Privacy Impact Assessment
for the

Border and Transportation Security Network (BTSNet) Spiral 1

January 18, 2005

<u>Contact Point</u>
Gerald R. Kirwin
BTSNet Program Manager
Science & Technology Directorate
Homeland Security Advanced Research Projects Agency
202-254-5773

<u>Reviewing Official</u>
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

The Border and Transportation Security Network (BTSNet) is a project of the Department of Homeland Security (DHS), Science and Technology Directorate, Homeland Security Advanced Research Projects Agency (HSARPA). BTSNet is a proof-of-concept prototype development. Its mission is to develop technology to secure our nation's borders by preventing the entry of terrorists and their instruments of terror, criminals, and illegal aliens into the country. BTSNet will be implemented using a spiral development, which means with each spiral there will be increased capabilities and a broader user base. Spiral 1 is focused on U.S. Border Patrol field operations with an emphasis on the Southwest border area. This development essentially extends the law enforcement data base query capability that is currently a field station function and moves it to the field agent via wireless communications using a handheld personal digital assistant (PDA) and/or a vehicle-mounted mobile data computer (MDC). The field agent will be able to make biographic and biometric queries on detainees from the field rather than physically transporting detainees to the station. Initially, BTSNet will query biographical data from the Enforcement Case Management System (ENFORCE), the Automated Biometric Identification System (IDENT), and the National Criminal Information Center (NCIC) based on personal data collected from a detainee. NCIC will be accessed through the Arizona Criminal Justice Information System (ACJIS). The ACJIS will also return some criminal information (wants and warrants) and vehicle information (registered owner and stolen vehicle alerts) from Arizona state and local data bases. Future developments will provide the agent access to other data sources and expand the user base to other DHS components. Personally identifiable information collected or retrieved by the BTSNet system will not be stored on the server, the handheld device or vehicle-mounted computer. This PIA will be updated accordingly as other spirals are developed.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

In order to conduct the requisite queries, the field agent will need to collect specific personally identifiable information from a detainee. That information may include surname, first name, father's surname, mother's surname, date of birth, alien number, sex, hair color, eye color, height, and weight. BTSNet will use this data to initiate an identity check. Based on the information used to initiate the query, the information received in return may include surname, first name, father's surname, mother's surname, date of birth, alien number, photograph, IDENT event number, fingerprint identification number (FINS), sex, hair color, eye color, height, weight, and information on active warrants. The BTSNet system will not store the collected information or the returned query results; it is an access point that will allow entry into the data base systems that support the work of agents deployed at U.S. borders.

The BTSNet server located in the Border Patrol station will log all queries processed by the system and will record the following information: date, time, location and requesting agent. These logs will be used to conduct statistical analysis of BTSNet system usage and for audits.

1.2 From whom is information collected?

Individuals subject to the data collection requirements and processes of BTSNet are those who have been detained as a result of an observed or suspected illegal border crossing or other illegal border activity.

1.3 Why is the information being collected?

The information is being collected by Border Patrol agents in connection with their official duties. Currently information queries are performed at the Border Patrol station. BTSNet is extending the query capability from the station to the field by way of wireless enabled handheld digital devices and vehicle-mounted mobile data computers. BTSNet will provide Border Patrol agents the ability to conduct biometric and biographic queries to identify detainees, in the field and at the time of apprehension. This process will allow the field agent to assess their operational and security posture by identifying individuals on terrorist watch lists, known criminals, and repeat illegal border crossing offenders.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

U.S. Border Patrol Agents are authorized by the Immigration and Nationality Act Section 287 (8 U.S.C. 1357) to interrogate any alien or person believed to be an alien as to his right to be or remain in the United States.

1.5 Privacy Impact Analysis

The capabilities provided by the BTSNet prototype are intended to improve operational efficiency and enhance the field agent's safety and security posture. During BTSNet system design it was decided that the minimum information necessary to permit a positive detainee identity resolution check would be collected in order to maintain that posture, as attempting to collect too much information could distract the field agent. This is the same, or less, information that may be collected during current operations when the information is relayed via radio to a station dispatcher for applicable data base query. If a positive identity resolution check cannot be achieved from the field, then the detainee will be transported to the Border Patrol Station for more in-depth processing.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

The BTSNet Spiral 1 implementation and its associated devices will be employed by the agents of the U. S. Border Patrol in the Tucson Sector Douglas Station. It will be used to allow agents to conduct identity resolution of individuals detained as a result of observed or suspected illegal border crossings. Specifically, the system will be used to query data base systems in order to identify individuals on terrorist watch lists, known criminals, and repeat illegal border crossing offenders.

2.2 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 system will provide a federated data query capability, i.e., the ability to query multiple data sources from a single input. These data sources are already available to the agent in the station. BTSNet Spiral 1 does not provide access to previously unknown data, but consolidates access to known data to improve agent efficiency.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Since BTSNet Spiral 1 allows agents to access data that is already available to the agent in the station, there is no independent check by the system to verify accuracy. Data accessed will be from U. S. Federal or State Government sources and is assumed to be accurate.

2.4 Privacy Impact Analysis

To evaluate system use, the BTSNet server will log all queries processed by the system and will record the following information: date, time, location and requesting agent. These logs will be used to conduct statistical analysis of BTSNet system usage. The logs will also be available to the supervisory personnel for review and audit to verify valid law enforcement use of BTSNet and the connected databases. The Border Patrol has disciplinary programs in place regarding any misuse of Government systems and information. Additionally, system users will be restricted to field agents, Law Enforcement Communications Assistants (LECAs), and system managers. Due to the law enforcement sensitive nature of the data sources accessed by the BTSNet system, agents must have access credentials for the individual data sources as well as the BTSNet system.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Once it is determined whether an individual is a known person of interest, the BTSNet server will erase any personally identifiable information contained in the query input parameters. The query results will also be erased. The BTSNet server located in the Border Patrol station will log the query date, time, location and requesting agent to permit a statistical evaluation of BTSNet system utility and to facilitate auditing.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Because BTSNet is not the owner of the databases which are queried, any results from those queries will be retained consistent with the retention schedules established for the databases. The query log will be maintained for statistical evaluation and auditing only. In accordance with NARA General Records Schedule 20 Paragraph 1.a, this log does not require retention scheduling.

3.3 Privacy Impact Analysis

The BTSNet prototype is not designed for archiving of detainee personally identifiable information. Only a log containing query date, time, location and requesting agent will be maintained to permit a statistical evaluation of BTSNet system utility and to facilitate auditing.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The identity resolution check data query input parameters and corresponding query results will remain within the Border Patrol Station where BTSNet is installed and not be shared with any other DHS organization.

4.2 For each organization, what information is shared and for what purpose?

Not applicable.

4.3 How is the information transmitted or disclosed?

Not applicable.

4.4 Privacy Impact Analysis

The BTSNet Spiral 1 prototype is intended to enhance local operations at the station where it is installed. Data collected using BTSNet is of time sensitive value and therefore is only accessible by personnel immediately involved in system operations. Any data sharing will be conducted using other systems at the station when the detainee is returned for more in-depth processing.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The data collected to initiate an identity resolution check on a detainee will remain within the Border Patrol Station where BTSNet is installed and not be shared with any external organization. If BTSNet collects information during an encounter that is not already available from the data bases queried, then the detainee will be transported to the Border Patrol Station for further processing. BTSNet cannot add or change information in the data bases it accesses.

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 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Not applicable.

5.5 How is the shared information secured by the recipient?

Not applicable.

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

Not applicable.

5.7 Privacy Impact Analysis

The BTSNet Spiral 1 prototype is intended to enhance local operations at the station where it is installed. No data collected by the system is shared outside the local area or with any external organization or system. A privacy risk due to external sharing does not exist.

Section 6.0 Notice

6.1 Was 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?

A notice will not be provided prior to data collection, although notice about the existence of the underlying data systems that are queried will have been provided by each of those systems. The data collection and subsequent identity resolution data query are intended to help the agent establish probable cause for detaining an individual. All stops of individuals are based on reasonable suspicion of a violation of the law (see Section 1.2).

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

No. If a detainee declines to provide the information necessary to conduct an identity resolution check, they will be transported to the local Border Patrol Station for retention and processing outside of the BTSNet prototype.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis

The purpose of the BTSNet prototype is to assist field agents in securing our nation's borders by preventing the entry of terrorists and their instruments of terror, criminals, and illegal aliens into the country. As such, individuals subject to the data collection requirements and processes of BTSNet are those that have been detained as a result of observed or suspected illegal border activity. The data collected is solely for the purpose of conducting queries on existing data systems in order to produce an identity resolution check and to establish probable cause for further detaining the individual. Since the data collected is not shared with other entities or permanently stored within the system, there is no impact to the privacy of the detainee.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Data will be collected from the individual and is assumed to be correct. However, there will be no permanent data retention by the system. Individuals would have to request access from the databases BTSNet queries, not from BTSNet.

7.2 What are the procedures for correcting erroneous information?

BTSNET Spiral 1 will allow agents to query existing data systems. The procedures for correcting erroneous information in those systems are established by each data base. If, during an encounter, it is determined that information returned from a data base query is erroneous, the detainee will be transported to the Border Patrol Station for further processing and identity resolution. BTSNet cannot add or change information in the data bases it accesses.

7.3 How are individuals notified of the procedures for correcting their information?

Not applicable.

7.4 If no redress is provided, are alternatives are available?

Not applicable.

7.5 Privacy Impact Analysis

Data collected using the BTSNet prototype is not stored by the system nor is it transferred to any other system for storage. The record of apprehension and detention is maintained in data bases external to BTSNet. Individuals would have to request access to those data bases and not from BTSNet.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

System users will be restricted to field agents, Law Enforcement Communications Assistants (LECAs), and system managers. There will be no public access to the system. Due to the law enforcement sensitive nature of the data sources accessed by the BTSNet system, agents must have access credentials for the individual data sources as well as the BTSNet system.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Once the BTSNet prototype is installed and demonstrated, the BTSNet System Integrator will provide system maintenance support to include troubleshooting, repairs and software updates. The System Integrator is a contractor but will not be involved in data collection activities. No personally identifiable information will be stored in the system. During system development and maintenance the System Integrator does not have access to law enforcement data bases containing personally identifiable information. Development is conducted using a mock data base containing fictional data.

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

Yes, access to ENFORCE, IDENT, ACJIS and NCIC will be limited by the BTSNet software to those agents authorized for access to those data sources.

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

Not applicable.

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

For the BTSNet Spiral 1 implementation, the Border Patrol is assigning a specific set of agents to test the system functionality and operational utility. These agents are trained in current field operations and already have access to the data bases that BTSNet will query. Each user will be assigned unique authentication credentials for the BTSNet system. Overall, the BTSNet prototype system will utilize a three step username/password authentication process to access the system: 1) access to a field device (PDA or MDC), 2) access to the "over-the-air" encryption capability, and 3) authentication to the data bases being queried. This process will ensure that only authorized users have access to system information. The authentication credentials for each step are stored in separate locations, preventing single point access to that data. The system will maintain a user log that will be available for audit purposes.

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

The BTSNet server located in the Border Patrol station will log all queries processed by the system and will record the following information: date, time, location and requesting agent. This information is maintained principally to permit a statistical evaluation of BTSNet system utility. These logs will also be used for auditing purposes to ensure valid law enforcement use of BTSNet and the connected databases. The Border Patrol has disciplinary programs in place regarding any misuse of Government systems and information.

Because the query and receipt of personal information is being conducted in a field environment, privacy risks exist from the potential loss of personally identifiable information due to communications intercept or inadvertent disclosure due to theft/loss of field devices (PDA or MDC). Specific system design actions have been taken to mitigate these risks. Loss due to intercept is mitigated by BTSNet communications being encrypted in accordance with Federal Information Processing Standard (FIPS) 140-2. Though intercept may occur, reading of the transmitted data will not be possible. Several system features will prevent inadvertent disclosure. First, personally identifiable information collected by the field agent for entry into a data query will not be stored on the PDA or MDC. Second, access to the device will be controlled by a user authentication logon process requiring a unique username/password combination. Lastly, the PDA will be tamper resistant in that the information on the device will be encrypted and cannot be accessed without proper user authentication.

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

Users will be trained on the operation and use of the BTSNet prototype. Training will address the security and privacy issues related to BTSNet as operator functionality is moved from the station to the field.

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

BTSNet Spiral 1 Certification & Accreditation (C&A) is in process. Interim Authority to Operate is expected to be received in late January 2006. Completion of the C&A process and full Authority to Operate is expected to be received in July 2006.

8.9 Privacy Impact Analysis

The BTSNet prototype is designed to have strict controls over who may access the system. This is enabled by a three-step username/password authentication process; authentication to the field device, wireless communication encryption capability, and the data bases being queried. Since BTSNet is operated over a wide area wireless network, the principal risk to privacy is the intercept of communications signals. Though signal intercept cannot be prevented, BTSNet mitigates this loss by encrypting all data transmissions using the latest Federal Information Processing Standard (FIPS) 140-2. Though intercept may occur, reading of the transmitted data will not be possible. Lastly, the use of information processing devices in the field presents a privacy risk should a device be lost or stolen. To mitigate loss in this event, the BTSNet design incorporates several features: personally identifiable information will not be stored on a field device, device access will be controlled by a username/password authentication process, and any information on the device will be encrypted and inaccessible without proper user authentication. Because of the law enforcement sensitive and personally identifiable nature of the information processed by the BTSNet prototype, specific and conscious design features were incorporated to ensure its security.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The BTSNet Spiral 1 prototype was developed as an integration of commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) hardware and software, with some custom software development.

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

Coordination with the U. S. Border Patrol, DHS Chief Information Officer and DHS Privacy Office provided insight into the requirement and current approaches to safeguarding personal information.

9.3 What design choices were made to enhance privacy?

Types and levels of encryption were investigated, types of Anti-Tamper (AT) methods were considered and authentication schemes analyzed. Based on this research safeguards were selected and incorporated into the system design that would provide the appropriate protection of personally identifiable information.

Conclusion

The BTSNet Program mission is to effectuate the application of technology to securing our nation's borders by preventing the entry of terrorist and their instruments of terror, criminals, and illegal aliens into the country. This development extends the data base query capability that is currently a U. S. Border Patrol field station function and moves it to the field agent via wireless communications, providing the agent the ability to conduct biometric and biographic queries to identify detainees, in the field and at the time of apprehension. The process will allow the field agent to assess their operational and security posture by identifying individuals on terrorist watch lists, known criminals, and repeat illegal border crossing offenders. The system will become a part of the Border Patrol network and will not be accessible to external entities, government or civilian. This new operational posture presents the possibility of privacy risk due to loss of personally identifiable information. Field devices have been chosen and specific system design actions have been taken to mitigate the risk to loss of operational data and personal information. Loss due to intercept is mitigated by BTSNet wireless communications being encrypted in accordance with the Federal Information Processing Standard (FIPS) 140-2. Personally identifiable information collected from a detainee will not be stored by the system. Access to field devices will be controlled by a user authentication logon process requiring a unique username/password combination and lastly, the PDA will be tamper resistant in that the information on the device will be encrypted and cannot be accessed without proper user authentication.

This Privacy Impact Assessment will be revised and re-published as future spirals are developed.

Responsible Officials

Gerald Kirwin
BTSNet Program Manager
Department of Homeland Security
Science & Technology Directorate
Homeland Security Advanced Research Projects Agency

Approval

____ January 18, 2005

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security