From: ERO Taskings
Sent: 25 Nov 2015 17:22:56 +0000
Subject: 16112029 | CLEAR Social Media Analytics – Social Media Access through CLEAR and Non-Network Computer Installation

The following message is being sent on behalf of Matthew T. Albence, Assistant Director for Enforcement, with the concurrence of Jon Gurule, Assistant Director for Field Operations:

To: Field Office Directors, Deputy Field Office Directors, and Assistant Field Office Directors

Subject: CLEAR Social Media Analytics – Social Media Access through CLEAR and Non-Network Computer Installation

CLEAR, a commercial system used to run queries and searches to assist in locating targeted aliens, has the ability to provide social media analytics by gathering data from blogs and social media websites (e.g. Facebook) and analyzing that data. However at present, CLEAR users are prevented from using this analytics feature because of ICE firewall settings which prohibit most agency computers from accessing social media websites.

Use of social media and the analytics provided through the CLEAR system must be in compliance with the ICE Online Rules of Behavior for Law Enforcement Activities, which governs ICE's collection and use of social media and other online information. This policy is posted on the Social Media page of the ICE Privacy and Records Office website.

To ensure employees have the ability to utilize CLEAR to its fullest potential as an investigative resource, Field Office Directors (FODs) must work with their local Help Desk to authorize access to social media through the CLEAR system. FODs should ensure that social media is accessible through CLEAR on at least one computer with internet access for each Fugitive Operations Team, and an additional (2) computers with internet access, within each office / sub-office.

Future efforts should be made to establish a minimum of one (1) non-networked computer with internet access per Fugitive Operations Team, and an additional (2) non-networked computers with internet access, within each office / sub-office. These non-networked terminals may be utilized for any ERO enforcement or investigative activities. The use of non-networked computers will allow for appropriate operational anonymity during these activities.

As with any ICE sensitive equipment, these computers are to be used for official use only for the purpose of:

- Enhancing situational awareness,
- Investigating an individual in a criminal, civil, or administrative context,
- Making a benefit determination about a person,
- For any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual.

Please contact (b)(6); at (b)(6); (b)(7)(C) or (b)(6); (b)(7)(C) with any CLEAR related questions.

NOTICE: This communication may contain privileged or otherwise confidential information. If you are not an intended recipient or believe you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use this information. Please inform the sender that you received this message in error and delete the message from your system.

Privacy Impact Assessment
for the

Data Analysis System (DAS)

DHS/ICE DAS/PIA-048

September 29, 2017

Contact Point
Patrick F. Gannon
National Criminal Analysis and Targeting Center
Office of Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement
(802) 657-4606

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Data Analysis System (DAS) is an analytical database owned, operated, and maintained by the U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO). The National Criminal Analysis and Targeting Center (NCATC), located within ERO's Targeting Operations Division, uses DAS to assist ERO field offices in locating aliens convicted of criminal offenses and other aliens who are amenable to removal. DAS was first deployed in 2006 and a discussion of the system was included in the Privacy Impact Assessment (PIA) for the Fugitive Case Management System (FMCS), which has been dispositioned.[1] ICE is publishing this PIA to describe the personally identifiable information (PII) within DAS and the way in which the NCATC uses the database. ICE will retire the FCMS PIA with the publication of this PIA.

Overview

ICE enforces the nation's civil immigration laws by apprehending and removing aliens who are amenable to removal. Individuals who are amenable to removal are those who are unlawfully present in the United States or those once lawfully present who have been convicted of crimes that render them removable. In support of the Agency's immigration enforcement mission, ICE's NCATC uses DAS, along with other technical and knowledge-based capabilities, to generate comprehensive, actionable, and timely leads, called "Information Referrals." ERO and others with immigration enforcement authorities pursuant to Section 287 of the Immigration and Nationality Act (INA)[2] (*e.g.*, certain state and local law enforcement officers) use these Information Referrals to assist in identifying and locating aliens who are amendable to removal.

DAS Data

DAS resides on an encrypted server behind ICE's firewall and compiles and stores dataset extracts from various DHS and non-DHS sources, thereby allowing for the efficient and effective analysis of data. These data sources include: ICE's Enforcement Integrated Database (EID), the U.S. Citizenship and Immigration Services (USCIS) Computer Linked Application Information Management System 3 (CLAIMS 3), the USCIS Central Index System (CIS), the Federal Bureau of Prisons (BOP) SENTRY System, the Federal Bureau of Investigation (FBI) Interstate Identification Index (III), and the California Department of Corrections and Rehabilitation (CDCR) Strategic Offender Management System (SOM), and publicly available data from two commercial sources.[3] ICE has entered into information access agreements and arrangements to

[1] *See* DHS/ICE/PIA-009 Fugitive Case Management System (FCMS), *available at* www.dhs.gov/privacy.
[2] Section 287 of the INA (8 U.S.C. § 1357) describes the authorization of immigration officers and employees.
[3] For reference, the Privacy Impact Assessments for these systems may be found at the locations below:
- *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at*

receive data from the non-DHS sources listed below in Question 2.2. The datasets contain a variety of categories of information including: biographical information, criminal history, immigration history, custody data (immigration and criminal), case history (immigration and criminal), immigration benefit information, naturalization information, and vehicle and insurance information. They are routinely obtained from each source via scheduled batch jobs, manual extracts, or responses to requests for information (in the case of open source data from a commercial vendor with which the NCATC has a contract), and each dataset uploaded into DAS. The previous dataset from each source is fully replaced with every update to ensure DAS contains the most current information available. Each dataset remains separate and distinct within DAS, and data elements are pulled together to populate Information Referrals in response to searches entered by DAS users.

The data within DAS is primarily about aliens; however, information about U.S. citizens may be included in some datasets. The presence of U.S. citizen information in DAS occurs when the source of the dataset does not maintain or is otherwise unable to provide NCATC with the citizenship status of the individuals within the dataset. For example, DAS contains a dataset from the BOP that contains biographic and criminal custody information about inmates in federal prisons who are foreign-born, but may or may not be United States citizens. This dataset does not include the inmate's citizenship status and, in some cases, foreign-born inmates may be U.S. citizens. NCATC employees attempt to verify the citizenship status of all individuals during their analysis by searching against data from other U.S. Department of Homeland Security (DHS) databases (*e.g.*, CIS) to which they have access. If individuals are confirmed to be U.S. citizens or their status cannot be confirmed, ERO does not pursue enforcement action against them.

DAS also contains the names and geographical areas of responsibility (AOR) of certain ERO officers who are the NCATC points of contact (POC) within the AORs. NCATC Management and Program Analysts (Analysts) who have full read and edit access to DAS input the names and AORs into a separate table in DAS. DAS pulls information from this table to ensure leads for specific AORs are provided to the correct points of contact.

---

www.dhs.gov/privacy.

- *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, *available at* www.dhs.gov/privacy.
- *See* DHS/USCIS/PIA-009(a) Central Index System (CIS), *available at* www.dhs.gov/privacy.
- *See* Bureau of Prisons SENTRY System PIA, *available at* http://www.bop.gov/foia/sentry.pdf.
- See Federal Bureau of Investigation Fingerprint Identification Records System (FIRS), Integrated Automated Fingerprint Identification System (IAFIS) which includes the Interstate Identification Index (III), *available at* https://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis.

The California Department of Corrections and Rehabilitation is a state entity and is therefore not subject to Section 208 of the E–Government Act of 2002 (P.L. 107-347) which requires federal agencies to complete Privacy Impact Assessments. Records maintained by the California Department of Corrections and Rehabilitation are available for inspection pursuant to procedures located here: http://www.cdcr.ca.gov/News/CPRA.html. Additional information about the Strategic Offender Management System may be found here: http://www.cdcr.ca.gov/SOMS/index.html.