Privacy Impact Assessment
for the

eTrace

May 30, 2006

Contact Point

Charles J. Houser, Chief
National Tracing Center Division
Office of Enforcement Programs and Services
304-260-1510

Reviewing Official

Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) National Tracing Center (NTC), a service-oriented entity, has developed an electronic interface to its firearm tracing services, called eTrace, which allows for the secure exchange of crime gun incident based data. By definition, firearms tracing is the systematic tracking of the movement of a firearm recovered by law enforcement officials from its creation by the manufacturer or its introduction into U.S. commerce by the importer through the distribution chain (wholesaler/retailer) to the first retail purchase. Recovered firearms are traced by Law Enforcement Agencies a) to link a suspect to a firearm in a criminal investigation; b) to identify potential firearms traffickers, whether licensed or unlicensed sellers, and; c) to detect in-state, interstate, and international patterns in the sources and kinds of gun crimes.

ATF has extended its on-going commitment to the law enforcement community by providing approved agencies with a paperless firearm trace submission system that is readily accessible through a connection to the worldwide web (Internet). The focus of the eTrace application is to enhance current trace protocols to efficiently function in a web-based environment and provide for the secure exchange of firearm trace related information between the user community and the ATF, National Tracing Center. The eTrace application provides the necessary utilities for submitting; retrieving, storing and querying all firearms trace related information relative to a participating Law Enforcement agency. This tool not only provides users with the ability to electronically submit firearm trace requests, but also to monitor the progress of traces and efficiently retrieve completed trace results in a real-time environment.

To access and utilize the eTrace application, the only infrastructure an agency needs is a personal computer and access to the World Wide Web, thus empowering even the smallest of agencies to comprehensively trace their firearms and perform on-line data analysis. eTrace access is achieved by obtaining a valid User Id. and password from ATF and authenticated using the eTrace site on the internet. Each participating agency also enters into a Memorandum of Understanding (MOU) with ATF. The MOU is intended to formalize a partnership between the participating agencies with regard to policy and procedures relative to the access and utilization of eTrace services. Successful access allows users the ability to enter new traces, view existing traces, and run reports on traces for which they are authorized.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The data consists of firearms trace requests, firearms trace results, purchaser, possessor, associate, vehicle and recovery information is captured. This can include an individual's date of birth, place of birth, name, address, height, weight sex, vehicle ID information, driver's license information, recovery information, firearms description, FFL information, requesting agency information, officer name and contact information, and special instructions.

1.2 From whom is the information collected?

The information is collected from official local, state Federal and international law enforcement agencies, Federal firearms licensee records kept under the Gun Control Act, 18 U.S.C., Chapter 44; FFL out of business records, and multiple sales information.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

To provide investigative leads to Federal, state and local law enforcement agencies in the course of bona-fide criminal investigations and to identify potential firearms trafficking trends. Recovered firearms are traced by Law Enforcement Agencies a) to link a suspect to a firearm in a criminal investigation; b) to identify potential firearms traffickers, whether licensed or unlicensed sellers, and; c) to detect in-state, interstate, and international patterns in the sources and kinds of crime guns. Firearm tracing is the systematic process of tracking a recovered crime gun chain of custody from its source (manufacturer/importer) through the chain of distribution (wholesaler/retailer) to the individual who was the first retail purchaser of the firearm, or to a point where all other possibilities of identifying the original purchaser have been thoroughly exhausted. Comprehensive firearms tracing by jurisdiction or community, involves the tracing of all recovered crime guns within a particular geographic area (e.g., city, county, metropolitan area, or State). Information obtained through the tracing process is utilized to solve and/or enhance individual cases and to maximize investigative lead development through eTrace. Law Enforcement agencies that make a commitment to comprehensive firearms tracing through ATF will be provided with an information platform for developing the best local investigative strategies for their community in the reduction of firearm related crime and violence.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The Bureau of Alcohol, Tobacco, Firearms and Explosives is the sole Federal law enforcement agency tasked with the tracing of firearms and is authorized under the GCA. Law enforcements agencies may trace any firearm that has been possessed illegally, used in a crime, suspected of being used in a crime or possessed by a juvenile or prohibited person. The ATF National Tracing Center processes firearms trace requests received from law enforcement agencies across the United States and around the world.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

If this information is accessed by a non-law enforcement individual, it could jeopardize an on-going criminal investigation and cause personal injury to law enforcement personnel, cooperating individuals and witnesses.. For the most part, however, privacy risks are minimal due to the fact that eTrace accounts are given to cleared ATF employees and law enforcement agencies that have entered into an MOU with ATF. In accordance with applicable appropriations laws, eTrace users can only access trace data that originated from their agency. In addition, the eTrace system includes the standard HTTP Level banner on the bottom of each web page which reads, "You have entered an Official United States Government System, which may be used only for authorized purposes. The government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Section 1001 and 1030."

Among risks that ATF has identified and mitigated over the life cycle of the eTrace system are:

1. Electronic Security – Access Controls for Authorized Users

   Unauthorized electronic access to data stored in the eTrace database. This risk is principally by persons who are employees of ATF or members of a Federal, State or local law enforcement agency that have been authorized access to the eTrace system in connection with their official duties. This risk is mitigated with extensive audit logging.

2. Physical security – Environmental impacts

Unauthorized access to data stored in the eTrace database. Addressed by ATF physical security measures (clearances, guards, cameras, MOU's, etc.)

3. Loss of power

   Unauthorized access to data stored in the eTrace database. This risk is mitigated by redundant power sources with instant coverage.

4. Theft of backup tapes in transit or at offsite storage locations.

   Unauthorized access to data stored in the eTrace database. This risk is mitigated by the use of a bonded official backup company.

5. Hacking – Attempts to access the database by unknown parties

   Unauthorized access to data stored in the eTrace database. Addressed with internal host and network intrusion detection systems, firewalls, log monitoring and Counterpane system review.

6. Loss of Data Integrity due to viruses, worms and Trojan horses

   Unauthorized access to data stored in the eTrace database. Addressed with numerous layers of malware detection and correction software at workstation, server, mail gateway and border devices.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

Recovered firearms are traced by Law Enforcement Agencies a) to link a suspect to a firearm in a criminal investigation; b) to identify potential firearms traffickers, whether licensed or unlicensed sellers, and; c) to detect in-state, interstate, and international patterns in the sources and kinds of gun crimes. Information obtained through the firearm tracing process is utilized to solve and/or enhance individual cases and to maximize investigative lead development through eTrace. Law Enforcement agencies that make a commitment to comprehensive firearms tracing through ATF will be provided with an information platform for developing the best local investigative strategies for their community in the reduction of firearm related crime and violence. They will be able to discern firearms trafficking patterns and allocate resources.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

eTrace provides approved users with immediate access to query their firearm trace-related data stored in the ATF Firearms Tracing System (FTS) database, through a user-friendly online search utility. Through eTrace, registered users have the capability to initiate a search for traces on virtually any data field or combination of data elements. For example, users can search by a firearm's serial number, individual name, type of crime, date of recovery, and numerous other identifiers. Registered eTrace users can also generate various statistical reports regarding the number of traces submitted over time, the top firearms traced, the average time-to-crime rates, and more. These reports provide a snapshot view of potential firearm trafficking indicators.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

Firearm trace request data submitted via eTrace is validated against numerous reference tables and validation tables contained in the front-end of the eTrace applications. These real-time edits and validations are performed on the eTrace front-end interface and help to ensure the completeness and accuracy of incoming data. In addition, the application contains “hard” and “soft” error messages to prompt the user to complete all required fields. Any incoming firearm trace related data that cannot be validated by the application is flagged for manual review and correction and sent to the Error Correction Module (ECM). The NTC also conducts routine quality control checks on outgoing information.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Draft scheduled for July 2006.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The eTrace system includes the standard HTTP Level banner on the bottom of each web page which reads, “You have entered an Official United States Government System, which may be used only for authorized purposes. The government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Section 1001 and 1030. In addition, hard copies of all MOU’s, which have been signed by the SAC and law enforcement official acknowledging the terms of use of the eTrace application are maintained by the NTC Division. Access controls are role dependent. In order to gain authorized access to the eTrace application data:

1. As stated earlier, for outside law enforcement agencies, an MOU must be in place before access is granted. The MOU will list the names of all individuals that should be granted access.
2. All users must go to the ATF eTrace website and click on the “How Do I Register Link”. The user completes the form and processes the request.
3. An email is then sent to the National Tracing Center indicating that the individual is requesting access.
4. If the individual if from an outside law enforcement agency, the MOU for that agency is checked to ensure that the individual’s name appears on the MOU.
5. NTC enters a Remedy ticket and the ticket is forwarded to the Oracle Group.
6. The Oracle Group sets up the eTrace account and then sends notification of the established account to the NTC.
7. The NTC then sends an email to the user advising them that an account has been established and providing them with their temporary password.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Usage of eTrace is Bureau-wide. eTrace access has also been provided to the Drug Enforcement Administration pursuant to a signed MOU.

4.2 For each recipient component or office, what information is shared and for what purpose?

Approved ATF users of the eTrace application (This includes ATF employees and ATF contractors and approved Federal, state and local law enforcement agencies) are provided access to all firearms trace related data collected by the NTC and referenced in Sections 1.0 and 2.0. In accordance with applicable appropriations laws, non-ATF users can only access trace data that originated from their particular agency. See Section 5.2 regarding information that is shared and the purpose.

4.3 How is the information transmitted or disclosed?

Information is made available through a secure web site to be viewed, printed or downloaded.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

All ATF users are required to complete the security awareness training course offered by ATF Training Division. The computer-based training (CBT) course is available on the ATF Intranet to be taken annually. Security Awareness training has been implemented to ensure that all employees, contractors, and volunteer personnel are aware of their security responsibilities. In addition, access to the eTrace application is administered through a secure transmission. Certification and Accreditation is in place ensuring controls are in place and vulnerability assessments are conducted against the application. Remediation is performed on deficiencies.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

eTrace is available only to official law enforcement agencies (local, state, federal and international) that have entered into a Memorandum of Understanding (MOU) with ATF acknowledging procedures, conditions, and terms of use.

5.2 What information is shared and for what purpose?

Participating Law Enforcement Agencies are provided with disposition information relative to a recovered firearm. Information provided by the NTC includes the federal firearms licensee' chain of custody as well as a description of the original retail purchaser of the recovered firearm. Recovered firearms are traced by Law Enforcement Agencies a) to link a suspect to a firearm in a criminal investigation; b) to identify potential firearms traffickers, whether licensed or unlicensed sellers, and; c) to detect in-state, interstate, and international patterns in the sources and kinds of gun crimes.

5.3 How is the information transmitted or disclosed?

Information is made available electronically thru a secure https web site.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Because of language contained in the Consolidated Appropriations Act of 2005, ATF is now prohibited from disclosing to the **public** ANY information required to be kept as a record by FFLs or reported to ATF. As such, ATF can only provide trace data to a law enforcement agency in connection with a bona fide investigation within their jurisdiction. This applies to disclosures through FOIA requests or otherwise. The purpose of this MOU is to establish an interagency agreement governing the access and utilization of eTrace. In addition, the MOU will designate a primary and alternate point of contact within your agency. The agency point of contact will be charged with ensuring adherence to the MOU between the Bureau and the client agency users. The MOU will require the designated agency point of contact to identify individuals from their respective agency who will require system access, to periodically validate the list of users and to notify the National Tracing Center immediately in the event that it becomes necessary to revoke or suspend a user's account.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

eTrace is a user-friendly web-based application for use by official law enforcement agencies only. An eTrace User's Guide is available on-line.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

The auditing is accomplished on the Oracle database recording the following information activity within the database.

- Userid
- Terminal id
- Action code
- Time stamp of action

Audit trails are designed and implemented to record appropriate information that can assist in intrusion detection. Descriptions of records captured include:

- Unsuccessful selects, inserts, updates and deletes
- Successful deletes
- Create index, alter index and drop index
- Create function, create library, create package, create package body, create procedure, drop function, drop library, drop package and drop procedure
- Create profile, alter profile and drop profile
- Create public database link and drop public database link
- Create public synonym and drop public synonym
- Create role, alter role, drop role and set role
- Create sequence and drop sequence
- Failed session logons and successful session logons
- Grant system privileges and roles
- Revoke system privileges and roles
- Create table, drop table and truncate table
- Create view and drop view

Audit trails are also used as online tools to help identify problems other than intrusions as they occur. Audit trails are employed as follows:

The audit trail can be used to troubleshoot the following:

- Unauthorized users
- Potential database problems
- Disk space
- Deadlock conditions
- Connection to the databases
- Users who have DBA privileges
- Users who have been granted some type of administrative or DBA role
- Users who have been granted an "any" role that gives them access to objects outside of their own schema
- Gather tuning data

According to the Oracle Security Checklist, the following audit data is enabled.

Oracle Auditing
Turn ON audit database administration (DBA) connections
Allow only Admins to turn auditing ON or OFF
Set the Audit trail table to be owned by the system
Locate the audit trail table in a separate tablespace/datafile
The following settings should be audited:
Create object
Drop object
Alter object
All deletes
All logons and logoffs
The following need to be added to every column in the database
Last created user
Last created data/time
Last updated user
Last updated date/time

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

External eTrace users are required to comply with the eTrace Memorandum of Understanding which specifies that external user accounts must be requested through a formal request (see the eTrace MOU) and then approved by the ATF eTrace administrator. External users cannot access eTrace until their account has been set-up and approved by the ATF eTrace administrator.

FIPS PUB 73, Paragraph 7.2.2. applies to internal eTrace users. Management has implemented the concept of "Separation of Duties" and divided critical functions between two or more individuals. All users are assigned to a role and each role gives the user a particular level of authorization.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

No. Information collected and made available via eTrace is strictly in furtherance of a law enforcement investigation. The eTrace system includes the standard HTTP Level banner on the bottom of each web page which reads, "You have entered an Official United States Government System, which may be used only for authorized purposes. The government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Section 1001 and 1030."

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. Access to and the utilization of eTrace is voluntary for Federal, state and local law enforcement agencies; however Federal Firearms Licensees (FFL's) are required by law to provide firearms trace information within 24 hours of a request being made by the NTC. However, FFL's are required by law to provide firearms trace information within 24 hours of a request being made by the NTC. eTrace does contain Privacy Act information on individuals that have been involved in a crime; however, this information is not available to private citizens and the information is used solely for bona-fide criminal investigations.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Access by law enforcement agencies to eTrace is voluntary; however, FFL's are required by law to provide firearms trace information within 24 hours of a request being made by the NTC.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The "individuals" from whom the information in question is collected are all law enforcement officer. They are the only people from whom ATF is authorized to trace firearms. The eTrace system includes the standard HTTP Level banner on the bottom of each web page which reads, "You have entered an Official United States Government System, which may be used only for authorized purposes. The government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Section 1001 and 1030." In addition, hard copies of all MOU's, which have been signed by the SAC and law enforcement official acknowledging the terms of use of the eTrace application.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

This is not a public system. eTrace is only available to approved Federal, State and local law enforcement agencies. Information that is entered by approved Federal, State and local law enforcement agencies can be updated by that entity. Since all eTrace fields are not accessible by these agencies, the National Tracing Center can be contacted to address other changes/updates that may need to be made.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Information is contained in the eTrace User's Manual.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

The individual agencies can contact the National Tracing Center Division.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

N/A.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

Approved Federal, State, local and international law enforcement agencies only.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes. Cleared contractors under the SAGE contract, Systems, Services & Designs contract and the FedSource Reimbursable Agreement have access to eTrace. In addition, other cleared contractors in the field also have access to eTrace. These individuals must sign a non-disclosure agreement and must undergo a successful background investigation. The complete SAGE contract is located in the Acquisitions Division.

8.3 Does the system use “roles” to assign privileges to users of the system?

Yes. These roles are designated by the Administrator of eTrace who is located at the National Tracing Center Division. See Section 8.5 for a description of these roles. Roles are as follows:

- ATF Users
- Local Law Enforcement Users
- ATF Admin User

8.4 What procedures are in place to determine which users may access the system and are they documented?

The eTrace application is administered by the ATF National Tracing Center Division. However, access to eTrace is being coordinated through the various ATF Field Divisions located throughout the United States. To gain access to eTrace, the requesting law enforcement agency's chief of police (or equivalent) must complete and return the eTrace Memorandum of Understanding (MOU). The MOU establishes an interagency agreement governing the access and utilization of eTrace. In addition, the MOU will designate a primary and alternate point of contact within each participating agency. The appointed individual(s) will be responsible for providing and maintaining a list of personnel within their department that require access to eTrace. eTrace access is only granted to Federal, State and local law enforcement individuals that are listed on the corresponding MOU. Written procedures relative to eTrace system access are maintained by the NTC Division.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The primary users of the system are personnel at ATF field offices and outside law agencies, accessing the system via web browser across the internet. The following are the user organizations for eTrace:

ATF Users: ATF users will be able to view and report on all traces in FTS through the eTrace interface.
Local Law Enforcement Users: Local Law enforcement users will be able to view and report on all traces submitted by their Agency's Originating Office Code (ORI).
ATF Admin User: ATF Admin Users will be able to view, update and report on all traces in FTS as well as update the reference tables for eTrace.

With the exception of a few individuals at the NTC who administer the eTrace application, all users to include internal ATF users and external Law Enforcement users are granted the same role in the database. Any determinations relative to the assignment of roles and rules will be made by the eTrace program manager in conjunction with the ISSO. In addition, a quarterly report listing all individuals with access to eTrace is sent to the NTC for review. Once the report is received, it is reviewed, updated and returned to ISD.

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

The auditing is accomplished on the Oracle database recording the following information activity within the database.

- Userid
- Terminal id
- Action code
- Time stamp of action

Audit trails are designed and implemented to record appropriate information that can assist in intrusion detection. Descriptions of records captured include:

- Unsuccessful selects, inserts, updates and deletes
- Successful deletes
- Create index, alter index and drop index
- Create function, create library, create package, create package body, create procedure, drop function, drop library, drop package and drop procedure
- Create profile, alter profile and drop profile
- Create public database link and drop public database link
- Create public synonym and drop public synonym
- Create role, alter role, drop role and set role
- Create sequence and drop sequence
- Failed session logons and successful session logons
- Grant system privileges and roles
- Revoke system privileges and roles
- Create table, drop table and truncate table
- Create view and drop view

Audit trails are also used as online tools to help identify problems other than intrusions as they occur. Audit trails are employed as follows:

The audit trail can be used to troubleshoot the following:

- Unauthorized users
- Potential database problems
- Disk space
- Deadlock conditions
- Connection to the databases
- Users who have DBA privileges
- Users who have been granted some type of administrative or DBA role
- Users who have been granted an “any” role that gives them access to objects outside of their own schema
- Gather tuning data

According to the Oracle Security Checklist, the following audit data is enabled.

Oracle Auditing
Turn ON audit database administration (DBA) connections
Allow only Admins to turn auditing ON or OFF
Set the Audit trail table to be owned by the system
Locate the audit trail table in a separate tablespace/datafile
The following settings should be audited:
Create object
Drop object
Alter object
All deletes
All logons and logoffs
The following need to be added to every column in the database
Last created user
Last created data/time
Last updated user
Last updated date/time

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All ATF users are required to complete annual Security Awareness Training and annual AIS training. External users gain access through a secure http web site and are required to complete an MOU.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Dates for Certification & Accreditation are maintained by ISSO. Certification and Accreditation is performed every three years or when a major change is made to the application.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

This information is maintained by the ISSO.

Section 9.0
Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. The contractor was selected through the ATF Acquisition Process and all SDLC guidelines were adhered to.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

All applications must be tested by ATF Security before an application is placed into Production.

9.3 What design choices were made to enhance privacy?

The HTTP banner, markings that indicate "Sensitive But Unclassified" and use of the Memorandum of Understanding.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

As stated earlier, all applications must pass stringent testing that is performed by the ISSO before it is placed into Production. In addition, eTrace contains the HTTP banner cited earlier, "Sensitive But Unclassified" markings and MOU's that are signed by all involved parties.

Responsible Officials

/signed/

Charles J. Houser, Chief

National Tracing Center

Bureau of Alcohol, Tobacco, Firearms and Explosives

Department of Justice

Approval Signature Page

________________________________ <<Sign Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice