

**U.S. Immigration and Customs Enforcement
Response to U.S. Senator Wyden
DATE**

1. For what type of enforcement activities does ICE utilize face recognition capabilities via CBP, Department of State, or other partner systems?

a. Please specify whether ICE utilizes this system for criminal or immigration enforcement, and what, if any, specific criminal investigations the system is utilized for.

(b)(5); (b)(7)(E)

Commented (b)(5)

(b)(5)

2. Please describe how ICE obtains or requests facial recognition capabilities through ATS-P and CCD.

a. For example, who provides probe photos, what agencies conducts any matching, and what agencies receive the results of any matching?

(b)(5); (b)(7)(E)

Commented (b)(5)

3. How many facial recognition searches has ICE requested via ATS-P and CCD since January 1, 2017?

ICE HSI does not track these queries and since the systems belong to outside agencies, does not have the ability to review system queries.

4. Please describe how ICE confirms that matches or identifications by any facial recognition systems are correct before taking further action.

a. Please describe how, if any way, inaccurate results are maintained by any face recognition systems.

ICE HSI treats matches similar to any other lead or evidence collected during an investigation and does not rely solely on a facial recognition match to establish probable cause of a violation. Specific questions about how the system operates would need to be directed to the system owner.

5. What evidentiary standard, if any, must be met for ICE to utilize facial recognition capabilities through ATS-P and CCD?
- a. What, if any, limits are placed on which probe photos can be submitted for face recognition matching?

(b)(5)

(b)(5)

6. Does ICE share its photo databases with any other federal, state, or local agencies, including departments of motor vehicles, for facial recognition matching use?
- a. Does ICE ever submit photos to the facial recognition systems of other federal, state, or local agencies, including departments of motor vehicles, so that those agencies can run facial recognition searches of their systems using ICE-submitted photos?

ICE users are subjected to the third-party rule when sharing any results from systems not owned by the Department of Homeland Security (DHS), they would seek and receive permission from DOS prior to sharing information derived from DOS systems.

7. Please provide all policies and procedures related to ICE's use of facial recognition capabilities through ATS-P and CCS or any other mechanism.

(b)(5)

(b)(5)

Recent news reports also suggest that ICE has met with vendors regarding potentially acquiring additional facial recognition capabilities. Please provide the following information:

1. Does ICE have plans to acquire additional facial recognition capabilities, either on its own or through other agencies?

(b)(5)

(b)(5)

- a. Has ICE issued any RFPs for facial recognition technologies?

ICE HSI has not issued any requests for proposals for facial recognition technologies.

2. Does ICE have Memorandums Of Understanding (MOU) with any other agencies, including local law enforcement agencies, regarding obtaining facial recognition capabilities?

(b)(5)

(b)(5)

- a. If so, please provide those MOUs.

(b)(5)

3. Please provide a complete list of cases for which ICE has explored acquiring facial recognition technology.

ICE HSI initiated over 44,000 investigative cases in fiscal year (FY) 2018 and does not have visibility on any that would have explored utilizing facial recognition technology.

4. Please provide a list of vendors that ICE has met with since January 1, 2018 regarding acquiring or using facial recognition technology.

On April 25, 2018, ICE HSI met with Vigilant Solutions regarding license plate reader and facial recognition technology. There have not been any follow up meetings or communications since that time.

- a. Please include any relevant agendas, materials, or follow-up communications regarding these meetings.

See attached.

5. Has ICE obtained a legal opinion from the General Counsel's office regarding whether existing or potential future uses of facial recognition technology would be lawful?

ICE HSI has not obtained any legal opinions from the General Counsel's office regarding the existing or potential future use of facial recognition technology.

In your October 16th response, you also stated that under ICE's "Alternatives to Detention Intensive Supervision Appearance Program (III) (ATD-ISAPIII), a new form of contractors-owned technology has been introduced that uses facial recognition software known as SmartLINK."

1. When did BI, the provider of ISAPIII, begin deploying SmartLINK at ICE's request?

ICE ERO deployed SmartLINK on February 5, 2018.

(b)(5)

- a. What percent of and how many ISAPIII enrollees are using SmartLINK at any given time?

As of January 29, 2019, the total active ATD population is 94,687 participants. Of the total active population, 6,771 aliens, or 7.2 percent, are on the SmartLINK technology.

b. How do the enrollees access SmartLINK; are they required to use their personal devices or does ICE provide smartphones or computers to enrollees?

When participants qualify for a SmartLINK assignment, they use their personal smartphone or tablet to access the program by downloading a free application.

2. What information does ICE and BI collect on enrollees using SmartLINK?

SmartLINK enables ATD officers and case specialists to keep participants focused on the conditions of release via their smartphone or tablet. They are able to verify a participant's identity, determine their location¹, and quickly collect status change information.

a. How long is that information retained?

Information is retained by the contractor (BI) until the end of the awarded contract and then records are turned over to ICE to follow record retention policies as directed by DHS.

b. Who has access to that information and under what conditions?

ICE ATD officers and BI case specialists have access to the information on a need-to-know basis. The information is accessed only through required duties related to ATD – ISAP participation.

c. What limitations exist, if any, on the use of that information?

The information is accessed through required duties related to ATD – ISAP participation.

3. What, if any, information is provided to enrollees using SmartLINK regarding the confidentiality of their data and any limitations on the use of their data?

The participant must agree to terms of use and user license agreement as established by BI prior to use of the SmartLINK application and enrollment. If the participant does not agree to the participation requirements, SmartLINK is not assigned.

4. Please provide any additional documentation in ICE's possession on the deployment of the SmartLINK technology in the context of ISAPIII.

The SmartLINK overview and participant enrollment agreement and the SmartLINK deployment memorandum are attached.

¹ The SmartLINK application only locates the participant when they are accessing the SmartLINK application.

~~FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE~~