Privacy Impact Assessment
for the

International Bombing Incident Program
DFUZE

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 US Bomb Data Center (USBDC) sponsored and participated in a project - the International Bombing Incident Program (IBIP) that included the United Kingdom, Mexico, and Columbia. The intent was to develop a commercial of the shelf (COTS)- application that could be used by various International Bomb Data Centers to manage explosives based incident information. In an effort to facilitate this task, IBIP selected the DFuze application to provide law enforcement with the tools necessary to produce a global product.

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?

It has an explosives search system that enables law enforcement and other government organizations to collect, store, and retrieve data relating to incidents involving explosive devices and related case information. Each agency will be able to populate DFuze with organization-specific law enforcement intelligence as well as have the ability to obtain data from other agencies, if permitted by the contributing agency. It includes device details, names, addresses, and birth dates of suspects, witnesses, and victims and organizations involved pursuant to the investigation.

1.2 From whom is the information collected?

The ATF implementation stores data ATF has received from its law enforcement organizations, international bomb data centers and allies. Other countries representing worldwide law enforcement organizations and international bomb data centers maintain their own copies and share some of the data. This data is obtained as a result of law enforcement investigations, including crime scene processing, and interviews of suspects, witnesses and victims; and information obtained from print and news media.

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 purpose of DFUZE is to capture information about international incidents involving explosives and terrorist organizations. DFuze establishes an information highway that facilitates and promotes the sharing of information between ATF, participating members, and National Bomb Data Centers worldwide. DFuze also serves as a reference library for research and training. ATF agents and analysts operating in an international capacity are key users of this system**.**

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

Pursuant to 18 U.S.C. 846, ATF is mandated to create a national repository of arson and explosives incidents.

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.

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

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.

DFuze information is used as reference material for agents working on explosives cases nationally and internationally. Although data is shared internationally, there are subsets of law enforcement investigatory data which may not be released while an investigation is pending. The library provides background information on explosives. Terrorists know no boundaries and the shared intelligence contained in DFuze is strategic for monitoring international threats that may impact the US and its interests.

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 agencies have the duty and responsibility to make reasonable efforts to ensure that information in DFuze is accurate, complete, timely, and relevant. It is up to the investigator putting data into DFuze to ensure the accuracy of that data. Agents and analysts understand 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 explosives incidents. 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)?

The DFuze system owner archives all data associated with explosive incidents and related material to include videos, images, and technical information. Official record retention decisions are awaiting further information from the program office as to the applicable retention schedule.

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 an extensive "clearance" process which ensures, among other things, that users correspond to bona-fide law enforcement-related entities. Users have to connect through the CITRIX front end authentication and the data itself is segmented by many rules of roles and permission levels. (CITRIX software that provides a timeshared, multi-user environment for Unix and Windows servers. Citrix Presentation Server uses the ICA protocol to turn the client machine into a terminal and governs the input/output between the client and server.) The system has operating system, database and application logging in use as well as network based intrusion detection systems installed. The application audit logs capture every query and record change made in DFuze.

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 DFuze or require access to its explosives library for use in their official dutes.

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

Outside of ATF investigations, FBI may need information to help them identify an explosives case they may be reviewing by looking for similar materials, techniques and other background information. FBI is heavily involved in counter-terrorism and works extensively in the International sphere. US Attorneys may need the reference material to support a case in court.

4.3 How is the information transmitted or disclosed?

Information is transferred on encrypted DVDs.

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

Since most of the information is reference material and available from disparate sources, it does not pose an increased risk by existing in DFuze. Given the extremely limited distribution, controls on access and limited data collected, most of the risk is mitigated.

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?

DFuze is a COTS product used by a number of international organizations involved with explosives and law enforcement. Although ATF is the principle user of its implementation of DFuze, there are some external organizations that under certain conditions may receive a copy of portions of the database. Scotland Yard is the principle external authority requesting updates, although the international bomb centers and law enforcement arms of foreign governments may request updates on some of the information.

5.2 What information is shared and for what purpose?

Within ATF, DFuze is used as a reference to explosives, known terrorists and historical data. The system contains a range of information about non-U.S. citizens and other persons who are referred to in potential or actual cases or matters of concern to the law enforcement communities, e.g. suspects or known associates of suspects. Examples of information in the system include: suspected criminal activity, and other personal information (i.e. address, phone, social security number, etc.) Subsets of this data may be exported for external users. However, no current investigation data is shared.

5.3 How is the information transmitted or disclosed?

The data is transferred to DVD and encrypted. The key is transmitted separately to the designated recipient via an encrypted file.

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

As the data is considered law enforcement data, it is treated internationally as law enforcement sensitive and handled according to international standards and protocols.

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

Since outside agencies are running their own implementations of DFuze and performing law enforcement functions they are trained according to their organization's policies. As an example, Canada has its own implementation of the Federal Privacy Act and they publish IPAs that address a number of their law enforcement systems. Privacy controls vary internationally and in some countries are considerably stricter than those of the U.S. .

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. ATF cannot monitor what external entities do with the data after they receive the DVD. 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.

Incident investigation data by its nature is "law enforcement sensitive" and requires controls due to the damage that improper disclosure could cause. ATF has sought to mitigate these risks by applying technical, operational and management controls on access and activity as specified in the NIST standards and evaluated according to FISMA. The external organizations with which ATF shares this data are not accessing ATF's version of DFuze. Users are made aware

of the law enforcement sensitivity of the data and improper usage or usage or transference would jeopardize future access to the system. They maintain their own versions totally independent of the ATF system. There could be an increased risk of inadvertent misuse of information due to the larger audience of DFuze users. The impact on privacy of individuals, however, will be the same as the impact of any current case analysis and investigation that includes the same data obtained manually form 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 involvement with criminal case investigations and law enforcement concerns. This is generally case data previously collected by Law Enforcement in the performance of their duties and according to the rules of their native jurisdictions. Because the information is mostly referential and historical in nature and this isn't the primary residence of that data, yet a part of law enforcement efforts, the individual is not contacted. This exemption is specified in the Privacy Act of 1974, 5 USC section 552a (j2).

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

No. There is no general opportunity to decline providing this information at this point because the information contained in the system is existing data that was lawfully gathered and maintained based on law enforcement 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 case data. There is no general opportunity to consent to particular uses of information because the information contained in the system is existing data, and was lawfully gathered and maintained based on law enforcement authority.

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 given to individuals for DFuze data per the exemptions granted in the Privacy Act for criminal investigation reporting.

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 Dfuze. As defined in chapter 5 USC 552a (j) (2), according to the Privacy Act of 1974 "General exemptions … The head of any agency may promulgate rules, in accordance with to exempt any system of records within the agency from any part of this section **if the system of records is maintained by an agency or component which performs as its principal function any activity pertaining to the enforcement of criminal laws**…"

"(b) This system is exempted from the following subsections for the reasons set forth below:

(1) From subsection (c (3) **because making available to a record subject the accounting of disclosures of criminal law enforcement records concerning him or her could inform that individual of the existence, nature, or scope of**

an investigation, or could otherwise seriously impede law enforcement efforts."

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

They are not notified, due to the exemption granted by the Privacy Act section 552a (j) (2) covering law enforcement investigations.

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

When a case goes to court, the defendant can address items in question in the United States Federal or State court in question**.** Otherwise, it will be handled according to the protocol of the country involved.

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 of 1974 is not applicable to DFuze for the reasons set forth above. ATF has determined that there is no adverse impact on the due process rights of individuals caused by the operation and use of the DFuze 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?

Only ATF personnel have direct access to the system. They must have in-depth background checks and supervisor recognition of a "need to know" in order to obtain credentials for the system. Other law enforcement entities such as Scotland Yard share information via pre-arranged data selections copied to encrypted DVDs.

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 only Department contractors are the ATF operations support contractors who perform day to day operational support, backups, disaster recovery etc. 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 a number of roles, each of which only allows certain types of system interaction. Administrator allows operational support. Then there are eight more roles: Edit – existing records, Add – add records, Compliance – validates that the record is acceptable, Read Only, Print – specific to printing and chronicling those requests, Export – to allow export of a transmission file, Import – to allow a transmission file to be imported, Delete, and Transmit which allows the building and transmission of DFuze 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 DFuze operations and maintenance manuals, ATF network access procedures, 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 affect 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. Account activity is monitored for inactivity and other anomalies.

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

Authorized users can only access their own data unless special documented access is implemented. Access is gained after crossing multiple firewalls, encrypted communications, network based intrusion detection systems. Also, activity is logged and reviewed. There are roles and views defined to limit data access. DFuze incorporates a system user audit process that logs every query, and record action taken by a user to provide further oversight. In addition, the database is segmented so that even data exports can be tailored to the minimum data required providing support to external law enforcement organizations

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.

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 issue within ATF system management. The possibility of power users or administrators being able to access information inappropriately has been addressed by having system and audit logs copied off in real time to a secured logging server where the data is reviewed daily for anomalies. The system administrators and database administrators do not have access to the logs on the secured server. 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 an unauthorized manner.

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. An internationally successful explosives COTS product was chosen for its track record of securely storing data while providing the ability to promote information sharing among law enforcement organizations.

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 most of the data is historical and comes from other sources, it is dependent on the original source being accurate. The COTS database was designed to provide assorted field integrity checks as well as requiring a wide range of logging options. Using the proven law enforcement COTS product ensured that concerns with data integrity, data protection, and general security were inherent in the product. Field reports indicate that the data submitted has proven accurate.

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. Output is encrypted to a DVD with a separate password protected key file.

Conclusion

DFuze contains international criminal law enforcement sensitive records. The DFuze system offers ATF's international explosives investigators an unparalleled opportunity to have historical and current research readily available. With the constant flow of terrorist activity across national

boundaries, sharing of background information is critical to providing law enforcement with the information they need to successfully stem this activity. Because the point of DFuze is to collect and disseminate investigatory information internationally, it is exempt from some aspects of the Privacy Act of 1974. Nevertheless, 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 these threats to a reasonable degree 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