# Privacy Impact Assessment
for the

# SBI*net* Program

July 20, 2007


**Contact Point**
**Dr. Kirk Evans**
**SBI*net* Program Manager**
**United States Border Patrol**
**United States Customs and Border Protection**
**(202) 344-2450**

**Reviewing Official**
**Hugo Teufel III**
**Chief Privacy Officer**
**Department of Homeland Security**
**(703) 235-0780**

## Abstract

The Secure Border Initiative-net (SBI*net*) is a Department of Homeland Security (DHS) Customs and Border Protection (CBP) system designed to detect, identify, apprehend, and remove illegal entrants to the U.S. on and between the Ports of Entry (POE). This PIA addresses Project 28, which is a concept demonstration prototype for the SBI*net* program. Project 28 focuses on a 28 mile border segment surrounding the Sasabe, Arizona Port of Entry (POE). This privacy impact assessment (PIA) has been conducted because SBI*net* collects and processes personally identifiable information (PII).

## Introduction

The Secure Border Initiative (SBI), created in November 2005, is the Department of Homeland Security's (DHS) plan to reduce illegal immigration and secure America's borders. SBI addresses three goals essential to DHS's border security and immigration missions: (1) to gain effective control of the borders; (2) to strengthen interior enforcement and compliance with the immigration and naturalization laws; and, (3) to support Congressional passage and Executive Branch implementation of a Temporary Worker Program. To achieve the first goal, SBI*net* was created to provide U.S. Customs and Border Protection (CBP) with the resources and capabilities needed to achieve a more comprehensive operational awareness on the border. SBI*net* will assist CBP officers in classifying the illegal entry (number of aliens, armed, with animal, etc.), help with the decision process in order to efficiently respond to the entry, and help bring the illegal entry to an appropriate law enforcement resolution.

New SBI*net* technologies will include video cameras that provide continuous monitoring of the border, especially remote areas. When an agent receives an alert from a triggered sensor, video surveillance will allow a Common Operational Picture (COP) operator to zoom into that location and identify whether the disturbance might be an animal, vehicle, or human. Surveillance recordings are routinely over-written, unless a significant event has occurred that requires the recording to be saved. A significant event might include capturing the apprehension of an individual illegally entering the country who is subsequently arrested by a Border Patrol Officer. CBP will have up to 30 days to retrieve a significant event from earlier recordings. The recorded event may become evidence in an apprehension incident and therefore would be retained as an evidentiary (criminal) file until it is no longer required. In the instance of associating the video with a law enforcement activity, the video information will be linked to PII maintained in reports and records residing in either the TECS System of Records (66 FR 52984) or ENFORCE System of Records (71 FR 13987). Both systems provide electronic case management capability to support DHS law enforcement activities, and where appropriate the case status will be updated to reflect the existence of video, maintained external to the system, to support the narrative remarks contained in the system.

All persons who cross the border at any point other than a designated border crossing point (*e.g.*, Port of Entry) are in violation of the customs and immigration laws. While a person's status as a violator may reduce their expectation of certain privacy protections, this reduced expectation does not eliminate CBP's responsibility to provide fundamental safeguards for personally identifiable information. Currently, legacy CBP systems provide deterrence capabilities at the border. These systems include fencing, lighting, vehicle barriers, patrol roads, remote video surveillance system, and unattended ground sensors (UGS). In addition, CBP employs video and control center monitoring and dispatch capabilities to detect potential border intrusions. Where deployed, the legacy components work collectively to provide deterrence, surveillance, and detection capabilities to support CBP operations.

The Secure Borders Initiative programs call for CBP to absorb past systems, to enhance the operational environments and to provide improved deterrence, detection, identification, surveillance, and communications capabilities to further CBP's mission. For example, improved capabilities will result in a greater level of deterrence for cross- border criminal organizations and terrorist groups seeking to exploit historically weak entry points, by improving CBP's ability to detect illegal entries and provide a coordinated response to these incursions. In addition, systems to be developed include agent field systems (*e.g.*, upgraded mobile, electronic, and computing devices), detection and surveillance platforms, communications systems, tactical infrastructure deployments, and command and control centers.

Project 28 is the first operational task order for SBI*net*. Project 28 focuses on a 28 mile border segment surrounding the Sasabe, Arizona Port of Entry (POE). Project 28 includes the design, development, delivery, and deployment of the following: re-deployable sensor towers with associated sensors to improve detection; mobile command, control, and communications units to enable situational awareness; provide rugged, secure, mounted laptop computers to enable displays of the Common Operational Picture—a display image which integrates the spatial representation of a geographic area and the persons or objects within, as fed from a video camera, with the global positioning data of the user and other law enforcement responders, to permit a comprehensive image of the operational context of a law enforcement activity, in a real time context; satellite phones to improve communications to agent vehicles; provide rapid response transports to increase the speed of transportation of illegal immigrants from the field to processing and detention facilities; Project 28 is the initial demonstration and analysis of the technology that could be deployed across U.S. borders and POEs. This PIA concentrates on the Project 28 effort. This PIA will be updated as the SBI*net* program matures and/or future technology implementations are realized.

SBI*net*, as a program, is a multi year, multi step transformation and hardening of the U.S. border. Project 28 is a concept demonstrator of the first proposed step and incorporates enhancements to current technology and operations. Under Project 28, SBI*net* does not enable CBP to collect new information or to use the information that CBP currently collects and maintains to support a new mission. As a matter of policy, CBP continues to share data collected from and

about illegal entrants by officers and agents between CBP and internal DHS personnel, including U.S. Immigration and Customs Enforcement (ICE), the DHS Office of Intelligence and Analysis (I&A), the DHS National Operations Center (NOC), U.S. Citizenship and Immigration Services (USCIS), and U.S. Coast Guard (USCG). SBInet improves the technology used to collect and employ operational data, such as the creation of the COP, at the border: the cameras are more capable, both in terms of power and range, and the communications between field units and control units provide greater range and capacity, allowing for more information to be shared more expeditiously. As part of current CBP practice, information obtained through SBInet technological enhancements will also be shared, on an as needed basis, with non-DHS personnel, including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), National Guard, local, tribal, state, and federal prosecutors and law enforcement. Lastly, SBInet could encompass the sharing of system data with international partners who participate in border security related and international law enforcement activities for their nations, for example sharing with Mexican or Canadian border officials.

These technologies will provide officers and agents greater situational awareness. Information collected through investigation of potential illegal entry will be input to CBP's Treasury Enforcement Communications Systems (TECS) and DHS's Enforcement Operational Immigration Records System (ENFORCE/IDENT) as is done with current procedure. This enhanced border awareness and use of technology will create a COP which enhances the safety and situational awareness for the General Public, Agents, and Officers in the field. On a graphical display the COP will provide Officers and Agents with a geographically referenced situational overview that identifies their proximity to the indicated illegal entry as well as their fellow agents.

SBInet solutions will include video cameras that provide continuous monitoring of the border areas. When an alert from a triggered sensor, video surveillance allows an operator to direct a camera to that location and identify whether the disturbance might be an animal, a vehicle or a human. Video signals from the cameras are recorded 24/7 and are routinely over-written, unless a significant event has occurred that requires the recording to be saved. CBP will have up to 30 days to determine to save a significant event from a recording. The recorded significant event may be used as evidence in an adjudication resulting from an apprehension. In instances where there is a resulting law enforcement action, the recording will be maintained for as long as operationally necessary.

This PIA follows a different format than the traditional PIA Template because the majority of the information relates to video cameras. As such, this PIA template has been modified to help address issues that arise specifically from this type of technology. This PIA was adapted from a PIA developed specifically for video surveillance by students at the Samuelson Law, Technology & Public Policy Clinic at the Boalt Hall School of Law, University of California at Berkeley.

# 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 collected, as well as the reasons for its collection as part of the program being developed.*

## 1.1 What information is to be collected?

*Please check the following if applicable:*

*The System's Technology Enables It to Record:*

☑ Video

Static Range:

Zoom Range: [The SBInet system has a detection range of up to 10 kilometers]

☑ Tracking

☐ Automatic (for example, triggered by certain movements, indicators)

☑ Manual (controlled by a human operator)

☑ The system does not provide for the collection of sound.

*The System Typically Records:*

☑ Video signals are viewed in operations centers and in vehicles within broadband coverage areas. Equipment will be mounted on towers that are generally located near border areas where illegal border crossings may occur. The video signals typically encompass near-border landscapes where agents may not be patrolling at the time of an incursion.

## 1.2 From whom is the information collected?

☑ Targeted populations, areas, or activities (please describe).

The video surveillance targets a specific area, and is employed to collect images of possible illegal entrants within its range. Following apprehension of an illegal entrant, Information (PII) is collected during an interview of said illegal entrant. The illegal entrant may have been viewed by surveillance cameras while traveling across the border, or intercepted as a result of responding to a triggered sensor. Images from the camera may become associated with the information collected during the interview, where such corroboration is possible.

☑ Training included directives for program officials to focus on particular people, activities, or places.

## 1.3 Why is the information being collected?

☑ To aid in criminal prosecution

☑Terrorism investigation

☑Terrorism prevention

☑Other (please specify)

Camera surveillance, event recordings and PII from illegal alien interviews are collected so that the officers and agents can get a better picture of whether or not a threat exists. If so, the illegal persons will be arrested for a present or past transgression, deported, or be held or transferred to the custody of another law enforcement group as a "person of interest" (i.e. ICE, ATF or FBI).

### 1.3.1 Policy Rationale

☑Crime prevention rationale:

Surveillance cameras are an asset to the program because they allow CBP to monitor the vast remote border areas without having a patrol agent in the immediate area. The ability to detect and respond to an illegal border crossing is greatly enhanced.

### 1.3.2 Cost Comparison

The principal alternative is to increase patrolling of remote locations, which incurs increased costs for staffing and equipment, and creates greater risks to officer safety, because of expanded patrol areas.

### 1.3.3 Effectiveness

☑ Program includes a timeline for evaluation

## 1.4 How is the information collected?

☑Real-time monitoring with footage stored with the capability to go back and retrieve up to thirty days past footage.

## 1.5 What specific legal authorities, arrangements, and/or agreements defined the surveillance system?

☑Executive or law enforcement decision: The implementation of the Executive Branch Program "Border Security and Control Between the Ports of Entry," as authorized under title 8, United States Code, section 1357, and implemented pursuant to title 8, Code of Federal Regulations, section 287.

☐ Entity making the decision relied on:

☐ case studies

☑ research

☑ hearings

☐ recommendations from surveillance vendors

☐ information from other localities

☑ other (please specify)

Project 28 is a concept demonstrator directed by OMB so that the primary integrator could demonstrate the feasibility of its proposed technical solutions.

*Funding:*

☑ Other (please specify)

2005 Congressional funding provided DHS with a multi-year plan to enhance border security and immigration.

## 1.6 Privacy Impact Analysis

SBInet incorporates technological improvements to existing CBP procedures and methods for surveilling and detecting intrusions at remote locations along the United States border. These improvements include higher resolution cameras, faster and more powerful computers, and digital, satellite communications for improved range and clarity. By definition, the persons observed, captured on video, and/or apprehended are persons crossing the border at locations that are not designated border crossing points, and therefore, the persons are automatically in violation of the law. In this instance, the presence of surveillance cameras poses the greatest privacy risk to those persons who choose to violate the law, and by so doing have the least privacy interest. The association of personally identifiable information with a video image will only be possible as a result of a person being apprehended and will be no more intrusive than the current practice of apprehending persons at the border and then collecting their PII incident to that apprehension. The privacy risk posed by mis-identification of a person on a video image following an apprehension is mitigated by the professional training of the apprehending officers. Additionally, since apprehension and determination of a violation are not dependent upon the association of a person's PII with a possible video image, the privacy risk posed by mis-identification is practically non-existent.

# Section 2.0 Uses of the System and Information

## 2.1 Describe uses of the information derived from the video cameras.

*Please describe the routine use of the footage. If possible, describe a situation (hypothetical or fact-based, with sensitive information excluded) in which the surveillance cameras or technology was accessed for a specific purpose.*

SBInet technologies include video cameras that provide continuous monitoring of the border, especially remote areas. When an agent or officer receives an alert from a triggered sensor, video surveillance will allow the COP operator to zoom into that location and identify whether the disturbance might be an animal, vehicle or human. Surveillance recordings are routinely over-written, unless a significant event has occurred that requires the recording to be saved. CBP will have up to 30 days to retrieve a significant event from earlier recordings. The recorded event may become evidence in an apprehension incident and saved for an indefinite period of time. In the instance of associating the video with a law enforcement activity, the video information will be linked to PII maintained in reports and records residing in either the TECS or ENFORCE systems. Both systems provide electronic case management capability to support DHS law enforcement activities, and where appropriate the case status will be updated to reflect the existence of video, maintained external to the system, to support the narrative remarks and information contained in the system.

# Section 3.0 – Retention

*The following questions are intended to outline how long information will be retained after the initial collection.*

## 3.1 What is the retention period for the data in the system (i.e., how long is footage stored)?

☑1 week – 1 month

Information is maintained for no more than 30 days except where an image becomes associated with a law enforcement activity and then the retention period persists for the duration of the law enforcement activity.

## 3.2 Retention Procedure

☑Footage automatically deleted after the retention period expires.

There is enough storage capacity to retain surveillance footage for no more than thirty days. After that time, the footage is over-written by new surveillance footage.

## 3.3 Privacy Impact Analysis.

The retention period for video images is 30 days, unless the image becomes associated with a law enforcement activity. Once associated with a law enforcement activity, the retention period becomes the duration of the law enforcement activity and its related proceedings. The principal privacy risk posed by the general 30 day retention period is that an image, during review or analysis, might be mis-identified by comparison to other law enforcement information that is information obtained from federal, state, local, tribal, or foreign law enforcement partners. This risk is mitigated by the experience, knowledge, and training of officers. The privacy risk posed by a proper identification is not mitigated as this is an aspect of the law enforcement purpose behind the system.

# Section 4.0 Internal Sharing and Disclosure

*The following questions are intended to describe the scope of sharing within the surveillance operation, such as various units or divisions within the police department in charge of the surveillance system. External sharing will be addressed in the next section.*

## 4.1 With what internal entities and classes of personnel will the information be shared?

Internal Entities

☑Investigations unit

☑Command unit

Classes of Personnel

☑Command staff (please specify which positions)

Information about an arrest or event may be shared among the arresting agents and the commanding personnel. An illegal entrant's PII will be inputted into TECS or ENFORCE data systems as part of the record of the enforcement activity. This information may include corroborating video images as appropriate. Information about an event may be shared among shift personnel, Supervisors, or intelligence analyst.

## 4.2 Policies regarding granting access

### 4.2.1 Is there a written policy governing how access is granted?

☑ Yes –Both DHS's management directive on information security (MD 4300) and CBP Information Systems Security Policy & Procedures Handbook CIS HB 1400 05C sect. 6.3 Logical Access.

☐ No

### 4.2.2 Is the grant of access specifically authorized by:

☐ Statute (please specify which statute)

☐ Regulation (please specify which regulation)

☑ Other (please describe)

Grant of access is based on "need to know" and only authorized by managing staff.

☐ None

## 4.3 How is the information shared?

### 4.3.1 Can personnel with access obtain the information:

☑ Off-site, from a remote server

☑ Via copies of the video distributed to those who possess an authorized need.

## 4.4 Privacy Impact Analysis.

In order to mitigate the privacy risks of personally identifiable information being misused or inappropriately used, all personnel requesting information from TECS, ENFORCE, or the retained video image, must establish a need to know the information as part of official employment responsibilities. Additionally, any internal DHS access to the data is controlled by CBP through the use of strict access controls for the users, passwords, background checks for individuals accessing the data as well as system audits that track and report on access to the data.

# Section 5.0 Technical Access and Security

## 5.1 Who will be able to delete, alter or enhance records either before or after storage?

☑ Other.

A record may be deleted by a staff member with access rights only after this action has been approved by a higher authority, such as a supervisor. Every action of this nature is recorded by the system auditing component and reviewed for appropriateness.

### 5.1.1 Are different levels of access granted according to the position of the person who receives access? If so, please describe.

☑ Only certain authorized users can control the camera functions.

☑ Only certain authorized users can delete or modify footage

Authorization to delete or modify footage is done through a process which requires supervisor approval.

### 5.1.2 Are there written procedures for granting access to users for the first time?

☑ Yes (please specify) CBP Information Systems Security Policy & Procedures Handbook CIS HB 1400 05C sect. 6.3 Logical Access

☐ No

### 5.1.3 When access is granted:

☑ There are ways to limit access to the relevant records or technology

System Owners, supervisory staff and ISSOs will periodically review user access control lists and access levels for appropriateness and accuracy.

☐ There are no ways to limit access

### 5.1.4 Are there auditing mechanisms:

☑ To monitor who accesses the records?

☑ To track their uses?

### 5.1.5 Training received by prospective users includes discussion of:

☑ Liability issues

☑ Privacy issues

☐ Technical aspects of the system

☑ Limits on system uses

☑ Disciplinary procedures

☐ Other (specify)

☐ No training

The training lasts:

☐ None

☐ 0-1 hours

☐ 1-5 hours

☐ 5-10 hours

☑ 10-40 hours

☐ 40-80 hours

☐ more than 80 hours

The training consists of:

☑ A course

☑ A video

☑ Written materials

☐ Written materials, but no verbal instruction

☐ None

☑ Other (please specify) Computer Simulation

## 5.2 The system is audited:

☑ Once a week

There are procedures in place at the Network Operating Center to have IT system staff audit specific areas of the system on a daily to weekly basis.

### 5.2.1 System auditing is:

☑ Performed by someone within the organization

## 5.3 Privacy Impact Analysis

Privacy risks identified with respect to access and security were in appropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, CBP Code of Conduct and Disciplinary system, and the practice of least privileged access.

# Section 6.0 – External Sharing and Disclosure

*The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including federal, state and local government, as well as private entities and individuals.*

## 6.1 With which external entities is the information shared?

*List the name(s) of the external entities with whom the footage or information about the footage is or will be shared. The term "external entities" refers to individuals or groups outside your organization.*

- ☑ Local government agencies (on a need to know for the purpose of law enforcement or terrorism, investigations or prosecution)
- ☑ State government agencies (on a need to know for the purpose of law enforcement or terrorism, investigations or prosecution)
- ☑ Federal government agencies (on a need to know for the purpose of law enforcement or terrorism, investigations or prosecution)
- ☑ General public via Freedom of Information Act requests
- ☑ Other (please specify)

If an event occurs which requires other federal investigative groups participation, a case file will be provided, which may included recorded video. In the case of international partners, where appropriate, the sharing of hard copy case files occurs during regular coordinating meetings.

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

### 6.2.1 For each entity or individual listed above, please describe:

☑ The purpose for disclosure

Information may be disclosed to other investigative groups (federal, state, local, tribal, and foreign) for the purpose of law enforcement or terrorism, investigations or prosecution. Consistent with the video imagery associated with a law enforcement activity once it contains PII, public access to this information by the person to whom it pertains may be obtained through a FOIA request. Both TECS and ENFORCE, the law enforcement

systems in which the associated video, PII, and law enforcement activity information are maintained, are exempt from access under the Privacy Act.

## 6.3 How is the information transmitted or disclosed to external entities?

☑ Discrete portions of video footage shared on a case-by-case basis

☐ Certain external entities have direct access to surveillance footage

☐ Real-time feeds of footage between agencies or departments

☐ Footage transmitted wirelessly or downloaded from a server

☐ Footage transmitted via hard copy

☐ Footage may only be accessed on-site

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

☐ Yes

☑ No

☐ If an MOU is not in place, explain steps taken to address this omission. [Information sharing that occurs on a case-by-case basis is covered by a letter of authorization permitting the exchange of information and establishing the law enforcement conditions for use and possible further dissemination.]

## 6.5 How is the shared information secured by the recipient?

*For each interface with a system outside your operation:*

☑ There is a written policy defining how security is to be maintained during the information sharing under the "Chain of Custody" information sharing process.

☐ One person is in charge of ensuring the system remains secure during the information sharing (please specify)

☑ The external entity does not have the right to further disclose the information to other entities

## 6.6 Privacy Impact Analysis

When sharing information with third parties, the same specifications related to

security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the interface request and the implications on privacy related concerns are two factors that are included in both the initial and ongoing authorization. Should a recurring sharing arrangement between CBP and an external to DHS entity develop a written arrangement (MOU) and Interconnection Security Agreement would be negotiated to establish the terms of use and security for the exchanged data. The written arrangement specifies the general terms and conditions that govern the use of the functionality or data, including limitations on use. The Interconnection Security Agreement ("ISA") specifies the data elements, format and interface type to include the operational considerations of the interface. The written arrangements and ISAs are periodically reviewed and outside entity conformance to use, security and privacy considerations is verified before Certificates to Operate are issued or renewed. Such arrangements currently exist for the sharing of data within the TECS and ENFORCE systems.

# Section 7.0 – Notice

## 7.1 Is notice provided to potential subjects of video recording that they are within view of a surveillance camera?

Notice is provided in the form of public scoping sessions, environmental assessments and CBP town hall meetings. This PIA also serves to inform the public of the presence of video cameras at the border and the use of these cameras to detect and support the apprehension of persons crossing the border illegally.

# Section 8.0 – Technology

*The following questions are directed at analyzing the selection process for any technologies used by the video surveillance system, including cameras, lenses, and recording and storage equipment.*

## 8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

☑ Yes

☐ No

## 8.2 What design choices were made to enhance privacy?

☐ The system includes face-blurring technology

☐ The system includes blocking technology

☐ The system has other privacy-enhancing technology (Please specify)

☑ None

The system is intended to identify illegal entry into the United States. By definition, anyone who crosses the border at other than a defined port of entry is in violation of the law and prima facie is a violator.

## Responsible Officials

Dr. Kirk Evans

SBI*net* Program Manager

Department of Homeland Security

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of Regulations & Rulings, Office of International Trade, CBP, (202) 572-8790.

## Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security