Privacy Impact Assessment
for the

Bomb and Arson Tracking System

BATS

September 7, 2006

Contact Point
Jose Vazquez
US Bomb Data Center
OSII
202-648-9040

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

Introduction

The United States Bomb Data Center (USBDC) developed the Bomb, Arson, Tracking System (BATS) to facilitate and promote the collection, sharing and diffusion of intelligence information concerning fires, arsons, and the criminal misuse of explosives. BATS is a web-based incident collection and sharing program. It is an automated incident reporting system that streamlines information that is reported, retrieved and archived by valid law enforcement agencies and investigators. The data in BATS contains information from fires, arsons and the investigation of explosives. BATS is used as a case management system by law enforcement organizations all around the U.S. BATS facilitates the connection of the nation's fire and explosives investigations through the use of reliable, stable and secure information and communications technologies.

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?

BATS provides law enforcement agencies the ability to enter, retrieve, and share information concerning active and closed investigations; it provides general management statistics, and it performs queries on the local, state and national levels. The BATS program includes the ability to track motives, trends and similar explosive devices. Furthermore, BATS includes the ability to track incidents spatially, generates a number of useful law enforcement reports, and appends incident based images (.jpg, .tif, etc) to individual incident records. It includes personal identifier information such as birth date, social security number and address associated with suspects, witnesses, and victims.

1.2 From whom is the information collected?

Law enforcement organizations with proper authority in BATS may create, read, edit, modify, search and close incidents containing their own data, which is drawn from their investigative actions including crime scene processing, and interviews of suspects and witnesses. State and local law enforcement agencies that investigate arsons, bombing and the criminal misuse of explosive collect the raw data via approved methods and use BATS as a record management mechanism.

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 BATS system establishes a single location that facilitates and promotes the sharing of information between ATF and approved federal, state and local law enforcement organizations. Data includes locations, accelerants, explosives, suspects and their personal identifier data, and many other details necessary for an investigation. ATF is able on a nationwide basis to query information contributed by other BATS participants. It includes the ability to track motives, trends and similar explosive devices. For example, the multiple Alabama church arsons in 2006 that were investigated utilized BATS as the information repository. It provides a comprehensive case management system for the individual organizations and a trend and correlation tool for the USBDC and its partners.

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

ATF enforces the Federal explosives laws, 18 U.S.C. Chapter 40. Pursuant to section 846 thereof, ATF was authorized to establish a national repository of information on incidents involving arson and the suspected criminal misuse of explosives. All Federal agencies having information concerning such incidents are required to report the information to ATF. The repository also contains information on incidents voluntarily reported to ATF by State and local authorities." In addition, the Attorney General, in a memorandum dated August

11, 2004, directed Department of Justice components to consolidate their arson and explosive incidents databases under the ATF.

State and local law enforcement-related agencies must execute a Memorandum of Understanding and Rules of Behavior Agreement, as well as completing training on how the system is used. Because it is a law enforcement system, all data must be collected according to legally defined methods.

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 majority of the data collected and mined in BATS is directly tied to arson and illegal use of explosives investigations, and there are some personal identifier related fields. To avoid misuse, access to the system and the data is tightly controlled, encrypted, and monitored.

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.

BATS is foremost a case management system. It provides simplified case tracking, statistics, trending, and resource management of investigatory elements. Law enforcement agencies use the data to pursue their cases for investigation and prosecution. At the ATF level, all the data can be aggregated to determine trends, movement, and possible links that would not be possible from the state and local level.

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.)

No

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

The contributing organizations have the duty and responsibility to make reasonable efforts to ensure that information in BATS is accurate, complete, timely, and relevant. It is up to the investigator entering data into his cases in BATS to ensure the accuracy of that data. Law enforcement understands that if the data is inaccurate, they will be damaging cases and potentially compromising legal action. Most of the data is fact-based and relevant to past or present cases. Basic database data integrity controls are in place to control field entries and record audits, system logging, and role and permission controls are deployed. .

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)?

BATS data has archived all of its data since its inception a draft of the retention schedule will be available in the near future.

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.

Access to this data is extremely limited and tightly controlled. Each user has been through a "clearance" process. Users have to connect using authentication and an encrypted connection, and the data itself is segmented by many rules of roles and permissions. Detailed local case data entered in BATS can only be seen and manipulated by the person who inserted it and his supervisors unless the material is marked "unrestricted". Juvenile data is automatically marked as restricted. Other BATS users can browse general data based on the rules associated with their IDs. The system has database auditing and system logging as well as network based intrusion detection systems.

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?

FBI, US Attorneys and Criminal Division may need access to some of the data in BATS in connection with their official duties.

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

FBI uses the BATS system to analyze trends and search for potential patterns that relate to their investigations. Cases are marked by the originator as either Restricted or Unrestricted. Any case marked Unrestricted can be queried by other authenticated BATS users. However any subject labeled as a "juvenile" is automatically designated as "Restricted".

4.3 How is the information transmitted or disclosed?

Information is transmitted across encrypted links.

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

Given the limited distribution, controls on access and limited data collected, the risk is mitigated to the extent possible.

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?

External users consist of duly recognized Federal, state, and local law enforcement organizations.

5.2 What information is shared and for what purpose?

The USBDC was created to facilitate and promote the collection, sharing and diffusion of incident information concerning fires, arsons, and the criminal misuse of explosives per Federal law. BATS was designed to promote incident data sharing for Federal, state, and local arson and explosives investigators. Users may run user-defined queries which will return a line item which the user can view if the case is within the user's local organization, or if the case is "Unrestricted" by a user from an outside agency. If a user runs a query that finds data in a "Restricted" case, he will receive a response that the subject exists but is restricted. The information is shared to increase the chance that law enforcement has all the data possible to track and thoroughly investigate a case.

5.3 How is the information transmitted or disclosed?

The information is transmitted across an encrypted link.

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

The Memorandum of Understanding that all external users must have in place, covers the importance of the security and privacy of the data that may be shared. The Rules of Behavior are also signed and cover this topic.

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

Users are required to participate in extensive BATS User Training before being granted access.

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

Standard system logging and authentication methods are in place to control access and document what participants do while connected. While personnel are logged into the system, their database accesses, queries etc are logged and reviewed.

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

The data maintained in BATS is added by each responsible entity. It is up to them to ensure at their end that their information is not compromised. ATF acts as the support organization that makes the combined database possible and, from that angle, protects the information. Incident investigation data by its nature is "law enforcement sensitive" and requires controls due to the damage that improper disclosure could cause. Sharing data with external organizations poses Different challenges which US BDC has sought to mitigate by applying technical, operational and management controls on access and activity as specified in the National Institute of Standards and Technology standards and evaluated according to Federal Information Security Management Act (FISMA) including the method used for sharing data with the external entities. There could be an increased risk of inadvertent misuse of information due to the larger audience. The impact on the privacy of individuals, however, is no greater than that of any current case analysis and investigation that includes the same data obtained manually from other law enforcement agencies.

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?

The information pertaining to individuals is based on their suspected criminal involvement or as witnesses or victims in criminal case investigations and law enforcement concerns. This is case data collected by Law Enforcement in the performance of their duties. This information is within the scope of the Privacy Act exemption for law enforcement records pursuant to 5 U.S.C. § 552a(j2).

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

There is no general opportunity to decline use of this information because the information contained in the system is existing data that was lawfully gathered previously and maintained based on law enforcement statutory authority.

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?

No. This is law enforcement data. There is no general opportunity to consent to particular uses of information because the information contained in the system is existing data that was lawfully gathered and maintained based on law enforcement authority pursuant to an investigation.

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

There is no notice required per the exemptions defined in the Privacy Act for criminal investigation reporting. Data was collected via authorized investigation techniques.

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?

There are no procedures to allow individuals the opportunity to access or redress their own information in BATS because this information is within the scope of Privacy Act exemption for law enforcement records set forth in 5 U.S.C. 552a (j) (2).

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

They are not notified, due the Privacy Act exemption described in Section 7.1.

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

Anyone can seek redress via the filing of a lawsuit in Federal court. However, a judge would require that the individual has exhausted all forms of administrative process before considering the merits of the lawsuit.

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.

This aspect of the Privacy Act is not applicable to BATS. During an investigation, the individual is not offered any opportunities to contest the information in the system if it is collected outside of official statements made and acknowledged by the individual in question. The information is placed into the database after it has been collected per law enforcement standards. Personal identifier information is only used in the case of prosecution and in that event, the individual and counsel will have access to the data for review. ATF has determined that there is no adverse impact on the due process rights of individuals caused by the operation

and use of the BATS system as the data was previously collected via legally appropriate means.

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?

Any recognized US law enforcement-related organization can apply for access to BATS. They must have background checks and supervisor recognition of a "need to know" in order to obtain credentials for the system.

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.

The ATF operations contractors have access to this system in terms of supporting its day to day operations, backups, disaster recovery etc. These contractors are subject to security agreements and information security training. Questions concerning the contract may be addressed to the ATF Contracts Office or Information Systems Division.

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

Yes. There are several roles in place in BATS so as to provide enough access without providing complete "freedom to roam." There is a BATS administrative role which is used to perform server and application support but cannot be used to access system records the way a user can. There are several user level roles – the standard organizational based user account can add, modify and delete records that were invoked by that user in that role. There is a BATS "ORI" administrative account which allows the supervisor to modify that organization's user account data and gather statistics of interest to a manager. There are specialty read-only roles for ATF partners such as DHS explosives trainers. The

data categorization as Restricted or Unrestricted also helps minimize accessible data.

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

The procedures for requesting, obtaining, and maintaining access to the system are documented in the BATS operations and maintenance manuals, the Rules of Behavior, and supported by DOJ and ATF information security policy.

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

Individuals have specific roles that limit them to the data they enter as defined in the procedures. Auditing and system log review are on-going activities. Additionally, Oracle and system audits are conducted at least monthly to check for vulnerabilities, weak passwords, undocumented system changes, and policy deviations. Regular reports are run on account activity and reviewed for inactivity and other anomalies.

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

Access is gained after crossing multiple firewalls, encrypted communications, network based intrusion detection systems. Activity is logged and reviewed. There are roles and views defined to limit data access. Authorized users can only manipulate their own data unless special documented access is implemented. Data is marked as “restricted” or “unrestricted” at the data owner’s discretion which controls data viewing.

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

ATF personnel must participate in several training programs annually. These programs include ethics, information security, and investigation techniques which overlap covering aspects of privacy rights and obligations. External users participate in an extensive training program for BATS use, security, and privacy.

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

Yes. C&A was last completed on January 5, 2005 and will expire on January 5, 2008

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

Because the data is law enforcement sensitive, its security is a key point within ATF system management. The possibility of power users or administrators being able to access information inappropriately has been addressed by having forced system and audit logs copied off in real time to a secured logging server where the data is reviewed daily for anomalies. If logs do not arrive as expected, alerts are generated. The intrusion detection systems are monitored for unusual traffic, especially traffic going to the Internet. However, there is always the possibility that authorized users can retrieve their own data and use it in irresponsible ways.

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, assorted technologies and designs were assessed for their ability to meet functional requirements.

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

When developing system requirements, system and data security were included. Because the system heavily supports external users, there was considerable review as to how to protect their data from inappropriate access. ATF has a well

developed Configuration Management and Data Management process in support of the System Development Life Cycle. Every stage requires a security review as well as configuration and data management validation. Data integrity is partially covered by legal processes for collecting law enforcement data and largely controlled by actual field parameters and data integrity checks. Since the investigative data is sensitive but unclassified (SBU), privacy is assured by many system access limits and controls. Security is reviewed at all stages of the SDLC in terms of ATF's security checklists and scans to ensure any design is FISMA-compliant and documented. These requirements are part of the system design documentation and during development it cannot be promoted if these steps are not addressed.

9.3 What design choices were made to enhance privacy?

Strict database security controls such as limited views were built in from the beginning. User populations are carefully checked and limited in system use. Queries are limited so that users cannot indiscriminately browse data. The addition of an application level audit table ensured even deeper tracking of user actions.

Conclusion

The BATS system contains criminal law enforcement sensitive records. It is used by investigators across the US to track and coordinate their own cases. BATS was developed to provide considerable autonomy to these agents and their supervisors where they have full editing rights to their own data only – yet all activity is tracked in system, database, and application audit logs. At the same time, it allows queries for producing trending and methodology questions, without allowing direct access to the data. This is a Federal E-Gov initiative that provides better service through an Internet based web application. Because it is Internet-based, considerable thought and effort went into applying security in depth through authentication and technical controls such as firewalls and intrusion detection systems, all working together to protect this critical law enforcement tool. Because the point of BATS is to collect and disseminate investigatory information nationally, some aspects of the Privacy Act are exempted in order to allow the agency to pursue its mission efficiently. However, securing the data and ensuring it is used properly is critical to successful law enforcement and ATF has implemented a solution that it believes controls those threats to the extent practicable and possible in today's technology.

Responsible Officials

__/signed/_____ _9/7/2006__

Jose Vazquez
Chief, US Bomb Data Center
Bureau of Alcohol, Tobacco, Firearms, and Explosives

Date

Approval Signature Page

_____ _____

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

Date