



Privacy Impact Assessment
for the

Firearms Integrated Technology (FIT)

June 29, 2006

Contact Point

Lee Alston-Williams

**Firearms and Explosives Services Division
Enforcement Programs and Services Directorate
202 927-8441**

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) mission is to provide industry regulation, revenue collection and protection, and law enforcement of federal statutes regarding firearms, explosives, arson, alcohol and tobacco. In support of the firearms component of its mission, Enforcement Programs and Services (EPS) Directorate has developed over 20 applications to perform crime gun tracing, firearms licensing, and firearms law enforcement. Unfortunately, EPS systems have been developed using a "stove pipe," standalone implementation, resulting in data and application logic redundancy, making application maintenance and enhancements increasingly difficult. Additionally, ATF is planning to meet the 1998 Government Paperwork Elimination Act (GPEA), which requires federal agencies to provide for the option of electronic submission of information as a substitute for paper.

The Firearms Integrated Technology (FIT) investment closes an existing gap in the Bureau's mission and ability to effectively provide focused, real-time, integrated information products for ATF agents and inspectors, our federal partners, industry, foreign allies, stakeholders and the general public. Through this initiative, ATF will modernize the current IT infrastructure creating opportunities for database consolidation as well the retirement of legacy systems. FIT will help to create a web-enabled, customizable, information analysis portal, whereby ATF personnel can acquire firearms, arson and explosives information to better protect the public, prevent diversion, deter violent crime, disrupt / prevent terrorist attacks, support Homeland Security initiatives, and protect our National Security. Additionally, this investment supports ATF's core mission objective of enforcing the Federal firearms laws. e.g., the Gun Control Act (GCA) and the National Firearms Act (NFA). From a technology standpoint, FIT will integrate the various systems and applications ATF uses to fulfill its regulatory and enforcement mission. These systems are listed in the table below:

System Name	Acronym
Annual Firearms Manufacture and Exportation Report	AFMER
Electronic Forms 6	eForm 6
Firearms and Explosives Imports System	FEIS
Federal Licensing System(including FFLeZ Check and automated Criminal History Check (ACHC))	FLS
National Firearms Act	NFA

Currently, ATF personnel must access ten or more systems to view the complete history of a particular crime gun. The goal of FIT is to eliminate the standalone and isolated applications and ensure that all firearms and explosives systems interface and communicate effectively with other ATF systems.

In 2003, the Safe Explosives Act (SEA), which amended Title XI of the Organized Crime Control Act of 1970, (18 U.S.C. Chapter 40), was enacted. Modifications were made, and are currently being made to the FLS component of FIT, by the Firearms and Explosives Services Division, the owners of FIT-Firearms Services Applications (FSA) to support the SEA. The FLS is the automated system used to issue Federal firearms and explosives licenses and permits and for tracking license information on firearm and explosive manufacturers, importers, and dealers. The Federal Firearms Licensing Center (FFLC) and Federal Explosives Licensing Center (FELC) use the system to support the process of reviewing and making final determinations on applications for firearms and explosives licenses and permits. The new legislation enables ATF to systematically identify and conduct background checks on such employees, to

reduce the risk that prohibited persons will gain access to explosives. The SEA also expands the categories of prohibited persons to include: (1) aliens (with limited exceptions); (2) persons dishonorably discharged from the military; and (3) citizens of the United States who have renounced their citizenship.

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?

Information collected in FIT is required by ATF personnel to make determinations as to whether an application for a permit or license for firearms and explosives, or the possession or transfers of National Firearms Act Weapons or the importation of firearms, ammunitions or implement of war, is to be approved. The demographical information that is collected included the name, date of birth, social number, alien registration number, maiden name race, sex and place of birth.

1.2 From whom is the information collected?

The information is collected from the firearms or explosives license/permit applicants and employees of the explosives licensees or permittees, persons wishing to import firearms into to the US, and persons wishing to possess National Firearms Act (NFA) weapons.

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?

The information is collected to determine if the applicant, licensee or permittee, has suitable business premises and is not prohibited from conduction business in the regulated industry for which it intends to do business.

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

DISCLOSURE

**Confidentiality of Tax Return Information, 26 U.S.C. § 6103 -
Freedom of Information Act, 5 U.S.C. § 552 -
Privacy Act, 5 U.S.C. § 552a -**

ETHICS

**Ethics in Government Act of 1978 -
Hatch Act -**

EXPLOSIVES

Title XI of the Organized Crime Control Act of 1970, 18 U.S.C. Chapter 40 -

Title XI of the Organized Crime Control Act of 1970 (18 U.S.C. Chapter 40) establishes controls over explosive materials, including black powder and other pyrotechnic compositions commonly used in fireworks. Part 55 of Title 27, Code of Federal Regulations (CFR), contains the regulations which implement Title XI. § 555.141(a)(7) exempts "the importation and distribution of fireworks classified as Class C explosives and generally known as 'common fireworks,' and other Class C explosives, as described by U.S. Department of Transportation regulations in 49 CFR 173 .100(p),(r),(t),(u), and (x)."

FIREARMS

Gun Control Act, 18 U.S.C. Chapter 44 -

(a) The Attorney General may prescribe only such rules and regulations as are necessary to carry out the provisions of this chapter, including—

- (1)** regulations providing that a person licensed under this chapter, when dealing with another person so licensed, shall provide such other licensed person a certified copy of this license;
- (2)** regulations providing for the issuance, at a reasonable cost, to a person licensed under this chapter, of certified copies of his license for use as provided under regulations issued under paragraph (1) of this subsection; and
- (3)** regulations providing for effective receipt and secure storage of firearms relinquished by or seized from persons described in subsection (d)(8) or (g)(8) of section 922.

No such rule or regulation prescribed after the date of the enactment of the Firearms Owners' Protection Act may require that records required to be maintained under this chapter or any portion of the contents of such records, be recorded at or transferred to a facility owned, managed, or controlled by the United States or any State or any political subdivision thereof, nor that any system of registration of firearms, firearms owners, or firearms transactions or dispositions be established. Nothing in this section expands or restricts the Secretary's^[1] authority to inquire into the disposition of any firearm in the course of a criminal investigation.

(b) The Attorney General shall give not less than ninety days public notice, and shall afford interested parties opportunity for hearing, before prescribing such rules and regulations.

(c) The Attorney General shall not prescribe rules or regulations that require purchasers of black powder

under the exemption provided in section 845 (a)(5) of this title to complete affidavits or forms attesting to that exemption

National Firearms Act, 26 U.S.C. Chapter 53 -

The National Firearms Act provides for the registration, and the taxing of the transfer, of a class of weapons described as NFA Title 2 weapons (sometimes referred to as "Class 3 weapons"). These include machine guns, short barreled rifles, short barreled shotguns, silencers (also known as suppressors) and also a class of weapons known as "Any Other Weapon" (AOW). An example of an AOW is, but not limited to, a smooth barreled pistol or a short barreled combination gun.

Brady Handgun Violence Prevention Act -

Federal firearms licensee required to conduct criminal background check before transfer of firearm to non-licensee.

FORFEITURE

Forfeiture Laws, 18 U.S.C. §§ 981, 982 -

Providing false information to U.S. Customs related to the importation of merchandise into the United States may be a criminal and, or, civil violation. Primary laws associated with violations found in Title 18 U.S. Code and other statutes, including the following:

18 USC 541	Entry of goods falsely classified
18 USC 542	Entry of goods by false statements
18 USC 545	Smuggling into U. S.
18 USC 981-982	Forfeiture
18 USC 1001	False statements, generally
18 USC 1956-1957	Money laundering
18 USC 2319-2320	Intellectual Property Rights
15 USC 1121-1127	Trademarks
17 USC	Copyrights
19 USC	Customs laws
35 USC	Patents

In addition, violations of Title 18 Sections 542 and 545 provide a basis to charge money laundering under Title 18 Sections 1956 and 1957. Funds used to promote the violations of Title 18 Sections 542 and 545 or the proceeds of the violations may be forfeited to the U.S. government through Sections 981 and 982. The U.S. Customs Service shares forfeited assets with domestic and foreign law enforcement agencies who participated in the investigations.

Gun Control Act, 18 U.S.C. § 924(d) -

The primary focus of Title I of the Gun Control Act is to provide federal assistance to state firearms control efforts by requiring licensing for all persons dealing in firearms or ammunition. The Gun Control Act also specifies certain high risk individuals who are declared ineligible to purchase firearms. Other provisions in the Title prohibit interstate mail order sale of all firearms and ammunition, interstate sale of all handguns, interstate sale of certain long gun, and importation of non-sporting firearms.[14]

National Firearms Act, 26 U.S.C. § 5872 -

The National Firearms Act provides for the registration, and the taxing of the transfer, of a class of weapons described as NFA Title 2 weapons (sometimes referred to as "Class 3 weapons"). These include machine guns, short barreled rifles, short barreled shotguns, silencers (also known as suppressors) and also a class of weapons known as "Any Other Weapon" (AOW). An example of an AOW is, but not limited to, a smooth barreled pistol or a short barreled combination gun.

INTERNATIONAL LAW (AS APPLICABLE PURSUANT TO TREATY OR FEDERAL LAW)

European Union Laws -

Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials -

World Trade Organization -

LITIGATION

TAX

Internal Revenue Code of 1986, Title 26, United States Code -

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.

The data required is limited to what is authorized by Federal law and regulation in order to act appropriately on an application. Information is only disseminated on a need to know basis. Information relating to NFA is not disclosed to anyone except the applicants. Standard Operating Procedures (SOP's), system user's manuals, and employees' desk manuals that are issued to all employees within the Firearms and Explosives Services Division (FESD). These manuals outline the employee's responsibilities and to the acquisition, handling and protection of the data for each automated system.

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.

The system is used to generate the required licenses, permits, transfer authorizations and approval required to engage in regulated activities involving the manufacture, import, dealing, use or transfer of firearms and/or explosives. The system is used to generate report relating to these activities.

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.)

Yes. Each system has internal reports for which data can be mined for trend analysis and performance reporting.

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

All reports are reviewed and tested by member of an Integrated Project Team to determine their accuracy prior to being placed into production. There are also validations built within the systems that prevent the entry of inaccurate data.

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)?

FIT is a permanent system of records. The retention schedule is scheduled to be drafted in 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.

Each system within FIT has User Guides, the FIS-FSA System Security Plan, FIT-FSA Risk Assessment and Contingency Plan that are strictly adhered to. Any release of information must be approved by a supervisor, including responses to FOIA requests.

**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?

The FBI and other components on a case by case basis, to the extent authorized by Federal law.

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

FIT information is shared with the FBI for the purpose of conducting “criminal background checks” to determine if an applicant is a “prohibited person”.

4.3 How is the information transmitted or disclosed?

Fingerprint cards are either mailed to the FBI for processing or scanned and transmitted through an electronic batch file. Demographical data such as the name, date of birth, race, sex and social security number is encrypted and transmitted electronically.

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

Firewalls, dedicated circuits and encryption is used to protect the data provided in the electronic files.

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?

Federal, State and local governments often request information on the names and location of Federal firearms and explosives licensees and permittees, as well as other information, which is only provided as authorized by Federal law. Private sector can request the information through the Freedom of Information Act.

5.2 What information is shared and for what purpose?

Names and locations of Federal firearms licensee and permittees, and other law enforcement and regulatory information, to ensure that they are aware and in compliance with other Federal, State and local laws and regulations.

5.3 How is the information transmitted or disclosed?

It is disclosed through the use of printout or electronic media such as CD's for diskettes.

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

The information is to be used only for official purposes and tax information is subject to the disclosure restrictions in 26 U.S.C. 6103. All CD's, printout, and disk are marked with "FOR OFFICIAL USE ONLY".

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

Not aware of any.

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

Not aware of any.

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

None.

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?

A notice is placed into the Federal Register upon the creation of a form/application and with every “major revision” of the forms/application in conformance with Federal law and policy.

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

Yes, they do, but declining to provide some of the information may delay or jeopardize the approval of the form/application. Those items that are considered optional are indicated on the forms/applications. The forms specifically read: “Failure to supply complete information will delay processing and may result in denial of the application.”

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?

Yes, the individual completing the forms certifies that he/she is consenting to the fact that the information provided is true, correct and complete and that he/she authorizes DOJ to examine the necessary records associated with the application, and disclose them in conformance with Federal law.

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

There are no risks associated with the notice provided.

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?

The individual can request copies of any information on file through the Freedom of Information Act, subject to the exemptions set forth therein. They can also file a form to amend the information they previously provide, such as change of address, change in name of business or individual.

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

Through the regulations, seminars, newsletters and direct inquiries.

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

N/A.

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.

An individual whose application has been denied based on information provide can request an hearing before an ATF Hearing Officer (in the case of firearms) or an Administrative Law Judge (in the case of explosives).

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?

Employees of the Bureau of ATF.

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. Yes contractors currently perform two functions within the FESD. They are data entry clerks, or customer service representatives. Copies of their contracts can be obtained from the Chief, Firearms and Explosives Services Division. The data entry clerks are all assigned the roles of “clerks” within each automated system and are responsible for the initial entry of the information contained in the form for each system. The customer services representatives are all given a read only access and are responsible for receiving telephone inquiries received in each branch of the FESD.

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

Yes. User roles are used to determine what privileges are performed by users of the system. The user roles are based on the responsibilities of the employees. All the FESD systems have a “read-only role”.

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

Users must request access on ATF Form 7200.1. The 7200.1 Forms must be signed by the requestors’ supervisor, and the owner of the systems, who determine what user roles a requestors are given.

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

The system owner will determine the role to be granted to the requestor based on their areas of responsibility. The user completes the 7200.1, which is then signed by their supervisor. It is forwarded to IDS for processing. IDS forwards a copy to the system owner for approval, user role assignment or verification, and signature

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

Lists of users and their roles are provided the designated security officer and the system owners of each system on a quarterly basis for validations. The reports are validated against the access request forms that are maintained on file for each application, by the system owners, designated

security officers or local administrators. Each automated system has audit history tables that record the userid, date and time when records are created and modified.

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

User training is provided for all new employees and with every new release of the system, in which privacy related issues are discussed. Also every employee is required to take mandatory Information Security Training.

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

Yes. 09/30/2003. Recertification of FIT has begun and is and is anticipated to be completed within the next couple of months.

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

None.

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, a cost benefit analysis and feasibility study was done. Copies are on file in the Firearms and Explosives Services Division.

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

Every new system or revision to any existing system within ATF is cleared through the ATF's Information Systems Security Officer (ISSO) prior to implementation.

9.3 What design choices were made to enhance privacy?

Designs were based on recommendations from the ISSO's Office. Each automated system must receive accreditation prior to its being placed in production. Upon each subsequent release/modification of the application, the application must be reevaluated by the Issue's office. Design choices are also based on the latest technological advances available.

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.

ATF Faces Technology Challenges in Performing Firearms Mission

- Applications not ready to meet upcoming e-Government mandates
- Information locked into separate "stove pipe" applications
- Two dozen separate software applications for firearms
- Application maintenance and support is resource intensive

FIT Goals:

- Easily access all ATF information by individual, firearm or business
- Deploy web-based tools to interact with citizens, industry and law enforcement agencies
- Reduce the cost to maintain and support firearms applications
- Pull separate software into 4 integrated applications:
 - Licensing (FE Services Division)
 - Tracing (National Tracing Division)
 - Enforcement (Brady Branch)
 - Analysis (EPS Directorate)

FIT Benefits –

Increased Productivity and Service

- Automated processes will reduce workload, increase productivity and better support workload surges
- Increased service levels, consistent service delivery and online application submission will improve the quality of ATF relationships with those the Bureau monitors and serves.
- The processing efficiencies include
 - Improved consistency across applications
 - Simplified tracing processes and access to trace results
 - Enhanced data validation and error handling/reconciliation
 - Online status reporting Increased reporting analysis processing speed
 - Increased participation by industry members
 - Increased customer satisfaction
 - Increased transaction speed for ATF and industry members Improved record keeping efficiency and data analysis opportunities
 - Improved information benefits to the public, Congress, the Administration and other government agencies.

Intelligence Sharing

Information will be available to parties who previously had to do a manual request (i.e., field agents) Different data sources will be available for complex querying as well as trend analysis (e.g., view all activity for a particular licensee simultaneously with any pending applications) Analysis capability is enhanced with FIT delivering both new data sets on which to report, as well as increasing the value of analysis performed on existing data sets.

Reduced Support Costs

The costs of printing the forms required to be filed by industry members will be dramatically reduced with the electronic submission portion of this investment.

Processing Efficiencies Logic is repeated in multiple applications and is inconsistent across applications a single logic change in one system requires multiple heat tickets to incorporate changes in the affected systems.

Electronic forms submissions and acceptance System Maintenance cost to support the current fat client applications start at 12,096 and increases at approximately 5 percent annually. A result of the change from a client server based system to a three tier architecture that supports both web based and client desktop applications is a decrease in systems maintenance cost over the FIT life cycle, which is ten (10) years. The reasons for the decline in maintenance cost fall into three categories data will be centrally located the three tier architecture will allow for adding additional functionality efficiently without disruption shifting away from the fat client will minimize efforts to perform maintenance for individual users.

Security

Heightened Security Consolidating data retrieval or entry into a single access point with consistent security policies implemented across each point will lead to increased data security.

Audit trails enhance security

Improved Data

Currently data that is entered into the FEA systems is not always validated in a consistent fashion and errors are not always prevented to the fullest extent practicable. This investment will dramatically reduce the error rate by scrubbing the current data within the systems (insuring uniformity in new database), consolidating and integrating the systems and implementing entry point automated data validation and rules processing.

Information captured in these applications is inconsistent and cannot be validated from one system to the next. Data entry accuracy will increase, reducing errors and improving service.

Responsible Officials

/signed/

LeeAlston-Williams

Firearms and Explosives Services Division

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

Approval Signature Page

_____ <<Sign Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice