From: (b)(6); (b)(7)(C)
Sent: 2 Mar 2020 17:44:49 +0000
To: (b)(6); (b)(7)(C)
Subject: Enforcement Integrated Database (EID), EAGLE PIA, July 25, 2012
Attachments: PIA Update, ICE EID EAGLE 20120725 [signed].pdf, EID Update EAGLE 1 5 (LMR 07 23 2012).docx, EID Update EAGLE 1 5 (HSI 07 19 2012).docx, RE: EID PIA Update for EAGLE

Hi (b)(6); (b)(7)(C)

I have attached the Enforcement Integrated Database (EID), EAGLE PIA, July 25, 2012 that is here in the shared drive at (b)(5); (b)(7)(E) Update (EAGLE 1.5 ABIS) and available on DHS Privacy public website at https://www.dhs.gov/sites/default/files/publications/PIA%20Update%2C%20ICE%20EID%20EAGLE%20120725%20%5Bsigned%5D.pdf

I have also attached what appears to be the most recent draft before this PIA was published. I have also attached the most recent draft received from HSI, and OPLA before this PIA was published.

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (b)(6); (b)(7)(C)
Main: (

Privacy Impact Assessment Update
for the

Enforcement Integrated Database (EID) – EAGLE

DHS/ICE/PIA-015(e)

July 25, 2012

Contact Point
James Dinkins
Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

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

Abstract

U.S. Immigration and Customs Enforcement (ICE) has established a new subsystem within the Enforcement Integrated Database (EID) called EID Arrest Guide for Law Enforcement (EAGLE). EAGLE is a booking application used by ICE law enforcement officers to process the biometric and biographic information of individuals arrested by ICE for criminal violations of law and administrative violations of the Immigration and Nationality Act (INA). Once fully deployed, EAGLE will replace the existing EID booking applications the Enforcement Apprehension and Booking Module (EABM), Mobile IDENT, and WebIDENT and will perform the identical functions of those applications as described below and in the EID PIA. EAGLE will also forge a new connection to the Department of Defense's (DOD) Automated Biographic Information System (ABIS) and permit the comparison of the fingerprints of foreign nationals arrested by ICE with the DOD's information in ABIS. This PIA Update is being conducted to provide public notice of the operation of the EAGLE booking system and its interconnection to the DOD ABIS database.

Overview

ICE has launched a new booking application known as EAGLE within the EID, an ICE-owned shared common database repository for several DHS law enforcement and homeland security applications.[1] EID captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and U.S. Customs and Border Protection (CBP). EAGLE is the booking application used to process the biometric and biographic information of individuals arrested by ICE Homeland Security Investigations (HSI) Special Agents for violations of law and ICE Enforcement and Removal Operations (ERO) officers to support bookings of individuals arrested for criminal and administrative violations of the INA and related laws. ICE Office of Professional Responsibility (OPR) agents also will use EAGLE to support bookings of individuals for criminal violations of law investigated by OPR.[2]

Once fully deployed, EAGLE will replace the EID booking applications EABM, Mobile IDENT, and WebIDENT and will perform the identical functions of those

[1] The specific ICE applications are EABM, ENFORCE Alien Removal Module (EARM), Enforcement Automated Biometric Identification System (WebIDENT), Mobile IDENT, and the User Account Management Module. The CBP application is called E3.

[2] ICE OPR is responsible for investigating allegations of employee misconduct.

applications as described below and in the EID PIA.[3] EAGLE will also connect to DOD's ABIS and permit the comparison of the fingerprints of foreign nationals arrested by ICE with DOD's information in ABIS.

EAGLE as Replacement for EABM, Mobile IDENT, and WebIDENT Applications

Once fully deployed, EAGLE will perform all functions of the EID booking applications EABM, Mobile IDENT, and WebIDENT and permit the retirement of those applications from the EID environment. The specific data collected, uses of the data, and information sharing undertaken pursuant to EAGLE will not change from these prior applications. EAGLE will provide a single integrated arrest and booking application that supports fingerprint/photograph capture, collection of biographic information, recording of allegations and charges, preparation and printing of appropriate forms, and interfaces with the three major U.S. government biometric databases for the enrollment and query of fingerprints.[4] EAGLE will be used to track the apprehension of individuals, both U.S. citizens and foreign nationals, who have been arrested by ICE, CBP, or other law enforcement officers within DHS for violations of criminal or administrative laws, including the INA (Title 8, United States Code).

EAGLE will also support the creation of records about individuals who are amenable to immigration removal proceedings but are not in the custody of DHS. These subject records may be used as part of an ongoing investigation and sometimes are used to place immigration detainers when DHS is seeking custody of an alien who is already in the custody of another federal, state, or local law enforcement agency. EAGLE will also support the query of fingerprints of individuals who are the subjects of ongoing criminal investigations to identify previous encounters. These queries do not result in the enrollment of an individual's fingerprints in IDENT or the creation of a new encounter in IDENT, but, for previously enrolled fingerprints, the DHS law enforcement officer may set an alert in IDENT that will notify him or her if the individual is encountered again.

Like its predecessor applications, EAGLE will submit biographic information, fingerprints, and arrest information to the FBI's IAFIS biometric database for storage and for fingerprint-based criminal records checks. EAGLE will receive the results of the fingerprint check from IAFIS, including any criminal history information or wants and warrants on the individual. EAGLE will also submit biographic information, fingerprints, photographs, and arrest/encounter information to the DHS IDENT biometric database for enrollment and query. EAGLE will receive the results of the IDENT check, which

[3] *See* DHS/ICE/PIA-015 EID PIA (Jan. 14, 2010) for a full description of the functions of EABM, Mobile IDENT, and Web IDENT.

[4] The three databases are DHS's Automated Biometric Identification System (IDENT), the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS), and the Department of Defense's Automated Biographic Information System (ABIS).

include any matching biographic information, Fingerprint Identification Number, photographs, and previous encounter information. EID uses the Fingerprint Identification Number to identify EID records that may be about the same person, enabling the user to determine whether to link the records. EAGLE also has the ability to retrieve additional information from U.S. Department of State (DoS) databases pertaining to visa issuance and passport data based off of the fingerprint match.

EAGLE also supports arrest processing and fingerprint checks from DHS law enforcement officers in the field via mobile device. This technology allows DHS personnel to determine a subject‘s immigration status, check for prior criminal history, and check for wanted subjects in the field without driving long distances to DHS offices, thereby improving booking times and enabling any appropriate release from law enforcement custody onsite.

New Connection with ABIS

EID/EAGLE will send the fingerprints of arrested foreign nationals to ABIS for matching purposes only. ABIS will not retain (enroll) the fingerprints. Any matching fingerprints in ABIS will trigger an automated message from ABIS to EID/EAGLE containing biographic information about the individual and limited information about why the individual's fingerprints are in ABIS. An individual's fingerprints may be in ABIS based on derogatory information about the individual, such as a known criminal history, intelligence justification, or as a known or suspected terrorist. Alternatively, an individual's fingerprints may be in ABIS after DOD or its partners fingerprint the individual and compare the prints against ABIS for purposes of base access, employment, benefits, or other administrative reasons. Finally, DOD also includes in ABIS fingerprints from historical sources, such as criminal fingerprint records from the Iraqi government. These historical records may reflect derogatory information about the individual, or simply contain identification data only.

The response from ABIS will be retained in EID/EAGLE and used by ICE law enforcement personnel to identify the individual. Encounter information may be used to question the individual or develop leads during the course of the investigation or law enforcement activity in which the individual was arrested. The EAGLE application may be used by any ICE office that arrests individuals, including HSI, ERO, which arrests individuals for criminal and administrative violations of the INA, and OPR, which conducts internal investigations into suspected misconduct or criminal activity.

Reason for the PIA Update

This update is necessary to describe the launch of the new EAGLE application and the new connection to the DOD ABIS biometric database to compare fingerprint records with those maintained in ABIS. An update to the EID PIA is required to maintain public transparency and to identify and assess privacy risks associated with this new connection.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

DHS has been authorized to collect information under 5 U.S.C. § 301; 8 U.S.C. § 1103; 8 U.S.C. § 1225(d)(3); 8 U.S.C. § 1324(b)(3); 8 U.S.C. § 1357(a); 8 U.S.C. § 1360(b); 19 U.S.C. § 1; and 19 U.S.C. § 1509. Additional authority is provided in 6 U.S.C. § 202; 8 U.S.C. §§ 1158, 1201, 1365a, 1365b, 1379, and 1732; and 19 U.S.C. §§ 2071, 1581-1583, and 1461; and the Immigration Reform and Immigrant Responsibility Act of 1996.

The DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) System of Records Notice (SORN) (75 Fed. Reg. 23,274, May 3, 2010) applies to the information collected and maintained by EID/EAGLE. A system security plan has been approved for EID and the system was granted an Authority to Operate which expires on January 29, 2013. The EID system operates under a records retention schedule approved by the National Archives and Records Administration (NARA). The Paperwork Reduction Act does not apply to the information collected by ICE during the criminal or administrative arrest of an individual.

Characterization of the Information

With this update, EID will now receive and maintain the results of biometric-based record checks on arrested foreign nationals from a new source, ABIS.[5] The ABIS response will consist of biographical/identifying information including a photograph where available; any derogatory information such as criminal history, known/suspected terrorist status, or intelligence-based information; date, time, and location of any DOD encounter that triggered the fingerprinting; and the reason for fingerprinting, such as base access, employment, or benefit application. In the case of historical fingerprint records loaded into ABIS, the ABIS results will consist of a brief descriptor of the historical source and an actual image of the fingerprint card itself. The results information will be sent to EID via a secure electronic connection with ABIS.

There is a risk that the ABIS data returned to EID/EAGLE may not be accurate or complete for several reasons. First, not all of the data is collected by DOD but may

[5] As described in the DHS/ICE/PIA-015 EID PIA, EID already maintains the results of biometric-based record checks against the DHS Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS).

originate from other sources whose data collection methods are not known or subject to review. Second, DOD-collected data is not subject to system-enforced uniform standards of labeling in ABIS, which could interfere with accurate interpretation of the results by EID/EAGLE users. Finally, DOD's national security and national defense reasons for collecting and using this data do not necessarily require that the information be accurate or complete, therefore systems and processes may not have been established to emphasize data integrity to the same degree as government biometric data systems used for other purposes.

This risk is mitigated by the fact that DHS will not rely on the ABIS results to make determinations about the individual. The individuals queried against ABIS have already been encountered and arrested or detained by DHS personnel, and DHS will primarily use the ABIS results to help confirm or otherwise identify the individual. DHS will use any additional information received from ABIS, derogatory or otherwise, only as a source of potential leads and not as evidence or a basis for a decision about the individual's case. In addition, DHS personnel will be able to contact DOD for assistance interpreting ABIS results in the event that the contextual information (*e.g.*, reason for fingerprinting) is unclear.

Uses of the Information

ICE will use the results of biometric-based record checks to identify individuals who were previously encountered by the DOD. The ABIS results will provide information about the individual's identity and the circumstances of the previous DOD encounter. ICE will use this information to better identify the individual. ICE may also use the information about where and when the DOD encountered the individual as a source of potential leads in the context of an ICE investigation or other law enforcement action in which the individual was arrested, but will not use it as evidence in prosecution or as a basis for a decision about the individual's case.

Notice

No new notice to the individual is required. Generalized notice of the fact that the system is now comparing booking fingerprints with ABIS is provided by this update.

Data Retention by the project

With this update, there is no change to the record retention policy for EID. The ABIS results will be maintained along with the other booking/arrest data in EID for 100 years, pursuant to the approved records retention schedule.

Information Sharing

EID EAGLE will now send to ABIS the fingerprints, Fingerprint Identification Numbers, and gender of foreign nationals arrested by ICE and booked using the EAGLE application. This transmission will occur via a Secure FTP connection between EID and ABIS governed by an Interconnection Security Agreement that details the security protocols and requirements in accordance with DOD and DHS security policies. DOD will not retain the queries or enroll the fingerprints sent to ABIS by ICE, but will retain an audit trail that indicates a query was performed. This sharing is authorized under an information sharing agreement between DHS and DOD, and under a Privacy Act routine use in the DHS/ICE-011 ENFORCE SORN which authorizes disclosure "to other federal, state, local, or foreign government agencies, individuals, or organization during the course of an investigation, proceeding, or activity within the purview of immigration and nationality laws to elicit information required by DHS/ICE to carry out its functions and statutory mandates."

Because DOD does not retain this data but only uses it to run a biometric comparison and return any matching results to ICE, there is no new privacy risk associated with the disclosure of this data to DOD. The communication channels between ICE and DOD are appropriately secured using encryption, thereby minimizing the risk of compromise or interception when Personally Identifiable Information (PII) is being sent between the DHS and DOD networks.

Redress

With this update, there is no change to an individual's rights of access, redress, and correction.

Auditing and Accountability

Access to EAGLE is the same as users who access EID, as described in the EID PIA and subsequent updates thereto. ICE is providing training to EAGLE users to ensure the proper use of the system. Otherwise, system auditing and oversight controls have not changed.

Any new information sharing agreements, Memoranda of Understanding (MOUs), new uses of the information, or new accesses to the system by organizations within DHS and outside would be controlled by the EID governance process. The ICE Privacy Office participates in this governance process and would coordinate on the initiation of any new projects or initiatives that have a potential impact on privacy.

Responsible Official

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Page 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 25

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6); (b)(7)(C) on behalf of OPLA Tasking
Sent: 21 Jun 2012 13:45:37 -0400
To: (b)(6); (b)(7)(C)
Cc: OPLA Tasking
Subject: RE: EID PIA Update for EAGLE
Attachments: EID Update EAGLE 1 5 (toOPLA 06 06 2012) (CLS Comments and Edits) (2).docx

(b)(6); (b)(7)(C)

OPLA concurs with the document and provides edits. The comments in the document are for awareness only. OPLA does not need to review the document again. Cleared by (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) Chief of Staff, ext. 2-5000.

Thank you,

(b)(6); (b)(7)(C) Associate Legal Advisor

Executive Communications Unit
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Desk: (b)(6); (b)(7)(C)
Mobile (b)(6); (b)(7)(C)
EMail: (b)(6); (b)(7)(C)

*** Warning *** Attorney/Client Privilege *** Attorney Work Product ***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

From: (b)(6); (b)(7)(C)
Sent: Wednesday, June 06, 2012 4:54 PM
To: #ICEOPLATaskings
Subject: EID PIA Update for EAGLE

OPLA,

I am requesting review and written concurrence via email of the attached EID PIA Update.

Response requested by COB June 20th.

Privacy POC for this is me.

(b)(6); (b)(7)(C)
Assistant Director for Privacy & Records
Privacy Officer
U.S. Immigration & Customs Enforcement
Office - (b)(6); (b)(7)(C) | Direct - (b)(6); (b)(7)(C)
Intranet website: (b)(6); (b)(7)(C)

Page 28

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 29

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 30

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 31

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 32

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 33

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 34

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 35

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6); (b)(7)(C)
Sent: 25 Mar 2020 15:58:28 +0000
(b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: FBI's biometric database - NGI

Good afternoon,

(b)(5)

Thanks, (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 5 Dec 2019 13:28:51 +0000
To: (b)(6); (b)(7)(C)
Subject: RE: DHS proposes expanding facial-recognition scans to US citizens

Very interesting, thanks (b)(6);

From: (b)(6); (b)(7)(C)
Sent: Wednesday, December 4, 2019 5:09 PM
(b)(6); (b)(7)(C)
Subject: DHS proposes expanding facial-recognition scans to US citizens

I don't know if this came up in the facial recognition session at the Federal Privacy Summit, but this was in the news yesterday in case anyone hasn't seen it yet,

https://techcrunch.com/2019/12/02/homeland-security-face-recognition-airport-citizens/2019/12/02/homeland-security-face-recognition-airport-citizens/

https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=1651-AB22&=biometric-collection-data-citizens

RIN Data

DHS/USCBP **RIN:** 1651-AB22 **Publication ID:** Fall 2019
Title: Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States
Abstract:

The Department of Homeland Security (DHS) is required by statute to develop and implement a biometric entry-exit data system. To facilitate the implementation of a seamless biometric entry-exit system that uses facial recognition and to help prevent persons attempting to fraudulently use U.S. travel documents and identify criminals and known or suspected terrorists, DHS is proposing to amend the regulations to provide that all travelers, including U.S. citizens, may be required to be photographed upon entry and/or departure.

Agency: Department of Homeland Security(DHS) **Priority:** Other Significant
RIN Status: Previously published in the Unified Agenda **Agenda Stage of Rulemaking:** Proposed Rule Stage
Major: No **Unfunded Mandates:** Undetermined
EO 13771 Designation: Other
CFR Citation: 8 CFR 215.8 8 CFR 235.1
Legal Authority: 8 U.S.C. 1357(b) 8 U.S.C. 1185(b) 6 U.S.C. 211(c)
Legal Deadline: None
Timetable:

Action	Date	FR Cite
NPRM	07/00/2020	

Regulatory Flexibility Analysis Required: **Government Levels Affected:** Undetermined

Undetermined

Federalism: Undetermined

Included in the Regulatory Plan: No

RIN Data Printed in the FR: No

Agency Contact:
Michael Hardin
Director, Entry/Exit Policy and Planning
Department of Homeland Security
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW, Office of Field Operations, 5th Floor,
Washington, DC 20229
Phone:202 325-1053
Email: michael.hardin@cbp.dhs.gov

From: (b)(6); (b)(7)(C)
Sent: Tuesday, December 3, 2019 1:32 PM
(b)(6); (b)(7)(C)
Subject: RE: 2019 Federal Privacy Summit: Registration Confirmation

Thanks,(b)(6); Sharing this with the team as I think it would be helpful for all of us to learn a little bit more about AI.

(b)(6); (b)(7)(C)
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: (b)(6); (b)(7)(C)
Mobile: (b)(6); (b)(7)(C)
Main: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, December 3, 2019 1:19 PM
To: (b)(6); (b)(7)(C)
Subject: FW: 2019 Federal Privacy Summit: Registration Confirmation

It was (b)(6); (b)(7)(C); (b)(7)(E) who had an interesting chart on AI Ethics Framework. It included 1) Stewardship & Accountability, 2) Periodic review, 3) Human judgement & Accountability, 4) Transparency & Explainability (do we understand how the black box works) & Interpretability (verify accuracy); 5) What bias might exist in the project; 6) What legal obligations govern AI and the data; 7) How do I account for iterations (e.g. perfecting your golf game), auditability; 8) Documentation of your purpose, parameters, limitations, and design outcome, Testing your AI.

(b)(6); (b)(7)(C) also brought up her concerns about AI, and Hiring. She asked if anyone new of any government agencies that were using AI for hiring. The following article is relevant to her concerns raised about using AI to determine an applicant's employability, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/. P. 9 of the attached comparative review of AI, dated January 2019 from the Library of Congress shows a map of countries that have a AI strategy in place (e.g. Canada, Mexico, Russia, China, France, Great Britain). The U.S. is listed as not having a national AI Strategy.

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (b)(6); (b)(7)(C)
Main:

Building an Artificial Intelligence Ethics Framework for Your Agency

(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C) **On Behalf Of** Privacy Council
Sent: Thursday, November 21, 2019 10:19 AM
Subject: 2019 Federal Privacy Summit: Registration Confirmation

Good morning,

This email is to **confirm your registration** for the 2019 Federal Privacy Summit on **Monday, December 2** at the Natcher Conference Center (NIH Campus, 45 Center Dr, Bethesda, MD 20894).

- If you were on the waitlist, this means you have been moved off and officially registered. Due to system limitations, MAX will not show this information.
- If you no longer plan to attend the Summit, please visit OMB MAX to unregister yourself or email (b)(6); (b)(7)(C) in consideration for those on the waitlist.

Attached is the program which includes the agenda and session descriptions. Please also refer to the program for detailed directions about transportation, security, lunch, and a post-summit happy hour.

- Registration will open at 8:00 am and the first breakout sessions will begin at 9:00 am.
- All visitors must enter through the NIH Gateway Center and clear security. Visitors are required to show one form of government-issued identification.
- Take the Metro Redline to Medical Center Station. Or, limited parking is available at Gateway Parking Garage (MP-11) at the cost of $2/hour or $12/day.
- The deadline to pre-order and purchase a boxed lunch is COB Tuesday, November 26. Ordering instructions can be found on page 2 of the attached program. Attendees also have the option of bringing their own lunch.

For questions, please email privacy.council@gsa.gov.

--

Information Governance and Privacy (IGP) Acquisition Review

Project Name: Lehigh County Gang Intelligence System - HSI

Contract Number: (b)(6); (b)(7)(C)

IGP Reviewer: (b)(6); (b)(7)(C)

Date: 01/27/2019

POTS Ref: (b)(6); (b)(7)(C)

(b)(7)(E)

Please contact the IGP Privacy Division ((b)(6); (b)(7)(C)) or (b)(6); (b)(7)(C) Acting Chief of Staff for OAQ (b)(6); (b)(7)(C) with any questions.

Page 41

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 42

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 43

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

From: (b)(6); (b)(7)(C)
Sent: 15 Jan 2020 15:27:23 +0000
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

(b)(7)(E)

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Wednesday, Jan 15, 2020, 8:59 AM
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Good morning (b)(6); (b)(7)(C)

Are you looking to re-establish a connection to CCD for its facial recognition capabilities, or are you looking to use IDENT's facial recognition algorithm? I can reach out to CBP, but as I

(b)(7)(E)

(b)(7)(E)

(b)(7)(E). It'll take a few weeks and I don't know if DHS Privacy will approve it, but it's worth a shot. Let me know if that's good by you and I'll start movement today.

Best,
(b)(6); (b)(7)(C)
____
Mobile: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Monday, January 13, 2020 5:04 PM
To: (b)(6); (b)(7)(C)
Subject: HSI facial recognition issues.

Hello,

I have been trying to coordinate with OBIM on how HSI agents can get basic facial recognition capabilities back after loosing them. (b)(6); told me to reach out to you. I sent her a basic summary of how HSI agents used to use facial recognition and how we no longer have the ability to do so and the obvious operational effect that it is having. Sadly the investigative arm of DHS has been reduced to "do you know someone at CBP that can run an image?"

(b)(7)(E)

Too be clear we are not looking to create some knew system for collection. We are just looking for a way that HSI can take an image gained during the course of a criminal investigation and see if there is a match in our very own DHS systems. It would be no different than if I lifted a fingerprint during the course of our investigation, and ran it in IDENT.

If there is already someone working on this issue please let them know that I have elevated it. It is ridiculous that a CBP Officer out of the academy has more facial recognition capability that I do and we are operating under the same exact laws (title 8, title 19 etc.). Even more disappointing is when a victim provides me a high def 4K image of a suspects face and I have to tell them that Homeland Security Investigations can't run facial recognition. They usually then point out sarcastically that they provide their own fingerprints and photo to Homeland Security every time they so much as take a cruise.

I'm sure there is an easy answer as we obviously have systems in place that already run off biometric query.

Thanks and let me know if there is anyone else that I should contact to get this capability reinstated.

Special Agent (b)(6); (b)(7)(C)
Homeland Security Investigations | Miami International Airport
11226 NW 20th street
Miami, FL 33172
Desk: (b)(6); (b)(7)(C)
Cell:
Email (b)(6); (b)(7)(C)
HSDN
C-LAN

From: (b)(6); (b)(7)(C)
Sent: 5 Dec 2019 18:11:19 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: DHS proposes expanding facial-recognition scans to US citizens
Attachments: DHS Data Privacy and Integrity Report_2019-03-11.docx, 15 EPIC-SJC-CBPOversight-Dec2018.pdf, DHS Privacy IFR Discussion.pptx

Hi (b)(6); (b)(7)(C)

While we're on the topic of facial recognition, I thought I'd share some resources I collected from the Deloitte team at CBP. They seem to work primarily on biometrics, but there's a lot of overlap between biometrics and facial recognition. You may already be familiar with these resources, but please share with the team if you feel they are relevant from the discussions at the Privacy Summit.

Thanks,
(b)(6);

From (b)(6); (b)(7)(C)
Sent: Wednesday, December 4, 2019 4:09 PM
(b)(6); (b)(7)(C)
Subject: DHS proposes expanding facial-recognition scans to US citizens

I don't know if this came up in the facial recognition session at the Federal Privacy Summit, but this was in the news yesterday in case anyone hasn't seen it yet,

https://techcrunch.com/2019/12/02/homeland-security-face-recognition-airport-citizens/2019/12/02/homeland-security-face-recognition-airport-citizens/

https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=1651-AB22&=biometric-collection-data-citizens

RIN Data

DHS/USCBP **RIN:** 1651-AB22 **Publication ID:** Fall 2019
Title: Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States
Abstract:

The Department of Homeland Security (DHS) is required by statute to develop and implement a biometric entry-exit data system. To facilitate the implementation of a seamless biometric entry-exit system that uses facial recognition and to help prevent persons attempting to fraudulently use U.S. travel documents and identify criminals and known or suspected terrorists, DHS is proposing to amend the regulations to provide that all travelers, including U.S. citizens, may be required to be photographed upon entry and/or departure.

Agency: Department of Homeland Security(DHS)
RIN Status: Previously published in the Unified Agenda
Major: No

Priority: Other Significant
Agenda Stage of Rulemaking: Proposed Rule Stage
Unfunded Mandates: Undetermined

EO 13771 Designation: Other

CFR Citation: 8 CFR 215.8 8 CFR 235.1

Legal Authority: 8 U.S.C. 1357(b) 8 U.S.C. 1185(b) 6 U.S.C. 211(c)

Legal Deadline: None

Timetable:

Action	Date	FR Cite
NPRM	07/00/2020	

Regulatory Flexibility Analysis Required: Undetermined

Government Levels Affected: Undetermined

Federalism: Undetermined

Included in the Regulatory Plan: No

RIN Data Printed in the FR: No

Agency Contact:
(b)(6); (b)(7)(C)
Director, Entry/Exit Policy and Planning
Department of Homeland Security
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW, Office of Field Operations, 5th Floor,
Washington, DC 20229
Phone:202 325-1053
Email: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, December 3, 2019 1:32 PM
To: (b)(6); (b)(7)(C) @ice.dhs.gov>
(b)(6); (b)(7)(C)
Subject: RE: 2019 Federal Privacy Summit: Registration Confirmation

Thank (b)(6); (b)(7)(C) Sharing this with the team as I think it would be helpful for all of us to learn a little bit more about AI.

(b)(6); (b)(7)(C)
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: (b)(6); (b)(7)(C)
Mobi
Main:

From:(b)(6); (b)(7)(C)
Sent: Tuesday, December 3, 2019 1:19 PM
To(b)(6); (b)(7)(C)
Subject: FW: 2019 Federal Privacy Summit: Registration Confirmation

It wa(b)(6); (b)(7)(C) (b)(6 who had an interesting chart on AI Ethics Framework. It included 1) Stewardship & Accountability, 2) Periodic review, 3) Human judgement & Accountability, 4) Transparency & Explainability (do we understand how the black box works) & Interpretability (verify accuracy); 5) What bias might exist in the project; 6) What legal obligations govern AI and the data; 7) How do I account for iterations (e.g. perfecting your golf game), auditability; 8) Documentation of your purpose, parameters, limitations, and design outcome, Testing your AI.

Ms.(b)(6); (b)(7)(C) also brought up her concerns about AI, and Hiring. She asked if anyone new of any government agencies that were using AI for hiring. The following article is relevant to her concerns raised about using AI to determine an applicant's employability, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/. P. 9 of the attached comparative review of AI, dated January 2019 from the Library of Congress shows a map of countries that have a AI strategy in place (e.g. Canada, Mexico, Russia, China, France, Great Britain). The U.S. is listed as not having a national AI Strategy.

(b)(6); (b)(7)(C)
Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct(b)(6); (b)(7)(C)
Main:

Building an Artificial Intelligence Ethics Framework for Your Agency
Moderator and Background Presenter:(b)(6); (b)(7)(C)
Panelists:(b)(6); (b)(7)(C)

From:(b)(6); (b)(7)(C)> **On Behalf Of** Privacy Council
Sent: Thursday, November 21, 2019 10:19 AM
Subject: 2019 Federal Privacy Summit: Registration Confirmation

Good morning,

This email is to **confirm your registration** for the 2019 Federal Privacy Summit on **Monday, December 2** at the Natcher Conference Center (NIH Campus, 45 Center Dr, Bethesda, MD 20894).

- If you were on the waitlist, this means you have been moved off and officially registered. Due to system limitations, MAX will not show this information.
- If you no longer plan to attend the Summit, please visit OMB MAX to unregister yourself or emai(b)(6); (b)(7)(C)n consideration for those on the waitlist.

Attached is the program which includes the agenda and session descriptions. Please also refer to the program for detailed directions about transportation, security, lunch, and a post-summit happy hour.

- Registration will open at 8:00 am and the first breakout sessions will begin at 9:00 am.
- All visitors must enter through the NIH Gateway Center and clear security. Visitors are required to show one form of government-issued identification.
- Take the Metro Redline to Medical Center Station. Or, limited parking is available at Gateway Parking Garage (MP-11) at the cost of $2/hour or $12/day.
- The deadline to pre-order and purchase a boxed lunch is COB Tuesday, November 26. Ordering instructions can be found on page 2 of the attached program. Attendees also have the option of bringing their own lunch.

For questions, please emai (b)(6); (b)(7)(C)

--

Federal Privacy Council
FPC.gov

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

December 11, 2018

Senator Chuck Grassley, Chairman
Senator Dianne Feinstein, Ranking Member
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Grassley and Ranking Member Feinstein:

The Electronic Privacy Information Center (EPIC) writes to you with regard to your hearing, "Oversight of U.S. Customs and Border Protection."[1] EPIC has long sought transparency and accountability from CBP and welcomes the committee's attention to this critical issue. Founded in 1994, EPIC is focused on the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[2] EPIC has consistently urged this Committee to ensure that law enforcement programs protect U.S. citizens' privacy.[3] And last week, EPIC submitted comments to DHS' Data Privacy and Integrity Advisory Committee urging CBP to halt implementation of the biometric border program.[4]

Without legal authority or the opportunity for public comment, CBP has deployed facial recognition technology in U.S. airports, sea ports, and land ports of entry and collected biometric identifiers from American travelers.[5] Further, the agency intends to "deploy biometric capabilities across all modes of travel — air, sea, and land — by fiscal year 2025."[6]

This vast biometric collection program exposes Americans and other travelers to substantial privacy risks. The problem begins when the State Department, without legal authority, transfers facial images collected for passport applications to the CBP. This largely immutable biometric information is then used to conduct government surveillance unrelated to the purpose for which the photos were collected. The legislation this program purports to implement does not authorize this

[1] U.S. Senate Comm. on the Judiciary, *Oversight of U.S. Customs and Border Protection* (Dec. 11, 2018), https://www.judiciary.senate.gov/meetings/oversight-of-us-customs-and-border-protection.

[2] EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/.

[3] *See e.g.* Statement of EPIC, *The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties*, Hearing before the Senate Committee on the Judiciary, U.S. Senate, June 23, 2017, https://www.judiciary.senate.gov/meetings/oversight-of-us-customs-and-border-protection; *see also* EPIC, EPIC v. CBP (Biometric Entry/Exit Program), https://www.epic.org/foia/dhs/cbp/biometric-entry-exit/.

[4] Comments of EPIC, *DHS Data Privacy and Integrity Advisory Committee; Committee Management; Notice of Federal Advisory Committee Meeting*, Docket No. DHS–2018–0066 (Dec. 6, 2018), https://epic.org/apa/comments/EPIC-Comments-DHS-DPIAC-Face-Rec-Report-Dec-2018.pdf.

[5] U.S. Customs and Border Protection, Biometrics, https://www.cbp.gov/travel/biometrics (last visited Dec. 7, 2018).

[6] Office of Inspector General, *Progress Made but CPB Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide* 2 (2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.

activity,[7] and there is currently no federal legislation to regulate the use of facial recognition or other biometric surveillance techniques in these circumstances.

Contrary to the agency's original representations, there is no practical way to opt-out of the CBP facial recognition program. EPIC knows for a fact that the original procedures described at the CBP website regarding alternative screening, "manual processing," is in fact not the agency's practice.[8] Remarkably, the agency has repeatedly modified the FAQ for alternative procedures for U.S. citizens who do not wish to have a photo taken and no longer provides for a simple check of travel documents as an alternative. Today, the FAQ reads:

> **Are U.S. Citizens required to provide biometrics for the entry-exit system?**
>
> U.S. Citizens who are entering or exiting the country are generally required to be in possession of a valid U.S. passport. At this time, however, CBP does not require U.S. Citizens to have their photos captured when entering or exiting the country. U.S. Citizens who do not wish to participate in this biometric collection should notify a CBP Officer or an airline or airport representative in order to seek an alternative means of verifying their identity and documents. CBP discards all photos of U.S. Citizens, once their identities have been verified.[9]

But on March 6, 2018, the same FAQ stated:

> Individuals seeking to travel internationally are subject to the laws and rules enforced by CBP and are subject to inspection. If a U.S. citizen, however, requests not to participate in the Traveler Verification System, specified agreements between CBP and the partner airline or airport authority will guide alternate procedures. For some participating airlines, a traveler may request not to participate in the TVS and, instead, present credentials to airline personnel before proceeding through the departure gate. In other cases of an opt-out, an available CBP Officer may use manual processing to verify the individual's identity.[10]

And on August 24, 2018 it read:

> Individuals seeking to travel internationally are subject to the laws and rules enforced by CBP and are subject to inspection. However, if a U.S. Citizen does not wish to participate in the biometric entry or exit process, he or she must

[7] Letter from Sens. Edward J. Markey and Mike Lee to Sec'y Kirstjen Nielsen, Dep't of Homeland Sec., 1-2 (Dec. 21, 2017), *available at* https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20.pdf.

[8] U.S. Customs and Border Protection, *Biometric Exit Frequently Asked Questions (FAQs)* (Sept. 7, 2018), https://web.archive.org/web/20180907171042/https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

[9] U.S. Customs and Border Protection, *Biometric Exit Frequently Asked Questions (FAQs)* (Dec. 3, 2018), https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

[10] U.S. Customs and Border Protection, *Biometric Exit Frequently Asked Questions (FAQs)* (Mar. 6, 2018), https://web.archive.org/web/20180306164048/https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

> request to be processed using alternate procedures, such as presenting travel credentials to an available CBP Officer or authorized airline personnel.[11]

Without legal authority or the opportunity for public comment, CBP is making up the rules as it rolls out the program.

And the underlying problem remains: personal data is automatically transferred from the State department to another agency without legal authority. By the time the passenger attempts to assert the right to "opt out," the passenger's photo has already been pulled from the State Department database into a gallery to be used by DHS for facial recognition.

Transparency about the entry/exit program is essential, particularly because the accuracy is questionable. In December 2017, a Freedom of Information Act lawsuit pursued by EPIC produced the public release of a CBP report on iris imaging and facial recognition scans for border control. The "Southwest Border Pedestrian Field Test" revealed that the CBP does not perform operational matching at a "satisfactory" level.[12] In a related FOIA lawsuit, EPIC obtained documents from the FBI concerning the Next Generation Identification database which contains facial scans, fingerprints, and other biometrics of millions of Americans.[13] The documents obtained by EPIC revealed that biometric identification is often inaccurate.[14] DHS itself acknowledges that facial recognition is inaccurate as implemented.[15] Inaccurate biometric matches affect all travelers, and particularly U.S. citizens. According to the Inspector General's report, "U.S. citizens accounted for the lowest biometric confirmation rate."[16]

The involvement of private companies raises additional concerns. CBP has enlisted airlines such as JetBlue and Delta to implement face recognition technology in U.S. airports.[17] Just last week, Delta opened the first "fully biometric terminal" in Atlanta.[18] It is unclear whether use by private firms of biometric identifiers obtained from the State Dept. for passport applications will lead to other uses unrelated to traveler identification

Today airlines are promoting facial recognition as a convenience, but it's clearly part of a larger effort by the government to expand biometric surveillance program of Americans. Just last

[11] U.S. Customs and Border Protection, *Biometric Exit Frequently Asked Questions (FAQs)* (Aug. 24, 2018), https://web.archive.org/web/20180824202202/https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

[12] U.S. Customs and Border Protection, *Southern Border Pedestrian Field Test Summary Report,* https://epic.org/foia/dhs/cbp/biometric-entry-exit/Southern-Border-Pedestrian-Field-Test-Report.pdf (December 2016).

[13] *EPIC v. FBI – Next Generation Identification*, EPIC, https://epic.org/foia/fbi/ngi/.

[14] DEPT. OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, NEXT GENERATION IDENTIFICATION (NGI) SYSTEM REQUIREMENTS DOCUMENT VERSION 4.4 at 244 (Oct. 1, 2010), https://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf.

[15] *Id.*

[16] *Id.*

[17] Asma Khalid, *Facial Recognition May Boost Airport Security But Raises Privacy Worries*, NPR, June 26, 2017, https://www.npr.org/sections/alltechconsidered/2017/06/26/534131967/facial-recognition-may-boost-airport-security-but-raises-privacy-worries.

[18] Thom Patterson, *US airport opens first fully biometric terminal*, CNN, Dec. 3, 2018, http://www.cnn.com/travel/article/atlanta-airport-first-us-biometric-terminal-facial-recognition/.

month we learned that the Secret Service is exploring the use of facial recognition at the White House.[19]

The committee should insist that CBP remove all facial-recognition technology from public use until proper regulatory safeguards to protect against the misuse of facial recognition and other biometric surveillance techniques are in place.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg* Marc Rotenberg EPIC President	/s/ *Caitriona Fitzgerald* Caitriona Fitzgerald EPIC Policy Director
/s/ *Jeramie D. Scott* Jeramie D. Scott EPIC National Security Counsel	/s/ *Jeff Gary* Jeff Gary EPIC Legislative Fellow

[19] DHS/USSS/PIA-024, Privacy Impact Assessment for the Facial Recognition Pilot (Nov. 26, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf.

Thanks for the information and helping us out. Agents have gotten to the point where it seems everyone can use facial recognition except HSI. We definitely collect a lot of facial images for DHS but seem unable to get image information from DHS.

The basic scenario that HSI agents keep encountering nationwide is simple. In cases of identity issues, the only information we have is often photographic or visual. Names provided and even documents

(b)(7)(E)

To be clear, HSI is in no way attempting to create some new program that will collect images and run them to see if there are "hits." I have been part of collection programs that needed privacy compliance reviews (Operation Southern Shield was my last) and this is in no way a request to create such a system. HSI agents aren't driving around looking for administrative fugitives, HSI agents work specific criminal cases and very often have encountered unknown individuals during the course of the investigation.

HSI is simply looking for a way to take an image and see if there is a match in the Department of Homeland Security's systems. This is no different if I lifted the subjects finger prints off a cup they threw in the trash and ran it to see if the finger prints were in one of the DHS systems.

In the past HSI agents would often use the ATS system to access the CCD facial recognition program. It was not the best system in the world and it was clearly an early attempt to get this capability in the hands of HSI agent and CBP officers. I used it successfully myself to identify an individual who was attempting to procure export controlled technology. ATS has been taken off line by CBP and replaced with UPAX. If an agent has access to UPAX (most are not allowed) the HSI version does not have any facial recognition component. I can review all the DHS images for a subject that I do have a name and date of birth, but if all I have is a image off a fake document used to open a bank account, I will not have any options. The current CCD system that HSI has access does allow me to run an image and will present a user with results (including US visit images) but when one tries to view the identity of a possible match, the system will tell the HSI user that they are not authorized to view the information.

It should be noted that HSI does constantly bombard CBP with requests to have CBP do the very same thing in their systems to obtain a possible identity. CBP Officers at the most basic level have access to all

(b)(7)(E)

responsible for even more areas of enforcement. These requests are almost universally done through personal relationships, and depending on the HSI agent, the requests may not be done at all. Obviously this will lead to the subjects to continue on there criminal enterprise until they can be identified some other way. At the best, illegal money will continue to be made. At the worst, someone is physically harmed. The time it takes is often the difference between taking someone off the street just in time, versus “too little, too late.”

HSI agent safety is also assisted when someone goes from being an unknown subject, to a subject who may be committing document fraud but has had multiple arrests for resisting arrest and fire arms possession.

It is difficult to tell someone who gives you a photo from a camera at their home or business with a 4k high def image of a subjects face that Homeland Security does not have facial recognition capabilities. Especially when that person has gone through the airport and had their fingerprints and photograph taken every time.

Let me know if there is anything else specific that you may need from me. I have worked both at the NTC and LESIM for HSI in the past so I am familiar with some of the ways things can get a little stuck and how easy it is for some entities to just say “no” versus do a little work to find a way to say “yes.”

Special Agent (b)(6); (b)(7)(C)
Homeland Security Investigations | Miami International Airport
11226 NW 20th street
Miami, FL 33172
Desk (b)(6); (b)(7)(C)
Cell:
Email: (b)(6); (b)(7)(C)
HSDN
C-LAN

From: (b)(6); (b)(7)(C)
Sent: 13 Mar 2020 14:58:58 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: HSI facial recognition issues.

That is a perfect summary. I would emphasize we already testify routinely to the use other biometric collection methods.

Thanks let me know if you have any other questions.

Special Agent (b)(6); (b)(7)(C)
11226 NW 20th street
Miami, FL 33172
Cell: (b)(6); (b)(7)(C)
Email: [redacted]
HSDN
C-LA

Sent with BlackBerry Work
(www.blackberry.com)

From (b)(6); (b)(7)(C)
Date: Friday, Mar 13, 2020, 9:38 AM
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Hi (b)(6);
Sorry for the multiple emails. We at privacy hate parallel construction, because it eliminates an opportunity for transparency in our information collections. Let me know if this paragraph is accurate and represents your workflow:

(b)(5)

We can get OPLA to opine on the legal parameters of all this, but for a "boots on the ground" perspective, let me know if I am missing anything

Best,
(b)(6); (b)(7)(C)

____

Mobile: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thursday, March 12, 2020 5:05 PM
To (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

This looks great,

(b)(5)

(b)(5)

Special Agent (b)(6); (b)(7)(C)
Homeland Security Investigations | Miami International Airport
11226 NW 20th street
Miami, FL 33172
Desk (b)(6); (b)(7)(C)
Cell:
Email: (b)(6); (b)(7)(C)
HSDN:
C-LAN:

From: (b)(6); (b)(7)(C)
Sent: Thursday, March 12, 2020 12:06 PM
To: (b)(6); (b)(7)(C)
Subject: FW: HSI facial recognition issues.

Find enclosed. We are trying to be as privacy sensitive as possible in the process, but if it doesn't work in an HSI agent's workflow we want to change it. Thanks for the help!

Best,
(b)(6); (b)(7)(C)

Mobile: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thursday, March 12, 2020 12:03 PM

To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

I did not. Shoot it my way and I'm sure I will have some questions based on current situational constraints that we are experiencing in the field.

Thanks for checking,

Special Agent (b)(6); (b)(7)(C)
11226 NW 20th street
Miami, FL 33172
Cell: (b)(6); (b)(7)(C)
Email: (b)(6); (b)(7)(C)
HSDN:
C-LAN

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Thursday, Mar 12, 2020, 11:55 AM
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Good morning (b)(6); ,
Recently I sent a PIA on facial recognition for HSI comments through the same channels I sent the IDENT FR PTA. I got only a few comments from a few people on both documents. Since you are an obvious stakeholder in this I wanted to check and see if you or your people received either document when it was tasked out.

Best,
(b)(6); (b)(7)(C)

Mobile: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Tuesday, March 3, 2020 8:46 AM
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Thanks for the update. Let me know who you send it to and I'll stay on them to get you a decision. I know sometimes they prioritize things without thought to the actual agents in the field.

Special Agent (b)(6); (b)(7)(C)
11226 NW 20th street
Miami, FL 33172

Cell(b)(6); (b)(7)(C)
Email:(b)(6); (b)(7)(C)
HSDN
C-LAN

Sent with BlackBerry Work
(www.blackberry.com)

From:(b)(6); (b)(7)(C)
Date: Tuesday, Mar 03, 2020, 7:01 AM
To:(b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Thanks for checking in (b)(6); (b)(7)(C We've just received comments/edits from HSI on the IDENT Facial Recognition PTA. It's sitting with the ICE Privacy Officer right now. He will review it and determine if it needs further work, needs to go to OPLA, or if it can go to DHS Privacy. If he thinks its ready to go to DHS Privacy it'll be at least another two weeks before we hear anything back from them. They've been sitting on a lot of our facial recognition PTAs recently, so I'd expect it to take longer.

Best,
(b)(6);

Mobile:(b)(6); (b)(7)(C)

From:(b)(6); (b)(7)(C)
Sent: Monday, March 2, 2020 5:13 PM
To:(b)(6); (b)(7)(C)>
Subject: RE: HSI facial recognition issues.

Hey buddy,

Just checking in to see where we stand with this. We came across a couple more issues where this would have been a valuable tool.

Thanks,

Special Agent(b)(6); (b)(7)(C)
Homeland Security Investigations | Miami International Airport
11226 NW 20th street
Miami, FL 33172
Desk(b)(6); (b)(7)(C)
Cell:
Email:(b)(6); (b)(7)(C)
HSDN:
C-LAN

From: (b)(6); (b)(7)(C)
Sent: Tuesday, January 28, 2020 12:32 PM
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Good afternoon (b)(6);

I followed up again with CBP on HSI access to the facial recognition capabilities in ATS. They say they are keeping access limited to select officers in CBP at this time. I heard we might have a call with OBIM this week. Hopefully we can figure out a way forward with them.

Best,
(b)(6); (b)(7)(C)

Mobile: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Friday, January 17, 2020 12:55 PM
To (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

This is great news. Thanks for staying on this. You were right privacy seemed more concern about facial collections as opposed to our ability to query our own images. I think they are more interested in reviewing what answer we come up with. I have a few outstanding emails with ICE LESIM people to see what has been tried (if anything) and why things failed.

Obviously I'll let you know if I hear anything.

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Friday, Jan 17, 2020, 12:17 PM
To: (b)(6); (b)(7)(C)
Subject: RE: HSI facial recognition issues.

Hi (b)(6); (b)(7)(C

I wanted to give you a quick update. I reached out to OBIM and CBP to see what was going on.
(b)(7)(E)
do before we can start submitting probe photos to IDENT directly. It might take a little time, but I'll keep on it.

Best,

From: (b)(6); (b)(7)(C)
Sent: 4 Jun 2019 17:08:20 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: *<3 HR TURNAROUND - CONFIRM RECEIPT*FW: Review and Comment -P-107492- R&C - Statement for the Record CBP - Facial Recognition Technology - WF # 1181451 ICATT:0045405
Attachments: SFTR CBP - Biometric Entry-Exit Facial Imaging.docx, DHS review - Statement for the Record CBP - Facial Recognition Technology - WF # 1181451 (Service 1181451) (Intranet Quorum IMA007081647)
Importance: High

Good Afternoon,

Tasking CL-Tsk-P-107492 has been received by IGP. Please find a brief of the tasking below. **Please note: this tasker is due today at 3:30 PM, please confirm receipt.**

Folder:	CL-Tsk-P-107492
Received Date:	6/4/2019
Due Date:	**Tuesday 6/4/2019 3:30 PM**
Clearance Level:	Standard
IGP Assignees:	Privacy
Tasking Description:	R&C - Statement for the Record CBP - Facial Recognition Technology - WF # 1181451
Tasking Request:	Review the attached document and provide edits/comments via track changes.
Previous Assignees:	N/A
Current ICE Assignees:	HSI, ERO, Policy, IGP, OCR, OPLA
Additional Information:	Please see attached.
Access Files:	CL-Tsk-P-107492 Assigned To IGP

Thank you,

(b)(6); (b)(7)(C)
Analyst
Office of Information Governance & Privacy
U.S. Immigration & Customs Enforcement
(b)(6); (b)(7)(C)

From: ICATT.Alert
Sent: Tuesday, June 4, 2019 1:03 PM

To: (b)(6); (b)(7)(C)
Subject: Review and Comment -P-107492- R&C - Statement for the Record CBP - Facial Recognition Technology - WF # 1181451 ICATT:0045405

Hello IGP,

A Clearance has been assigned to you. Please accept in 1 day

Clearance Name: CL-Tsk-P-107492 Assigned To IGP

Due Date: 06/04/2019 04:00 PM Eastern

Instructions:

Instructions:
Review the attached document and provide edits/comments via track changes.

Due Dates:
Non Lead:
HSI Taskings: NLT 4PM - 6/4/2019

ERO Taskings: NLT 4PM - 6/4/2019

Policy Tasking: NLT 4PM - 6/4/2019

IGP Tasking: NLT 4PM - 6/4/2019

Reviewer:
OCR Taskings: NLT 9AM - 6/5/2019

OPLA Taskings: NLT 11AM - 6/5/2019

OES is not responsible for coordinating or consolidating Program Office responses.

The lead program office must reconcile all ICE intra-agency comments and/or questions prior to closing their task bar.

Thank you,

(b)(6); (b)(7)(C)
Taskings Analyst
Office of the Executive Secretariat
Office of the Director
U.S. Immigration and Customs Enforcement
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Thank you.

From: (b)(6); (b)(7)(C)
Sent: 28 Jun 2019 13:21:19 +0000
To: (b)(6); (b)(7)(C)
Cc:
Subject: **DUE 12PM TODAY – CONFIRM RECEIPT**FW: Review and Comment -P-107964- R&C - CBP Authorization Testimony - Biometrics at DHS - Service 1182059 ICATT:0045879
Attachments: CBP Authorization Testimony # 1182059 - Biometrics at DHS - JULY10 (Service 1182059) (Intranet Quorum IMA007117646), DRAFT 071019 Biometrics written testimony.docx
Importance: High

Good Morning,

Tasking CL-Tsk-P-107964 has been received by IGP. Please find a brief of the tasking below. Please note – QUICK TURNAROUND TASKER – DUE 12PM TODAY – CONFIRM RECEIPT!

Folder:	CL-Tsk-P-107964
Received Date:	6/28/2019
Due Date:	**Friday 6/28/2019 12:00 PM**
Clearance Level:	Standard
IGP Assignees:	Privacy
Tasking Description:	R&C - CBP Authorization Testimony - Biometrics at DHS - Service 1182059
Tasking Request:	Review the attached document and provide edits/comments via track changes.
Previous Assignees:	N/A
Current ICE Assignees:	HSI, ERO, Policy, IGP, OCR, OPLA
Additional Information:	QUICK TURNAROUND TASKER – DUE 12PM TODAY – CONFIRM RECEIPT
Access Files:	CL-Tsk-P-107964 Assigned To IGP

Thank you,

(b)(6); (b)(7)(C)
Analyst
Office of Information Governance & Privacy
U.S. Immigration & Customs Enforcement
(b)(6); (b)(7)(C)

From: ICATT.Alert
Sent: Friday, June 28, 2019 9:17 AM
To: (b)(6); (b)(7)(C) >

Subject: Review and Comment -P-107964- R&C - CBP Authorization Testimony - Biometrics at DHS - Service 1182059 ICATT:0045879

Hello IGP,

A Clearance has been assigned to you. Please accept in 1 day

Clearance Name: CL-Tsk-P-107964 Assigned To IGP

Due Date: 06/28/2019 12:30 PM Eastern

Instructions:

Instruction:

Review the attached document and provide edits/comments via track changes.

Due Dates:

Non Lead

HSI Taskings : NLT 12:30PM - 6/28/2019

ERO Taskings: NLT 12:30PM - 6/28/2019

Policy Tasking: NLT 12:30PM - 6/28/2019

Privacy Taskings: NLT 12:30PM - 6/28/2019

Reviewer

OCR Taskings : NLT 2PM - 6/28/2019

OPLA Taskings : NLT 4:30PM - 6/28/2019

Please note:

- Any Law Enforcement Sensitive information provided must be labeled correctly.
- Program offices are required to review and edit all responses prior to submission.
- Immediately contact ICE Taskings if you believe a program with equities has been inadvertently overlooked.

Failure to complete any of the above requirements will result in a re-task.

Thank you.

Best,

(b)(6); (b)(7)(C)
Taskings Analyst
Office of the Executive Secretariat
Office of the Director
U.S. Immigration and Customs Enforcement
(b)(6); (b)(7)(C)

Thank you.

From: (b)(6); (b)(7)(C)
Sent: 28 Jun 2019 08:36:43 -0400
To: (b)(6); (b)(7)(C)
Subject: CBP Authorization Testimony # 1182059 - Biometrics at DHS - JULY10 (Service 1182059) (Intranet Quorum IMA007117646)

Good morning:

Please review Attachment #1 and upload any comments / edits into IQ NLT Monday, July 1st at 10:00AM.

This is a hard deadline considering the upcoming holiday.

Thank you,
(b)(6); (b)(7)(C)