Privacy Impact Assessment
for the

GangNet

5/31/2006

Contact Point
Marion Burrows

Intelligence and Information System Division
Office of Strategic Intelligence and Information
(202) 927-7885

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

Introduction

GangNet is a Commercial Off the Shelf (COTS) system acquired by ATF. The GangNet system is a user friendly browser-based investigation, analytical and statistical resource for recording and tracking gangs, gang members and their activities. GangNet provides gang/gang members/gang incident tracking, and also provides for gang intelligence analysis to discern trends, relation ships, patterns and gang demographics. GangNet uses dropdowns, partial word name searching, calendar controls, drilldown forms, wildcards etc. to make entering and retrieving useful information easy. The GangNet system is an information sharing application that operates in a network environment and can be can be connected to multi-agencies GangNet applications and multi- locations.

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 GangNet system contains identifying data on alleged gang members, including the individual's photos, street names, and addresses, date of birth, phone numbers, known associates, gang hand signals and images of their tattoos. ATF Intelligent Research Specialist, Analyst, Special Agents and ATF Task Force members gain access to and can input data into the GangNet system.

1.2 From whom is the information collected?

Suspected gang members and their associates, Federal, State and Local Law Enforcement Agencies. There is no uniform definition of the term "gang." For at least the initial testing phase of GangNet, the term "gang" means a group or association of three or more persons who share a common identifying sign, symbol, or name and who individually or collectively engage in, or have engaged in, criminal activity falling within the investigative jurisdiction of ATF. The term gang is intended to include street gangs and outlaw motorcycle organizations and does not include traditional organized crime organizations, international drug trafficking organizations, or terrorist groups.

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 support of ATF's missions in reducing violent crime and protecting the public.

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

18 U.S.C. 3051 (ATF enforces and administers the Federal firearms (18 U.S.C. Chapter 44 and 26 U.S.C. Chapter 53) and explosives/arson (18 U.S.C. Chapter 40) laws. See also, 28 C.F.R. 0.130(d) (ATF may investigate violent crime as delegated by the Attorney General).

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 GangNet system contains privacy information such as name, date of birth and photos. 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. Mitigation is accomplished via the System Security Plan which reflects input from the System Administrator, Designated Security Officer and the System Owner concerning GangNet. The Risk Assessment analyze threats to and vulnerabilities of GangNet to determine the risks (potential for losses), and using the analysis as a basis for identifying appropriate and cost-effective measures. The Contingency Plan consists of management procedures to respond to any loss or degradation of essential services due to a failure of GangNet. The Certification consists of comprehensive testing and evaluation of the technical and non technical GangNet security controls and other safeguards used in support of the accreditation process. The accreditation consists of the official management authorization to operate GangNet.

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 information in GangNet is used by ATF Special Agents, Intelligent Research Specialists, analysts and other Federal, State and Local law enforcement partners for Law Enforcement Investigations, intelligence sharing and analysis to identify trends and patterns, and resource allocation .

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.)

The data contained in the GangNet system is used by ATF Analyst to perform intelligence analysis to discern trends, relationships, patterns and gang demographics. This information is provided to ATF Special Agents for possible investigations and resource allocation.

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

In order to enter a subject into GangNet they must meet two of the following criteria or be a self admitted gang member:

- Subject has been seen affiliating with law enforcement-documented gang members
- Subject has been arrested alone or with known gang members for offenses consistent with usual gang activity.
- In custody Classification interview.
- Subject has been seen frequenting gang areas.
- Subject has been seen wearing gang dress.
- Subject has been seen displaying gang symbols and/or hand signs.
- Subject is known to have gang tattoos.
- Subject has been identified as a gang member through documented reasonable suspicion.
- Subject has been identified as a gang member by a reliable informant/source.
- Subject has been identified as a gang member by an untested informant.

The data in the system is re-accessed on a continuing basis by the contributor(s) to ensure accuracy and currency.

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)?

In accordance with 28 C.F.R. § 23, data contributed by State and Local law enforcement is purged after five years if there have been no update to the data within that five year span. ATF's Record Retention Order addresses these records with respect to the NARA 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.

GangNet access is controlled by the following user profiles:

- System Administrator
- User with view, edit and update privileges
- User with view only

Based upon a person's profile, a comparable role is granted to the end user at the application front end level. In order to gain authorized access to the GangNet system:

- The end user must complete an Information Systems Access Request form, ATF F 7200.1

- Submit the application to a first level supervisor for review and approval

- Upon approval by the first level supervisor, the supervisor faxes the request to the Information Services Division's (ISD) Operations Security Branch.

- The requester must have a valid and active networkID and Outlook email account as a prerequisite to the GangNet access request being processed. ISD's Operations Security Branch verifies the existence of an active networkID and Outlook account and faxes the request to the Intelligence

and Information Systems Division. A signed rules of behavior must be on file for a networkID.

- The GangNet System Owner and the Designated Security Officer reviews the application.

- Once reviewed, approved, signed and dated, the access request form is handed to a GangNet system administrator who creates an application USERID specific to the user's role and a temporary password.

- Upon completion of the creation of the user account and temporary password, the system administrator sends an email notification to the applicant.

- The user must change the temporary password upon the initial logon to the system to a password of their choosing and conforming to the prescribed data naming convention enforced by ISD.

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?

Internal components of the Department that the information is shared are the Bureau of Prisons, Federal Bureau of Investigations, Drug Enforcement Agency, and United Sates Marshal Services , and other entities consistent with Federal law, i.e. the Privacy Act..

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

Information can be shared in connection with a user's official duties and to the extent consistent with Federal law, i.e. the Privacy Act..

4.3 How is the information transmitted or disclosed?

GangNet is a web based application that is hosted in the ATF secure INTRANET environment. All users must have a valid USERID and Password (see 3.5 for process). External law enforcement components who enter into a Memorandum Of Understanding (MOU) with ATF receive access the GangNet system via an extranet connection.

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

The GangNet system contains privacy information such as name, date of birth and photos. 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. Mitigation is accomplished via the following system warning banner: This system is restricted to authorized users for legitimate Law Enforcement purposes. Your usage of this system is audited and monitored by your System Administer. The unauthorized access, use or modification of this system or the data contained therein or in transit to/from, is prohibited by law and may be reported to Law Enforcement by system personnel.

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?

The information is shared with ATF Task force members that have been vetted by ATF and other Federal, State and Local law enforcement partners. Task force members are assigned a valid USERID and PASSWORD via the method described in section 3.5. ATF establishes a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA) with the External law enforcement partner before access to GangNet. is granted.

5.2 What information is shared and for what purpose?

The information in GangNet is used by ATF Special Agents, Intelligent Research Specialist, analyst and other Federal, State and Local law enforcement partners for Law Enforcement Investigations, intelligence sharing and analysis to identify trends and patterns.

5.3 How is the information transmitted or disclosed?

The information is transmitted or disclosed via the ATF secure Intranet, Extranet, telephonic, hard copy report, email and PDF.

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

All internal employees are required to take the mandatory security training. There is Memorandum Of Understanding or Memorandum Of Agreements between ATF and the external agencies which contain the following language: The Parties are to obtain permission for the disclosure to third parties of information received pursuant to this MOU prior to such disclosure, unless exigent circumstances exist that would justify a Party's not making such a request, in which case the Party seeking to disclose the information is to give notice of the disclosure to the Party that was the source of the information as soon as practicable; Exigent circumstances would include circumstances wherein a delayed disclosure would significantly increase the danger to life and/or property.

To the extent either Party discloses information received under this MOU to a government third party in accordance with paragraphs 7d and 7e above, the Party is to provide notice to the government third party to which the information was disclosed that the government third party is prohibited from further disclosure unless it obtains authorization from the Party that was the source of the information;

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

Prior to receiving access to the GangNet system ATF personnel provides training on the system usage (data entry functionality querying) users are also provided a GangNet users guide.

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

The GangNet application logs every user who accesses the system to include date, time, who viewed it, what they viewed, and what actions they took (add, delete, modify). Auditing reports via the

GangNet application are produced on a monthly basis and can be run daily. External audit logs are run by the Information Services Divisions System Administrators quarterly and are provided to the system owner for review..

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

ATF enters into a Memorandum Of Understanding (MOU) with external law enforcement partner. The purpose of this MOU is to set forth terms by which the law enforcement partners and ATF are to share law enforcement information and intelligence relating to the information contained in the GangNet system. Information is shared between the law enforcement partners pursuant to an express understanding of confidentiality. Such information, as well as inquiries and requests for information, received by a law enforcement Party under the MOU, is to be protected from disclosure to third parties to the greatest extent permissible under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and subject to disclosure restrictions contained in the Privacy Act (PA), 5 U.S.C. § 552a.

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 GangNet 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 GangNet. 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 GangNet 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?

GangNet access is controlled by the following user profiles:

- System Administrator
- User with view, edit and update privileges
- User with view only

Refer to section 3.5 for process.

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 GangNet database have access to the database tables (back end) containing user information. Questions concerning the contract may be addressed to the ATF Office of Science and Technology (OST) Information Security Office (ISSO).

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

GangNet access is controlled by the following user profiles:

- System Administrator
- User with view, edit and update privileges
- User with view only

Based upon a person's profile, a comparable role is granted to the end user at the application front end level. In order to gain authorized access to the GangNet system:

- The end user must complete an Information Systems Access Request form, ATF F 7200.1
- Submit the application to a first level supervisor for review and approval
- Upon approval by the first level supervisor, the supervisor faxes the request to the Information Services Division's (ISD) Operations Security Branch.
- The requester must have a valid and active networkID and Outlook email account as a prerequisite to the GangNet access request being processed. ISD's Operations Security Branch verifies the existence of an active networkID and Outlook account and faxes the request to the Intelligence and Information Systems Division. A signed rules of behavior must be on file for a networkID.
- The GangNet System Owner and the Designated Security Officer reviews the application.
- Once reviewed, approved, signed and dated, the access request form is handed to a GangNet system administrator who creates an application USERID specific to the user's role and a temporary password.
- Upon completion of the creation of the user account and temporary password, the system administrator sends an email notification to the applicant.
- The user must change the temporary password upon the initial logon to the system to a password of their choosing and conforming to the prescribed data naming convention enforced by ISD.

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 contact the Help Desk and request a password reset. Users can make no more than 3 attempts to log in with the correct UserID and password. After the 3rd failed attempt, the account is locked at the database level. 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 GangNet User 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 this system access are audited regularly and are part of the annual FISMA audit review process. Auditing and system log review are on-going activities. Additionally, 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?

ATF's Information Security Office has implemented the concept of "Separation of Duties (administrators and users)" and divided critical functions between two or more individuals. All users are assigned a particular class in the user class field. Each class gives the user a particular level of functionality and access to the application. All activity is captured via audit logs.

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, GangNet is secured in accordance with FISMA and NIST requirements. GangNet's last full Certification and Accreditation was March 2006.

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

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, ATF evaluated other technologies and compared their abilities to effectively achieve ATf's goal of obtaining a user friendly browser-based analytical and statistical resource system for recording and tracking gangs, gang members and their activities.

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

The GangNet conformed to ATF's security policy as it pertains to password complexity, password expiration role based privileges, system log and application level auditing reports. GangNet complies with ATF Automated Information System (AIS) Minimum Security Requirement

9.3 What design choices were made to enhance privacy?

Separation of duties, access controls and auditing..

To enhance privacy the separation of duties were established were further defined via user roles. A user may only have the ability to view data and not have the ability to edit or delete data. Auditing was established with in the system via the application to allow the application system administrator the ability to run audit reports daily.

Conclusion

GangNet is a proprietary, off-the-shelf, database and software solution that tracks information on alleged gang members, including the individual's photo street names, addresses known associates, gang hand signals, and images of their tattoos. ATF has acquired GangNet to capture it's gang data in support of ATF's mission to reduce violent crime and protect the public

The ATF GangNet application resides on the ATF secure network. The application is used by cleared ATF employees who already have access to the ATF network and ATF vetted law enforcement partners. The GangNet application facilitates and promotes the sharing of gang-related information within ATF and among ATF state, local, and federal law enforcement partners.

The GangNet system contains Sensitive But Unclassified data that is protected by the Privacy Act of 1974 and the Freedom of Information Act (FOIA). Information from GangNet is made available to the appropriate individuals and organizations. Securing the data and ensuring it

is used properly is critical to successful law enforcement. ATF has implemented a solution that it believes controls those threats to a reasonable degree in today's technology.

Responsible Officials

/signed/
Marion Burrows Intelligence and Information Systems (IIS) Division Chief

Department of Justice

Approval Signature Page

_____ <<Sign Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice