



Privacy Impact Assessment
for the

**Air Entry/Exit Re-engineering (AEER)
Counting and Measuring (C&M) Project**

DHS/S&T/PIA-030

November 30, 2015

Contact Point

Arun Vemury

Apex AEER Program Director

Science and Technology Directorate

(202) 254-6830

Reviewing Official

Karen Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

One of the Department of Homeland Security's (DHS) primary missions is to facilitate legitimate travel and trade. To help achieve this goal, the DHS Science & Technology (S&T) Directorate and U.S. Customs and Border Protection (CBP) are implementing a short-term Counting and Measuring (C&M) Project at Washington Dulles International Airport for 12-14 months. The C&M project is a research, development, test, and evaluation project that assesses the accuracy and effectiveness of commercially available automated tools to determine the wait times and dwell times of international travelers arriving in the United States who enter through the airport's Federal Inspection Service (FIS) area. DHS S&T is conducting the C&M Project as a part of the existing Air Entry/Exit Reengineering Program. S&T is conducting a Privacy Impact Assessment (PIA) to address the steps taken to minimize the privacy risks of the C&M Project.

Introduction

The United States National Travel and Tourism Strategy¹ outlines a series of initiatives to enhance travel and tourism to the United States and provide an efficient and positive international arrivals experience, while ensuring the security of the U.S. borders and safety of the traveling public. To help achieve this goal, the DHS Science & Technology (S&T) Directorate and U.S. Customs and Border Protection (CBP) are implementing a short-term Counting and Measuring (C&M) Project at Washington Dulles International Airport for 12-14 months. The C&M Project will assess the accuracy and effectiveness of commercially-available automated tools to determine the wait times and dwell times² of international travelers arriving in the United States in the airport's Federal Inspection Service (FIS) area.³ The FIS area is designated for processing passengers, crew, and their baggage and effects arriving from, or departing to, foreign countries. The FIS coverage area includes, but is not limited to, the deplaning area, ramp area, international cargo facilities, and other restricted areas designated by the Port Director.

CBP is continually adapting to meet the significant anticipated annual increases in traveler volumes by exploring new ways to manage traveler flows through the FIS area. The

¹ National Travel and Tourism Strategy, International Trade Administration, Office of Travel and Tourism Industries (2012), available at <http://travel.trade.gov/pdf/national-travel-and-tourism-strategy.pdf>.

² Wait time is the measure of the time a traveler is waiting in a queue prior to each stage of the process. Dwell time is the measure of the time a traveler spends at each stage of the process (*i.e.*, the time the travelers spends in a line versus the time the traveler spends waiting for a bag at baggage claim.)

³ The Federal Inspection Services area is designated for processing passengers, crew, and their baggage and effects arriving from, or departing to, foreign countries. The FIS coverage area includes, but is not limited to, the deplaning area, ramp area, international cargo facilities, and other restricted areas designated by the Port Director.



C&M Project supports this goal by establishing objective metrics to evaluate the number of travelers passing through the FIS area, identify process bottlenecks, and improve CBP staffing efficiency within the FIS area. Counting and measuring solutions may also be leveraged to objectively measure the impact of other airline passenger entry transformation initiatives. These technologies have previously been tested by the Transportation Security Administration (TSA) to measure passenger screening wait times.⁴ The technologies are currently used by state and local governments to measure traffic volumes.⁵

S&T is conducting the C&M Project as a part of the existing Air Entry/Exit Reengineering Program.⁶ “Counting and measuring” refers to capturing traveler volumes and wait time information to increase CBP’s operational awareness within the FIS area. To capture traveler volumes and wait times, S&T will automatically count travelers entering the FIS area and measure the amount of time travelers spend in queues and completing tasks associated with the international traveler arrivals process. Automating this measurement process will provide real-time information to CBP Officers, enable recognition of process bottlenecks and delays, and potentially help CBP determine where to assign officers and resources.

Bluetooth & Wi-Fi

The project will use Bluetooth and Wi-Fi technologies. Bluetooth and Wi-Fi are short-range wireless technologies allowing enabled devices to communicate with one another.⁷ Every Bluetooth or Wi-Fi-enabled device is assigned a unique Media Access Control (MAC) address by the device manufacturer to allow other devices to recognize and establish communications. Devices continuously broadcast their MAC addresses in order to alert other enabled devices or sensors to their presence. There will be a specified starting point and end point of a queue, thus the queue will not account devices considered to be outside of that zone. The MAC addresses cannot be detected when the Bluetooth or Wi-Fi signal is disabled on the devices or when the devices are powered off.

The MAC addresses detected by Bluetooth and Wi-Fi sensors are scrambled or “hashed” in two steps. First, the detected MAC address is hashed using a hash key⁸ in the sensor, then a second hashing is made by the server, which will only provide anonymized aggregate timing

⁴ DHS/TSA/PIA-037 Automated Wait Times (AWT) Technology Privacy Impact Assessment, (August 3, 2012) at http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_tsa_awt_august2012.pdf.

⁵ See <http://www.wired.com/2011/03/cell-phone-networks-and-the-future-of-traffic/>.

⁶ See DHS/S&T/PIA-028 Air Entry/Exit Re-engineering (AEER) Project (May 28, 2014), available at <http://www.dhs.gov/sites/default/files/publications/privacy-pia-aeer-may-2014-signed.pdf>.

⁷ While S&T cannot predict the percentage of the traveling public that carry these devices, the International Data Corporation (IDC) forecasts that 87% of all phone sales in 2017 will be smartphones. This figure does not include internet, and other Bluetooth/Wi-Fi enabled devices.

⁸ A hash key or hash function is any function that can be used to change digital data of arbitrary size to different digital data of fixed size.



data results and trends to DHS. Only hashed data is transmitted to the server. The hash key is modified daily to minimize the possibility of re-identifying the MAC address.

People Counter

People counter systems are low-resolution thermal, infrared, vertical imaging systems that use one or more sensors to detect the movement of heat sources or shapes caused by people moving through an area. The thermal sensors are mounted overhead to detect heat source from a human and determine the number of people passing through a specified area. The sensors will only be able to discern heat source or moving shapes and will not be able to collect any personal identifiable information.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure the Homeland.

DHS conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that the C&M Project is a CBP and DHS S&T initiative, rather than a particular information technology system, DHS is conducting this PIA to examine the privacy impact of the C&M Project as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.



The C&M Project is being deployed at Washington Dulles International Airport for 12-14 months. The project is expected to begin in December 2015 and end in February 2017. The AEER C&M Project counts the number of international travelers within various queues in the FIS area as well as measures traveler wait and dwell times in this area.

The test system for the C&M Project consists of one or a combination of sensor types including Wi-Fi, people counters, and Bluetooth sensors. Each sensor collects a different set of information. The data captured by each sensor type are described below:

Bluetooth

- Media Access Control (MAC) address of device with enabled Bluetooth communication; and
- Date and timestamp of MAC address seen by sensor.

Wi-Fi

- MAC address of device with enabled Wi-Fi communication; and
- Date and timestamp of MAC address seen by sensor.

People Counter (e.g., low resolution thermal, infrared, vertical imager)

- Count of people passing through the count line; and
- Date and timestamp each object passing through the preset sensor line.

Examples of captured images from thermal, infrared, and vertical imager systems are shown in the Figure 1 & 2.

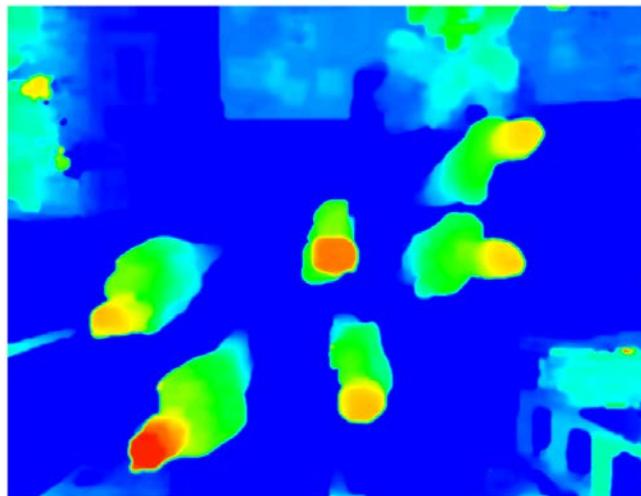
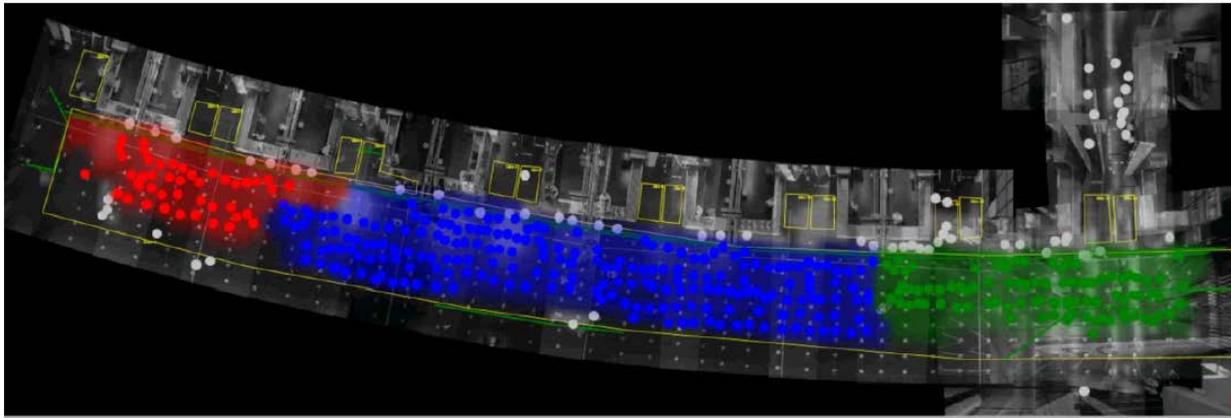


Figure 1. Thermal Sensor Feed Example



Name	Queue Length	Wait. Back.	Wait. Forw.	Out Flow
■ Business	44	3m	3m	674
■ Eco	205	8m	9m	1173
■ Transfer	91	6m	7m	729

Figure 2. Vertical Imager Sensor Feed Example

To provide notice to the public regarding the information collected as part of this project, S&T and CBP will post the following signage in the FIS area where the test will take place for the duration of the test period.

Signage such as the following or substantially similar will be used:

Wait Time Analysis

DHS is using Bluetooth and Wi-Fi technology in this area to calculate wait times. If you do not wish to participate, you can disable your Bluetooth and Wi-Fi connection. DHS encrypts the device's addresses and deletes all data within 24 hours. For more information please see the DHS website (<http://www.dhs.gov/privacy-documents-st>).

Privacy Risk: There is a privacy risk that individuals passing through FIS area at airports may be unaware that their information is being used for testing purposes by DHS.

Mitigation: This risk is mitigated by the signage that S&T and CBP will provide at the airport test locations. The signage will be posted at the entrance of FIS area after passengers deplane and enter the airport. CBP Officers within FIS area will also be trained to assist passengers if they have questions or concerns about the test or notice provided. S&T and CBP are also providing general notice to the public about this new test through the publication of this PIA.



Privacy Risk: There is a privacy risk that despite posted notice, individuals passing through FIS area are arriving from international destinations and therefore may not understand technical signage in English.

Mitigation: This risk is partially mitigated. S&T and CBP will provide signage in two or three languages, other than English, based on the most popular languages spoken by passengers arriving at the test FIS area locations. CBP will determine which languages should be used based on regularly collected international traveler language statistics. However, despite translation into multiple, popularly spoken languages, there is still a risk that some travelers will be unable to understand the posted notice.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

The C&M project's test system is only identifying total numbers of travelers and wait times. No traveler names are being collected, used, or linked to the MAC address. Signage posted at the entrance of the FIS area advises those travelers who wish to opt-out of any mobile data collection from this field trial may do so by disabling the Bluetooth and Wi-Fi connection on their mobile devices or by turning their mobile devices off. Instructions on how to disable the device is not provided as devices will have different interfaces/operations.

Privacy Risk: There is a privacy risk that S&T and CBP have not provided individuals with instructions on how to opt-out of this information collection.

Mitigation: Individuals do not have an opportunity to opt-out of passing through FIS area upon arrival at an airport, consistent with CBP's border security authorities for determining traveler's admittance into the United States. However, individuals do have the opportunity to opt-out of this test and information collection by either disabling the Bluetooth and Wi-Fi connections on their mobile devices or simply powering off their devices while in the FIS area.

S&T and CBP are not providing explicit directions for how to opt-out of this information collection because mobile devices vary in how to disable the Bluetooth or Wi-Fi connections. Because S&T and CBP are collecting aggregate information to determine wait and dwell times within FIS area, and because the mobile device identification information will not be linked back to an individual, this risk is minimal.



3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The test and evaluation activities for Apex AEER Program C&M Project are being conducted based on the authority established in the Homeland Security Act,⁹ which authorizes DHS S&T 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 research and development related to improving the security of the Homeland.

Consistent with this authority, S&T (in coordination with CBP) is conducting the C&M Project to assess the accuracy and effectiveness of commercially-available automated tools to determine the wait times and dwell times of international travelers arriving in the United States in the airport’s FIS area. The C&M Project will establish objective metrics to evaluate the number of travelers passing through the FIS area, identify process bottlenecks, and improve CBP staffing efficiency within the FIS area.

Because the C&M Project has a limited duration with clearly defined objectives, consistent with S&T’s authority to conduct research and development for any component of DHS, there is no privacy risk to purpose specification.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The C&M Project has been designed to minimize the retention of PII by S&T and CBP by limiting the retention period of the information, and by relying on aggregate information for the testing and evaluation. All hash keys are disposed of every 24 hours and all hash data shall be disposed of at the end of testing. The following data are linked to individual devices and stored for queuing management analysis:

⁹ P.L. No. 107-296, § 302(4), available at (http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf).



Bluetooth Sensor:

- Calculated dwell or queue time per device;
- Device profile data tag (e.g., Automated Passport Control (APC) queue, Foreign Visitors queue, Global Entry queue);
- Median and/or mean queue times and dwell time; and
- Sample counts of captured devices over a period of days, weeks, and months during times international flights arrive.

Wi-Fi Sensor:

- Calculated dwell or queue time per device;
- Device profile data tag, which determines travelers queue location by sensor location with strongest signals (e.g., APC, Visitors, Global Entry);
- Median and/or mean queue times and dwell time; and
- Sample counts of captured devices over a period of days, weeks, and months during times international flights arrive.

People Counter Sensor:

- Sensor Counts (number of people counted by the sensor over time).

C&M Test System Management:

- System Operator (DHS staff (S&T, CBP) and contractors) user profiles and application level accounts;
- Application configuration settings; and
- Access to the data collection server and database are restricted to project staff.

Privacy Risk: There is a risk of overcollection of mobile device signal information if the CBP Officers who are in the FIS area have personal mobile devices with them.

Mitigation: Since this project measures the time it takes for a particular hashed MAC address to move through the FIS area, CBP Officer MAC addresses would be outliers during their multi-hour shifts.

There is no risk of overcollection of information from passersby because the information is only collected from travelers within the designated FIS area queue. This is a controlled area that members of the public cannot access unless they have de-planed an international flight.



5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The C&M Project is designed to calculate FIS area queue wait times. C&M Project data are not used for any other purpose than as discussed in this PIA. Wait time calculations will be used for statistical purposes to inform CBP staffing and configuration decisions. Individual MAC addresses are not retained and therefore cannot be used for any purpose other than conversion by one-way hash, and the hashed address is only used to calculate wait time. The MAC addresses detected by Bluetooth and Wi-Fi sensors are scrambled or “hashed,” and only hashed data is transmitted to the server. The hash key is modified daily to minimize the possibility of re-identifying the MAC address. The MAC address is further obfuscated by being immediately hashed such that S&T cannot identify the original MAC address. The hashed address is deleted after twenty-four hours. The thermal sensors are mounted overhead to detect heat source from a human and determine the number of people passing through a specified area. The sensors will only be able to discern heat source or moving shapes and will not be able to collect any PII.

The set of collected data shall only be used by DHS S&T, CBP, and its contractors to analyze the effectiveness of the C&M Project system to determine traveler volume, queue times, and dwell times. All MAC addresses and associated hash data shall be disposed of within 24 hours.

Due to the limited collection of information, the minimal retention period, and the limited number of individuals who have access to this information, there is no privacy risk for use limitation.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The C&M Project only uses information that is publicly broadcast by a traveler’s Bluetooth or Wi-Fi enabled device. Accordingly, it is accurate, timely, and complete, and is directly relevant to wait time calculations.

Privacy Risk: There is a privacy risk that S&T will rely on inaccurate data to generate research and test evaluation results.



Mitigation: All research and development efforts face this risk. S&T relies on established research and development methodologies to ensure to the extent possible that the data used to determine test outcomes is accurate and useful. This risk is also minimized because S&T and CBP are collecting information directly from individuals as they make their way through the FIS area, as opposed to relying on estimates based on images from closed circuit television (CCTV) which are not as accurate, timely, or reliable.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The MAC address is detected, hashed twice, and the hash identifier is deleted after 24 hour period at the servers. Hash data will be stored in the contractor's database for analysis and data accuracy validation purposes. All hash data will be deleted at the end of testing. Data in the system is protected in accordance with DHS 4300A Sensitive Systems Handbook. The system requires an account name and password for access. All data transmitted between the sensors, servers, and database is encrypted with Secure Sockets Layer (SSL)¹⁰ protocol. The SSL protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

Due to the limited collection of information, the minimal retention period, and the security safeguards in place, there is no privacy risk to the security of the information.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All S&T program managers, contractors, and CBP staffs receive privacy awareness training on an annual basis. All project staffs are required to abide by DHS information security requirements. There is no privacy risk to accountability and auditing for the C&M Project.

¹⁰ *Secure Sockets Layer (SSL)* is cryptographic protocols designed to provide communications security over a computer network.



Conclusion

The Apex AEER Program C&M Project tests, evaluates, and develops technologies to implement a robust counting and measuring capability in the FIS area that could be used to improve situational awareness and support ongoing process improvement under the National Travel and Tourism Strategy. This capability has been tested by TSA¹¹ to measure passenger screening wait times, and other airports around the world. The C&M Project helps create a set of metrics and baseline for a nationwide strategy to enhance travel and tourism.

Responsible Officials

Arun Vemury
Apex AEER Program Director
Science & Technology Directorate
(202) 254-6830

Approval Signature Page

Original signed copy on file with DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

¹¹ DHS/TSA/PIA-037 Automated Wait Times (AWT) Technology Privacy Impact Assessment, (August 3, 2012) available at http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_tsa_awt_august2012.pdf.