTC Connect only contains information related to FFL transactions. The data provided by IMs documents the transfer of firearms from one licensee to another (e.g., licensed manufacturer to licensed distributor). ATF does not enter information into NTC Connect, does not access information without a corresponding trace request and does not use or disseminate information in NTC Connect for any purpose other than to respond to a corresponding trace request from law enforcement agencies.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure

electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			NTC Connect data is not accessed without a specific law enforcement firearms trace request. ATF does not use or disseminate information in NTC Connect for any purpose other than to respond to a corresponding trace request from law enforcement.
DOJ Components	X			NTC Connect data is not shared with other DOJ agencies when firearms requests are submitted. Other than assigned staff, no login access is provided into NTC Connect. Data taken from NTC Connect is, typically, the 1st step in a trace, and consists of manufacture and wholesalers' data.
Federal entities	X			Other federal entities can request a trace with the corresponding legal requirements. They are not provided direct access.
State, local, tribal gov't entities	X			ATF will share E-Trace information with other state, local and tribal law enforcement agencies upon request with the corresponding legal requirements. Data will be pulled from NTC Connect and emailed to the requestors. They are not provided access to NTC Connect.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector			X	IMs are private companies that share their information with ATF in order to facilitate the process of tracing weapons, e.g., weapons collected by local, state, and federal law enforcement agencies during the course of criminal investigations.
Foreign governments	X	X		ATF partners with various foreign law enforcement agencies and shares data as needed. Partner agencies are required to establish a memorandum of understanding (MOU) with E-Trace. Data will be pulled from NTC Connect and emailed to the requestors. They are not provided access to NTC Connect.
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The data contained in NTC Connect is owned and maintained by private companies, therefore it is not releasable under the Open Data program or Freedom of Information Act (FOIA).

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is

provided, please explain.

Not applicable as the data is owned and provided to ATF by private companies and is not covered by any SORN.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

All information within the NTC Connect system is generally second-sourced and is captured, organized, and managed by individual industry member users (e.g., licensees and firearms manufacturers). Individuals involved in investigations and litigation are properly notified in accordance with Federal criminal and civil procedure and court rules. All information collected is part of existing or requested case data, as captured, or requested through voluntary requests, subpoenas, discovery requests, search warrants, civil investigative demands.

Individuals applying for firearms purchases do not have the opportunity to decline to provide the requested data and documents. Certain information may be provided voluntarily by the data subject. As required by law, generally ATF provides data subjects with appropriate notice of information collection under the Privacy Act, 5 U.S.C. § 552a(e)(3), e.g., when individuals submit applications for employment. Notice is not provided to individuals for information collected from public sources, i.e., publicly available information.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Data is owned and maintained by private companies and provided to ATF. This information is not considered "records" under the Privacy Act of 1974 or the Freedom of Information Act, 5 U.S.C. § 552.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):
X	Granted: TBD Expires: TBD Extension:

	If an ATO has not been completed, but is underway, provide status or expected completion date: **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** This is a new system, and there are no POAMs at this time
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Confidentiality – Low; Integrity - Low; Availability - Moderate FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability). Based on the assessment, ATF determined that the potential impact for Confidentiality and Integrity are low (i.e., the unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals), while Availability was evaluated as moderate (i.e., the disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals).
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** System monitoring, testing and evaluations are performed monthly, during annual assessments, or when system assessments are required for ATO renewal. Requests for changes to NTC Connect are reviewed by a change advisory board before being applied. The core controls are assessed annually, and include the controls related to the application and through generally inherited from the infrastructure, policy, or parent system. All system documentation supporting these activities are maintained within the Department's Cyber Security Assessment & Management tool.
	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:

	Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy. The electronic A&D Record data provided by each participating IMs will be accessible to ATF NTC tracing personnel, including both Federal and contract employees, in performance of their law enforcement firearms tracing function pursuant to applicable laws and regulations. ATF contract tracing staff utilize the data provided by the IMs to complete trace requests submitted by Federal, state, local and foreign law enforcement agencies in furtherance of criminal investigations. Conducting traces online saves the IMs and ATF time and releases personnel for other functions. ATF contractors are provided the same annual privacy training as all other employees and those with greater access receive additional training for protection of PII. All contractors are required to sign the DOJ General and Privileged Rules of Behavior, as determined by their role. All associated IT related contracts within ATF are required to comply with applicable policies and guidelines defined and documented within the Department of Justice, e.g., Procurement Guidance Document 15-03, Security of Information, and Information Systems. System owners acknowledge that FAR language is included in the contracts as it would pertain to privacy and system use and the Acquisition Policy Notice 2021-07A.
X	
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: All ATF users are subject to organizational and Department annual computer security awareness and privacy specific training that includes sign off and acknowledgment of the DOJ General and Privileged Rules of Behavior. In addition, personnel who have specific administrative roles within the application require and have received specialized role-based training, both prior to starting their position and as needed.
X	

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

All NTC Connect users are required to undergo training and sign formal Rules of Behavior prior to being granted access to data within NTC Connect. Each user will use unique usernames and passwords to access their NTC Connect accounts. All NTC Connect users must access the system from an approved IP address.

The database servers are located on a private subnet and are not accessible from anywhere other than the NTC Connect application, and the databases are encrypted at rest, and data are encrypted during transmission. Data access is restrictive; users require formal approval and

authorization to access information on a case-by-case basis. IM users can access only data which they own (i.e., IMs can only access information input by their own companies, not any other companies). Approved ATF and contract users have access to search the IM online data for which they are approved and then by serial number only.

Finally, the activity log is scanned daily. Accounts that have not had activity for 90 days are automatedly set to 'inactive' (requiring an administrator to re-instate the account if still needed).

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Individual users are responsible for ensuring that records processed or disseminated through NTC Connect are appropriately retained or destroyed. Requirements governing retention and disposition of ATF documents and information are documented within ATF Order 1340.7: consistent with National Archives and Records Administration regulations and rules, including records schedules**.**

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

__X__ No. _____ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

NTC Connect does not constitute a "system of records" [6] under the Privacy Act, thus there are no applicable SORNs. Records contained in NTC Connect are the property of the industry members (e.g., FFLs, manufacturers, importers, and dealers). ATF personnel retrieve information only through the use of serial numbers when required for investigations. ATF provides funding for NTC Connect as a database for FFLs, who may opt-in to use of the service for data retention. An NTC contractor provides all administration of the system. Should the details of this contract change, the information within NTC Connect would be transferred to the new contract holder.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the

[6] The term "records" as used in this context is defined under the Privacy Act of 1974, 5 USC 552a, and is not synonymous with the term "records" as used in other contexts, such as the Federal Records Act and National Archives and Records Administration records schedules or 18 USC 926 (a)(3).

Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

Firearms tracing is the systematic process of tracking the movement of a firearm recovered by law enforcement officials from its first transfer by the manufacturer or importer through the distribution chain (wholesaler/retailer) to the first retail purchaser/transferee. NTC Connect provides a cloud database hosted on AWS to a participating Federal Firearms Licensee or IM at ATF's expense.

One privacy risk inherent in the use of NTC Connect is unauthorized access. The NTC Connect System gives the licensee the autonomy to grant ATF access to perform secure online serial number searches, thereby reducing the burden on the licensee, while improving response time and success rates through ATF's 24/7 access to firearm disposition information. This is accomplished through a secure web application hosted on the NTC Connect Web Server. Authorized NTC employees can query the IM's NTC Connect individual database by serial number only through a secure web interface (requiring access via a known IP Address). Once an IM or licensee is onboarded to the NTC Connect System, the IM will upload its limited firearms acquisition and disposition data and then periodically (preferably once a week, but at least monthly) update that data as it becomes available.

Strict firewall rules are implemented that restrict access to all servers. Database servers are located on a private subnet and are not accessible from anywhere other than the NTC Connect application. All databases, passwords, and user information are encrypted in transit and at rest.

The privacy risks associated with personal information collected within NTC is also limited primarily because PII is not collected as a requirement for a data entry to NTC Connect. Though some PII may be in the system, ATF endeavors to mitigate this risk by restricting access to authorized account holders assigned to the ATF NTC and IMs. User accounts are monitored with password expiration and complexity requirements. And the system automatically removes access for any user account that has been inactive for 90 days. User sessions are terminated following 20 minutes of inactivity, limiting the possibility of an unauthorized user gaining access to an untended session. The data for each IM is considered a separate database, there is no crossover or interconnection from one company to another. Tracing center staff are assigned to individual Industry Members and can only search the database for those Industry Members they have been assigned to.