
Privacy Impact Assessment

# National Field Office Case Information System (NFOCIS)

**May 31, 2006**

**Contact Point**
**Robert W. Tatro**
**NFOCIS Branch**
**Office of Strategic Intelligence & Information**
**202.927.7288**

**Reviewing Official**
**Jane C. Horvath**
**Chief Privacy Officer and Civil Liberties Officer**
**Department of Justice**
**202.514.0049**

# Introduction

The National Field Office Case Information System (NFOCIS) is the case management system used by the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), an agency of the U.S. Department of Justice, to document, track, and collect investigative information in support of ATF's law enforcement mission, strategic goals, program initiatives, and field activities. It serves many purposes:

a. NFOCIS provides special agents, Industry Operations investigators, and persons assigned to investigations and cases as "participants" graphical user interfaces (portals), to post data to tables in a central database repository on a single server. The user interfaces to the database are the four applications.

b. The NFOCIS applications provide field managers and supervisors with management reports and query tools to drill down into data stored in the NFOCIS database in order to measure office, field division, program, and individual performance.

c. The NFOCIS Branch provides Headquarters program offices with queries created in Oracle Discoverer to measure and report on the performance of program initiatives.

d. The NFOCIS Branch provides ATF's Budget Office with reports and data that can be reported to ATF's stakeholders, oversight entities (OMB, GAO and Congress), and the public.

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

## 1.1 What information is to be collected?

The NFOCIS System contains investigative case information relating to persons, places, charges, events, property in custody, etc. The information collection pertaining to "Persons" includes targets of investigations (suspects and defendants) as well as the names of victims, witnesses, and the names of other sources of information collected during the course of interviews in the conduct of the investigation. ATF personnel working investigations gain access to and can post data to structured data tables in the NFOCIS database via the four applications.

### 1.2 From whom is the information collected?

The information is collected primarily via witness interviews conducted by ATF field agents and investigators and other information including items of evidence obtained during the course of a criminal or civil investigation. The raw data is validated in subsequent interviews and by queries of Federal and State databases and financial databases.

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

### 2.1 Why is the information being collected?

The information is being collected in order to support investigations of:

(a) Persons suspected of being involved in criminal activities that violate Federal statutes subject to enforcement by ATF;

(b) Persons and/or businesses applying for licenses and permits to engage in activities that are subject to Federal statutes and the regulations issued there under.

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

ATF's collection of information is authorized principally under two Federal statutes:

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

Federal Explosives Laws, 18 U.S.C. Chapter 40.

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

Contraband Cigarette trafficking Act, 18 U.S.C. Chapter 114.

### 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 NFOCIS System and applications were released into production as early as FY 1999. A privacy impact analysis was performed in the late 1990s following the gathering of functional requirements and during the development and design phases. Access controls were initially imposed at the application level.

However, in preparation for Y2K and following passage of the Homeland Security legislation post 9/11 and ATF's organizational realignment from Treasury to Justice, ATF's Information Systems Security Office has identified global information security requirements for all ATF systems and ATF's Information Services Division has upgraded the information technology infrastructure to meet the information security requirements.

## Section 3.0
## Uses of the System and the Information.

### 3.1 Describe all uses of the information.

The NFOCIS System is used extensively within ATF by field special agents to collect and document criminal investigative data.

The NFOCIS System is used to collect and document leads in working a complex investigation involving either a large number of targets and/or a large number of sources of leads obtained via interviews conducted in the course of a complex investigation.

The NFOCIS System tracks via a "virtual vault" the status of items of property (firearms, explosives, currency, drugs, electronic surveillance tapes, grand jury documents) that are held physically in an ATF field office vault, seized either as evidence or as assets for forfeiture, 3rd party storage contracted by ATF, or an ATF laboratory's vault.

The NFOCIS System is used to collect civil (non-criminal) information related to entities (corporate, single proprietorship, partnership) and the individuals who have control of such entities and/or the individuals who are identified as responsible persons including under Federal statutory authority the requirement that ATF run criminal background checks for possessors of explosives. The data collection is stored to the NFOCIS database and can be queried within the applications or via ad hoc queries created in Oracle Discoverer against structured data tables.

## 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.)

Each application contains "canned", or templated management reports and a query tool that can be used to query data and to generate reports for subsequent analysis independent of the application.

Data is stored in structured data tables in a centralized database. The NFOCIS Branch uses a query tool to drill down into a "business area" that mirrors the production data in order to create ad hoc reports. This graphical user interface to a structured query language (SQL) tool, does not enable the user to alter production data.

ATF has obtained funding to identify functional requirements for a Super Query Tool that would enable the searching of data stored in different types of media. An example of an off-the-shelf software product that enables the searching, mining and collection of data from various media is Verity.

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

Information collected initially in interviews is subjective and requires subsequent validation by the special agent or investigator in order to verify its accuracy. Validation is performed via interviews of other parties including witnesses, other law enforcement personnel, searches of criminal histories in Federal and State databases, searches in Government and lawful commercial financial databases, and analyses of evidence by ATF laboratories and other experts.

## 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)?

All data is retained for official law enforcement use only. Parties outside of ATF do not have access to the data, except as authorized by Federal law. The Request for Records Disposition Authority, SF 115, Job No. NI-436-03-5 for the NFOCIS System and applications, approved 08/19/2004 and signed by the Archivist of the United States states in Subparagraph a(1) that the Disposition Schedule for agency copies of records created by users of N-Force/N-Quire is "75 years after case is closed, or when no longer needed for legal purposes, whichever is later." Subparagraph b(1) states that the Disposition Schedule for agency copies of

records created by users of N-Spect is "25 years after completion of inspection, or when no longer needed for agency business, whichever is later."

## 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 controls are role dependent. Based upon a person's role in the investigative business process, a comparable role is granted to the end user at the application (front end) level and at the database (back end) level. In order to gain authorized access to the NFOCIS data the end user must complete and submit an access application to a first level supervisor for review. Upon approval by the first level supervisor. ISD's Operations Security Branch ensures t user has a valid and active networked and Outlook email account. A signed "Rules of Behavior" acknowledgement form must be on file for a networkID. The NFOCIS System Owner or Designated Security Officer reviews the application. An NFOCIS system administrator creates an application userID. ISD's Operations Security Branch tasks a contractor database administrator (DBA) to create a database user account and temporary password.

When reviews of ATF programs are performed by external 3rd parties, e.g., DoJ's Office of Inspector General and the annual CFO Act review of ATF's Accountability Report and Auditable Financial Statement, the members of the audit teams work with OPRSO and ATF's Financial Management Division to obtain reports of performance data from NFOCIS. In the course of reviewing the data specific to ATF's mission and programs, the audit teams also provide ATF management with comment regarding their findings specific to the NFOCIS System. The NFOCIS Branch has strengthened information security controls as corrective actions following these reviews.

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

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

Under the One DOJ and Law Enforcement Information Sharing initiatives, extracts of closed investigative case data were shared in FY 2005, in conformance with Federal law. This marked the first and only time that NFOCIS data has been shared to the U.S. Department of Justice and made accessible to other participating agencies. Investigative data stored in the NFOCIS database is Sensitive But Unclassified and is restricted for "Official Use Only."

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

Non-grand jury data and National Firearms Act information were validated and then filtered for use by the DOJ RDeX information sharing pilot program and the DEA Fusion Center shared database initiative. ATF information is to be accessed only for official law enforcement purposes by law enforcement agencies with jurisdiction to investigate the matter in question. The filter only includes field defined data at this time.

## 4.3 How is the information transmitted or disclosed?

The extract of data was copied to a compact disk and formally released with a disclaimer and security statement requiring signature by the receiving DOJ component.

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

The risks are the same as those listed in Section 2.3. Until passage of the Homeland Security legislation, the realignment of ATF under DOJ, the One DOJ and Law Enforcement Information Sharing initiative, ATF information systems security policy and NFOCIS Branch policy did not sanction the sharing of wholesale extracts of investigative case data. For the one time sharing of an extract, the NFOCIS Branch labeled the CD "For Official Use Only", drafted a release statement that included a warning about unauthorized release of the data, and obtained a signature of the recipient DOJ representative to the statement and a

written commitment to return the CD to ATF and to purge the data from any system.

# Section 5.0
# External Sharing and Disclosure

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

None.

## 5.2 What information is shared and for what purpose?

Not applicable.

## 5.3 How is the information transmitted or disclosed?

Not applicable.

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

Not applicable.

# Section 6.0
# Notice

## 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?

NFOCIS is included in the listing of systems of records in a notice that is published in the Federal Register. Affidavits of interviews are provided in writing for review and acknowledgement by the individual. If the individual is unable to read, the affidavit is read to the individual. At the bottom of each page of the affidavit, there is space provided for signature or initials and the date signed or initialed by the individual.

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

Yes. For a criminal investigation, the individual has the right to request an attorney be present during questioning in custodial situations. In non-custodial situations, the individual has the option to decline to answer questions. For non-criminal civil investigations and inspections of premises of entities having or applying for a license or permit to engage in a business activity subject to ATF's oversight, the terms for the application, renewal, or continued compliance with Federal regulations stipulate that the entity or applicant must comply with Federal law and regulations. Failure to provide information to ATF may jeopardize the status of the license or permit whether issued or pending approval.

## 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. Information collected by ATF can be disclosed to the office of the U.S. Attorney in whose judicial district a case would be prosecuted and other parties, such as law enforcement agencies, consistent with Federal law.

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

The privacy risks are:

1. Personal information may be stored that could be used inappropriately. The data stored can only be used for the purposes outlined for this system and for no other purpose. Technical and management controls are in place to protect this data.
2. Sensitive data related to investigations is stored. This information is not available to public requestors as it may compromise an investigation as defined in section j2 of the Privacy Act of 1974.
3. Regulatory data is stored on the same system as investigative data. Regulatory data can be requested. Procedures are in place to analyze any requests for disclosure to ensure that only appropriate data is released.

# Section 7.0
# Individual Access and Redress

## 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 once it has been entered into NFOCIS. As defined in U.S.C. 552a (j) (2), according to the Privacy Act of 1974, section j), "General exemptions (*abstract*) 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.

-Information in N-Spect, an application within the NFOCIS System, can sometimes be released. This is the regulatory tracking of applications and renewals of licenses for firearms and licenses and permits for explosives. However, some of its data is used in civil cases and is not generally released during an on-going investigation.

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

ATF is required to post a notice in the Federal Register regarding systems of records. See 68 FR 3551 (January 24, 2003). Individuals are not notified of procedures to access or amend their information in NFOCIS because it is exempted under the Privacy Act due to its law enforcement function.

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

For information that is part of a criminal investigation that the U.S. Attorney's office has decided to prosecute in Federal court, the individual's counsel would have rights to review discoverable information.

### 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.

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.

## Section 8.0
## Technical Access and Security

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

Primarily those users whose roles are identified in the listing in Section 3.5.

### 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.

Database administrators contracted by ATF to provide Help Desk and technical support of the NFOCIS System and database have access to a limited number of database tables (back end) containing user information. These contractors must agree to not improperly access or disclose ATF information. Questions concerning the contract may be addressed to the ATF Acquisitions & Small Contracts Branch or to the Information Services

Division. Currently, no vendor under contract with the Department of Justice is authorized access to the NFOCIS database.

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

Yes. See response to Section 3.5.

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

Users must have an active userID and database account as well as a working password in order to access the system. Passwords expire every 55 to 60 days. Once a password expires, the end user must request a password reset. Login attempts, successful and failed, are tracked in an audit log. The procedures for requesting, obtaining, and maintaining access to the system are documented in the NFOCIS User and Operations 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 or have specific rights to address as defined in the procedures. Actual assignments of roles and rules are established as defined in Section 3.5 for obtaining an account. The procedures for creating and maintaining these system accesses, are audited regularly and are part of the annual FISMA audit review process. 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?

There are roles and views defined to limit data access. Changes to these roles and permissions are captured in the system audit log and maintained on a separate logging server for which the DBA and System Administrators do not have access. These events are reviewed daily by the Operational Security Team. A database administrator under contract to ISD Operations Security Branch runs a monthly report of locked accounts and provides the report to the NFOCIS System Owner and to the Designated Security Officer for review. All logins and access are tracked within the database. From a management control perspective, annual security training and the "Rules of Behavior" that have to be signed, reinforce the rights and restrictions of system access.

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

Completion of online information systems security refresher training is part of the annual mandatory training for all ATF employees and contractors. A certificate of completion of the refresher training is generated electronically in the Learn.ATF computer based training software and a status report of persons who have completed the refresher training and those who have not is provided to a manager in ATF's Office of Training & Professional Development. This training includes instruction of the provisions of the Privacy Act.

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

Yes, NFOCIS is secured in accordance with FISMA and NIST requirements. NFOCIS' last full Certification and Accreditation was May 5, 2005. All relevant documents have been updated in the annual review for 2006.

## 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. There is a clear separation of duties to prevent any one person from having sufficient access to allow inappropriate access or to work around the controls in place. 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. In accordance with the Information Technology Management Reform Act of 1996 and the "best practices" prescribed by GAO and OMB's Raines Rules, the NFOCIS System has been developed in phases. Also, prior to each phase, the NFOCIS Branch engages in the gathering of functional requirements and tasks the developer of each phase to compete technologies in order to identify solutions that best incorporate the latest information system security controls required by GISRA and now FISMA. With each new iteration of NFOCIS, the current technologies are evaluated for functional and security benefits.

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

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?

Due to the sensitive nature of the information captured, a number of design choices were made to protect the data. The tables are accessed by special purpose

limited applications to ensure that someone who may have access to one piece such as the property tracking aspect does not have access to active case data. A number of roles were designed to ensure that only the certain subsets of data could be viewed. Logs of user activity are in place as well as careful consideration of the client's interaction with the application further limiting potential user threat to the system.

## 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.

NFOCIS contains criminal and civil law enforcement sensitive records. Because the point of NFOCIS is to collect and disseminate investigatory information, some aspects of the Privacy Act of 1974 are inapplicable. 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 a reasonable degree in today's technology.

NFOCIS information will be used for official criminal and civil law enforcement and national security purposes only. NFOCIS information cannot be accessed or used for any other purpose, except as authorized by Federal law. NFOCIS information may not be disclosed in response to a request made under any State or local access law.

User limitations were created to ensure that NFOCIS is used for law enforcement purposes only and only law enforcement individuals with a "need to know" the information contained within the system will have access to the NFOCIS system. All persons requesting access to the NFOCIS system must undergo a background check, receive a clearance or waiver, and be granted access to Bureau systems by ATF's Personnel Security Office. In addition, the above-mentioned security controls, both administrative and technological, were developed and implemented in order to reduce the risk of unauthorized access to the data.

## Responsible Officials

/signed/_____
Signature Date

**Robert W. Tatro**

**Chief, NFOCIS Branch**

**System Owner**

/signed/_____
Signature Date

**Michael J. Breen**

**NFOCIS Designated Security Officer**

**N-Spect Program Manager**

/signed/_____
Signature Date

**Marion L. Burrows**

**Chief, Intelligence & Information Systems Division**

/signed/_____
Signature Date

**James E. McDermond**

**Assistant Director**

**Office of Strategic Intelligence & Information**

## Approval Signature Page

_____
Signature Date

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice