Privacy Impact Assessment
for the

Biometrics Access Control System at the Transportation Security Lab

July 1, 2011

DHS/S&T/PIA-023

Contact Point
Thomas Jerdan
Transportation Security Laboratory
Science & Technology Directorate
609-813-2801

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Biometrics Access Control System is a building facilities access control system used at the Department of Homeland Security Science and Technology Directorate's Transportation Security Lab. The system relies on biometrics (fingerprint and iris recognition) to enhance the physical security of the lab and provides a demonstration of advanced technologies. The S&T TSL is conducting a Privacy Impact Assessment because personally identifiable information is collected during the testing and operational use of this system.

Overview

The core mission of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Transportation Security Laboratory (TSL) is to enhance homeland security by performing research, development, and validation of solutions to detect and mitigate the threat of improvised explosive devices. DHS S&T TSL is a resource for test and evaluation of new and emerging technologies in the field.

In fulfilling its mission, TSL is conducting operational testing on the Biometric Access Control Systems (BACS). Once the system is validated, TSL will deploy the system for operational use throughout the TSL facilities. The purpose of the BACS is to provide access control measures to the various facilities and laboratories on the TSL campus using biometric identifiers to ensure that only authorized employees, including contractors, have access to certain buildings and laboratories. Currently, employees of TSL use a contact smart card method of authentication for physical access to restricted areas of the facility. The contact smart card that resembles a credit card in size and shape are issued to individuals once they are certified to access specific laboratory locations**.** The smart cards' embedded microprocessor stores information on which specific buildings each individual is allowed access.

During the test and evaluation of BACS, TSL will implement a biometric system to run in tandem with the current contact smart card system to add an additional layer of physical security to laboratory locations. Once BACS is operational, the contact card system will only be used as a backup authentication system; BACS will become the primary access control system.

TSL will use two commercially-available biometric verification technologies, an iris image and fingerprint image recognition system, for the BACS. The system requires the user to present his/her finger or iris (depending on laboratory or building location) to the system, which is then saved and matched against a stored image, and employee information collected during prior enrollment process to verify the user's identity for authorized entry into laboratories and buildings, just as he/she would with a badge to access an entry point. Information collected during enrollment by the TSL system administrator includes name, phone number, email address, physical building location, and biometric (iris and/or fingerprint) template.

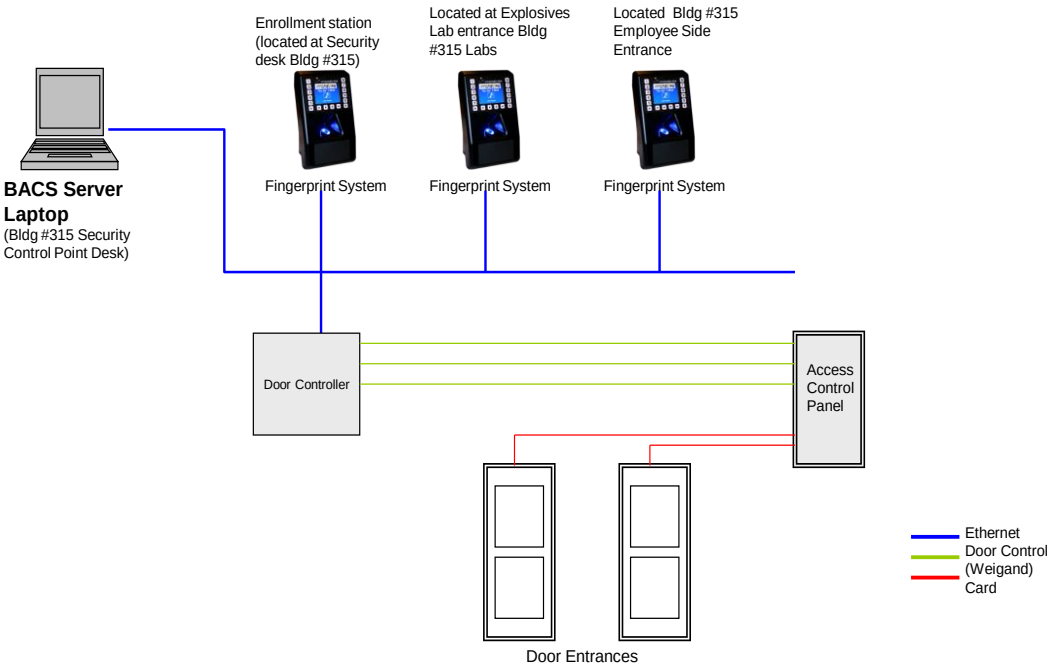
During the operational testing of the BACS, TSL system administrators will test and evaluate the system using TSL employees as voluntary participants. During this testing period, the voluntary participants will provide the TSL system administrators with their enrollment information. The participants provide their fingerprints and/or iris images, depending on the facility. The system

administrators use commercially-available technologies to capture and store the digital image of the fingerprints and/or iris scan. The system administrators will then match the enrollment information with the biometric information of the specific individual, which serves as the basis of identity verification. Throughout the course of the testing period, the participants will use the biometric system to access the TSL. For example, a volunteer will present their fingerprints to gain access to a building rather than their contact smart card.

After the operational testing of the BACS is complete, the TSL system administrators will analyze the research results, and make the appropriate changes to improve the operation and performance of the system. Once the testing phase is complete, the system administrators will determine when the system will be ready for operational deployment at TSL. TSL will transition the BACS to perform access control functions for the laboratories and buildings at the TSL campus. The BACS system will operate and function similarly, if not identically, to the system being tested. The enrollment information collected during the testing period will be maintained and used during the operational deployment of the system; this eliminates the need to recollect this information. If there are any changes to BACS after the test phase and before it becomes operational that impact the privacy protections detailed in this PIA, it will be updated to reflect those changes.

The BACS is a standalone system and is not connected to any other database or network during the testing and operational use of the system. The BACS system does not rely on any other network or system and will not be accessed remotely. During the testing and operational use, the BACS system is operated by TSL system administrators and security personnel who have completed DHS background and suitability investigations. Please see graphic below illustrating how each biometric access system works.

Innometriks Fingerprint System Diagram



Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland.

The Department's authority for this collection for the purpose of security of DHS property facilities is primarily 5 U.S.C. § 301 on Government Organizations and Employees; the Homeland Security Act of 2002; Executive Order (E.O.) 9397; E.O. 12968; and Title 41, Subtitle C, Chapter 101 Federal Property Management Regulations, issued July 2002.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) applies to the information?

DHS has issued Systems of Records Notice (SORN) DHS/ALL – 024 for DHS Facility and Perimeter Access Control and Visitor Management which covers the collection of enrollment and biometric information for the purpose of providing access control measures for government facilities.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The BACS system has a Security Plan (SP) in place and is maintained in DHS Trusted Agent FISMA (TAFISMA). The TSL-BACS SP will discuss the managerial, operational and technical controls that are in place to protect the system and the data contained within it. The SP will be in place for three years and then undergo a review. The SP also explains all preventative controls including physical security and technical safeguards, such as password protections and access controls, which are consistent with the information security and physical security requirements per DHS policy.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, the system is approved under General Records Schedule (GRS) 18, Item 22a for the retention of personal identity verification information, including biometric information, for no longer than five years after separation or transfer of the employee. However, when the TSL employee is no longer working at the facility, either during the pilot or operational use, the information is removed from the system.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This system administrator will only collect information from DHS employees and contractors working at TSL, therefore it is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The system administrator will collect and use employee and contractor names, work phone numbers, work email addresses, physical building locations, and biometric (iris and/or fingerprint) images.

2.2 What are the sources of the information and how is the information collected for the project?

The system administrator will collect this information directly from employees and contractors. Employees and contractors provide this information during the enrollment process into the system. This system will be a new system to enhance the access control to the restricted areas of the lab.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use any commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

During both the operational testing and operational use phases of the BACS, employees have the opportunity to verify with the system administrator that all information collected and stored in the BACS server is accurate by manually reviewing all enrollee accounts in the system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Risk: TSL may use the information for purposes other than what is stated in this PIA.

Mitigation: TSL will only collect and use the enrollment and biometric information of volunteers to test the operational effectiveness of the BACS system and, once deployed operationally,

provide access controls to various laboratories and buildings on the TSL campus. With the exception of cases involving law enforcement investigations, there are no other uses for this information. TSL will not collect any additional information, other than the necessary enrollment and biometric information, during the operational testing and use of the BACS.

Risk: Unauthorized disclosure of the information.

Mitigation: The data collected is located on a standalone server and uses current DHS information security software tools to lock down the system to ensure limited access to this information. System administrator(s) and DHS security personnel are the only users who have access to the system server.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

BACS provides TSL with an additional layer of security, helping verify only authorized DHS personnel enter building facilities.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

This system does not use technology to conduct search, queries or analyses.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Risks: Unauthorized users may view the stored enrollment and biometric information or use the information for unauthorized purposes.

Mitigation: Only authorized personnel with a need-to-know will have access to the enrollment and biometric information. In addition to the system administrator, authorized personnel include the information system security officer (ISSO) and the security personnel. The ISSO access the system to conduct weekly audits to ensure there is no suspicious activity or inappropriate use or access of the data. Security personnel will also have access to the information and the server system in order to operate the system. Access to the BACS will be restricted using user name and password protections.

Data may be shared with law enforcement on a case-by-case basis, such as an investigation of a potential security incident; requests of this nature will be coordinated through TSL security prior to disclosing the information.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

An official email message is distributed to all TSL employees and contractors. The email describes the purpose of the system, the data elements collected and used, and the security measures taken to protect the data. New TSL employees and contractors are provided this information during the orientation process.

A Privacy Act (e)(3) notice is also provided at the time of data collection.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All TSL federal employees and support contractors have a right to decline to provide information during the operational tests of the BACS. However, for the operational use of the BACS, if individuals decline to provide information they will not be processed for the enrollment portion, thus individuals will not be able to access particular buildings or areas of the lab. If an employee is unable to provide a usable fingerprint or iris scan, he/she can still access the TSL buildings using the smart card reader or be escorted by security personnel. The latter is the same procedure currently used when an employee's smart card is not working properly.

4.3 Privacy Impact Analysis: Related to Notice

Risk: Employees or contractors are not provided sufficient notification of data collection.

Mitigation: Notice will be provided to all individuals at the time of enrollment which includes background information on the system and its use as an additional measure of security for access control. The notice includes how the user's biometric information is used and retained for testing and/or operational use and an additional statement which cites S&T's legal authority to collect such information.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The data that is captured for this system are retained as long as the employee remains employed at the facility. The retention schedule allows the data to be retained for no longer than five years, however TSL policy provides that once the employee leaves, is terminated or access is no longer needed, their account information is deleted and no longer maintained on the system. This is done upon notification from the employee's supervisor or the TSL security staff and the data are then permanently deleted from the system. The system is reviewed weekly by the ISSO who works with the system administrator to ensure an accurate database is maintained.

There are no paper documents collected during the enrollment process into this system. The enrollment process is done in person with the system owner and employee.

5.2 Privacy Impact Analysis: Related to Retention

Risk: Data are retained indefinitely, even after the employee is no longer with TSL, putting it at risk for unauthorized disclosure.

Mitigation: Data are removed after the individual is no longer employed at TSL.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

TSL does not normally share this information with any external organizations. However, data may be shared with law enforcement on a case-by-case basis, such as an investigation of a potential security incident.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Sharing information with law enforcement agencies is compatible with DHS/ALL-024 SORN, routine use J.

6.3 Does the project place limitations on re-dissemination?

TSL may share information during investigations conducted by law enforcement on a case-by-case basis.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

TSL does not share this information with any external organizations except as noted above. If law enforcement requires data on this system they will work through TSL security who ensure requests are in writing and maintained on file by the system owner.

6.5 Privacy Impact Analysis: Related to Information Sharing

Risk: Information may be disclosed to external entities, who may use information for unauthorized purposes.

Mitigation: TSL only shares information in limited situations of supporting law enforcement investigations. TSL shares information on a case-by-case basis, and in accordance with the DHS/ALL-024 SORN.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals can contact the system administrators if they wish to obtain access to their information.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The employee confirms at the time of data collection that their information is correct.

The employee can contact the system administrator who will make any changes to the system if there any typographical or inaccurate data provided by the employee at the time of data collection. If during both the testing or after the system is deployed, an employee is somehow unable to provide a viable fingerprint or iris image, the card reader access is still available. Also, in the event an access card cannot be issued to the employee, the TSL security staff will provide escorted access to the areas the employee is cleared to enter.

The data is reviewed by the system administrator to ensure accuracy of the data entered into the system. Also, the system ISSO reviews the system weekly and looks for inaccuracies.

7.3 How does the project notify individuals about the procedures for correcting their information?

The system administrators will provide their contact information at the time of data collection and inform employees to contact them with questions or to correct collected information. The system administrator will also confirm data accuracy before the employee's BACS account is finalized.

The employee is notified via email that a change has been made to the system and to contact the system administrator for specific details.

7.4 Privacy Impact Analysis: Related to Redress

Given the available procedures for correcting inaccurate or erroneous information described above, no additional redress mechanisms are provided. Individuals will have the opportunity to correct any inaccurate or erroneous information by working directly with system administrators and their supervisors.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Only the system administrators, ISSO, and security officers will have access to the information in the BACS. System administrators and security officers are required by DHS policies to abide by all privacy and information security regulations. The TSL ISSO has access to the system to perform weekly audits.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All employees receive the DHS privacy and information security training annually. This is a mandatory requirement and the training records are maintained by the facility's human resources staff and the ISSO.

8.3 What procedures are in place to determine which users may access the information and how does the project determined who has access?

Access to the BACS database is limited to the system administrator, the ISSO, and security officers. Ultimately, the system owner controls who is granted access to the system.

Additionally, safeguards are in place to limit unauthorized access to the system. BACS is hosted on a computer that automatically encrypts all data. The computer is secured physically with a cable and/or within a locked cabinet that only the system administrator can unlock.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

BACS information is not shared outside of TSL other than the case-by-case law enforcement sharing identified in section 6.1. Therefore, no sharing agreements or MOUs are needed.

Responsible Officials

Thomas Jerdan

TSL Security Officer

Department of Homeland Security

Science & Technology Directorate

Transportation Security Laboratory

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security