Privacy Impact Assessment
for the

Arson and Explosives Incident System
AEXIS

June 27, 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) 514-004

Introduction

In 1996 Congress established the Arson and Explosives National Repository (AENR) (now known as the US Bomb Data Center) and made it a clearinghouse for information concerning bombings, arsons and the criminal misuse of explosives. The U.S. Bomb Data Center (USBDC) uses the AEXIS application to collect that information. AEXIS is a flexible database that aids agents in investigating and prosecuting cases involving arsons and explosives activities. The AEXIS 4.5 application assists in the collection, maintenance, evaluation, and dissemination of incident information useful in determining criminal activity patterns, trends and motives. The interface provides the user with a file structure to organize data into logical categories, share incident data, use automated incident review functions, automatic report generation, ad hoc query functions and generate statistical data. The information contained in AEXIS is sensitive but unclassified (SBU), data that is protected by the applicable exemptions of the Privacy Act of 1974 and the Freedom of Information Act (FOIA). This information is available for statistical analysis and investigative research by scholars and to the law enforcement community. Contributors of information contained in the AEXIS database include Federal Bureau of Investigation (FBI), ATF, and National Fire Incident Reporting System (NFIRS).

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 AEXIS 4.5 application assists in the collection, maintenance, evaluation, and dissemination of arson and explosives related incident information. It is a useful in determining criminal activity patterns, trends and motives. It includes data used in support of recently enacted amendments to the Federal explosives law, 18 U.S.C. Chapter 40 which require any person who wishes to transport, ship, cause to be transported, or receive explosive materials in either interstate or intrastate commerce to first obtain a Federal permit issued by ATF. Personal identifier data such as name, social security number, date of birth, arresting agency, persons-role (suspects, witnesses, and victims) in the incident identified during the course of an investigations. . Authorized AEXIS users are also able to submit explosive traces,

and search and analyze existing traces.

1.2 From whom is the information collected?

The information contained in AEXIS originates from reports written by special agents and investigators throughout ATF and is recorded in the NFORCE case management system, and of which is the result of investigations and associated interviews of witnesses, suspects, crime scene processing, and through the processing of explosives trace requests submitted to ATF by both ATF investigators, and law enforcement agencies outside ATF.

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?

In 1996, Congress established the Arson and Explosives National Repository and in 2002, the FBI bomb data center was transitioned to this group which is now known as the U.S. Bomb Data Center. It is a clearinghouse for information concerning bombing, arsons and the criminal misuse of explosives. The US Bomb Data Center uses the AEXIS application to collect that information.

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. Because it is a law enforcement system, all data collected must be done 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 AEXIS is directly tied to 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.

The AEXIS 4.5 application assists in the collection, maintenance, evaluation, and dissemination of information useful in determining criminal activity patterns, trends and motives. To maximize effective enforcement of the Federal explosives laws; AEXIS improves ATF's ability to retrieve information about explosives information purchased with limited use permits/coupons from the Federal Explosives Licensing System and relate it to existing explosive traces in AEXIS.

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?

ATF has the duty and responsibility to make reasonable efforts to ensure that information in AEXIS is accurate, complete, timely, and relevant. It is up to the

analyst entering data in AEXIS to ensure the accuracy of that data. Agents understand that if the data is inaccurate, they will be damaging investigations and prosecutions. Most of the data is fact-based and relevant to past cases. Basic database data integrity controls are in place to control field entries. 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)?

AEXIS data is archived in accordance with NARA requirements. It is maintained according to ATF RCS 201, Item 28.

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 limited and controlled. Users have to connect using authentication and the data itself is segmented by many rules of roles and permissions. Procedures exist for archiving the data and analysts review all data to be input into the system for reasonable accuracy.

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 AEXIS in connection with their official duties.

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

ATF uses the AEXIS system to analyze trends and search for potential patterns that relate to their investigations. ATF users can view high level information across the system, but it is restricted and they cannot see specifics unless they are looking at data they have entered into the system. DOJ components may request information and according to law enforcement protocols will receive it.

4.3 How is the information transmitted or disclosed?

Access to the system requires a specialized client and AEXIS does not have any connections outside the private ATF network. Law enforcement requests for information are provided via unalterable portable document format (PDF).

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

Given the limited distribution, and controls on access, the risk is mitigated to the extent possible. This data is available from individual primary sources which would be normally used for investigation and prosecution. AEXIS has a strategic purpose in providing statistical data and trends which do not involve personal identifier information.

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?

Currently, there are no external entities accessing AEXIS data. The USBDC performs updates and queries and prepares reports as necessary in response to requests from external law enforcement organizations. The public may access generic statistical reports.

5.2 What information is shared and for what purpose?

The USBDC developed AEXIS to facilitate and promote the collection, sharing and diffusion of intelligence information concerning fires, arsons, and the criminal misuse of explosives per Federal law.. Reports may be provided to law enforcement concerning specific cases, trends, and statistics in AEXIS, but only general statistics are released as public information.

5.3 How is the information transmitted or disclosed?

Generic statistical information is presented via the web interface and does not provide any case particulars and does not pose a threat to individual privacy concerns. Law enforcement queries are answered via unalterable Adobe PDF files and handled according to local protocols.

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

Once the data is shared, there are no additional agreements in place. However, being law enforcement sensitive, the requested information is bound by standard law enforcement data handling requirements.

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

There are no external users. ATF users are required to participate in ATF Security Awareness training and AEXIS training before being granted access.

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

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

There is no direct external sharing of AEXIS data. However, incident investigation data by its nature is "law enforcement sensitive" and requires controls due to the damage that improper disclosure could cause. USBDC has sought to mitigate these risks by applying technical, operational and management controls on access and activity as specified in the National Institute of Standards and Technology (NIST) standards and evaluated according to FISMA (Federal Information Security Management Act) including the method used for sharing data with the external entities. Contributing organizations outside of ATF will provide sensitive but unclassified (SBU) data. All data submitted will be uploaded by ATF. Since ATF performs the queries on behalf of external organizations, all information is reviewed for appropriate release before being provided to the requestor. There could be an increased risk of inadvertent misuse of information due to the larger audience but since no external sources have direct access to the database, the threat is mitigated to the extent possible.

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 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). Additionally, AEXIS is not a primary data source.

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

There is no general opportunity to decline to provide this particular information because the information contained in the system is existing data that was lawfully gathered 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 that was collected through appropriate means and AEXIS is not the primary source of 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.

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 AEXIS 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). However, once the case is closed, individuals can use FOIA or the court system to address any potential discrepancies.

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 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 (FOIA requests) 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 AEXIS. During an investigation, the individual is not offered any opportunities to contest the information in the system. 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 AEXIS system as the data was previously collected via legally appropriate means. The reports generated for non-ATF requests are either in support of an investigation or statistical in nature and do not include any personal identifier information.

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 AEXIS system. They must have background checks and supervisor recognition of a "need to know" in order to obtain credentials for the system. The US Bomb Data Center analysts are the main users of 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 Service Division.

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

Yes. AEXIS uses a set of roles to provide access yet limit that access. These roles are Admin, Senior, Junior and Read Only.

- ADMIN: User has full access to all AEXIS functions, to include the ad hoc query tool, lookup table maintenance, and user maintenance.
- SENIOR: User has ability to insert and update an incident. User cannot delete records or incidents, or perform maintenance or queries.
- JUNIOR: User has ability to insert and update an incident. User cannot delete records or incidents, or perform maintenance or queries. Junior level incidents will be flagged for review.
- READ ONLY: User has read only access to AEXIS, meaning they can view information but cannot insert or update information.

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 AEXIS user manual, ATF network access procedures, the Rules of Behavior, and supported by DOJ and ATF information security policy. These procedures include account submission, user vetting, supervisor sign-off and regular account reviews.

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?

Authorized users can only access data as provided by the roles and privileges they have been assigned. Access is gained after crossing multiple firewalls, monitored by network based intrusion detection systems, and activity is logged and reviewed. There are roles and views defined to limit data access. In addition, data loaded for external entities and reports generated for external requestors are reviewed and approved before submission.

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 May 23, 2005 and will expire on May 23, 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. The data is only accessed by a small group of carefully cleared personnel reducing the likelihood of abuse.

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. 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 covered by applicable 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.

Conclusion

The AEXIS system is tasked to provide critical arson and explosive related information to ATF and disseminate related information to other government law enforcement agencies in a timely manner. The system contains criminal law enforcement sensitive records. Failure to protect this information could result in a severe negative impact on law enforcement investigations, delays in time-critical activities and judicial proceeding. Further, prolonged system outages may result in a backlog of information requests.

There are**:** management controls such as training and Rules of Behavior**;** operational controls such as sufficiently complex 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 AEXIS is to collect and disseminate investigatory information nationally, some aspects of the Privacy Act are exempted in order to allow the agency to perform its law enforcement responsibilities. However, securing the data and ensuring it is used properly is also critical to successful law enforcement and ATF has implemented a solution that it believes controls those threats to the degree practicable and possible in today's technology.

Responsible Officials

_/signed/_____ _9/7/2006_____

Date

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

Approval Signature Page

_____ _____

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

Date