Privacy Impact Assessment Update
for the

Immigration and Customs Enforcement – Child Exploitation Tracking System (ICE-CETS)

DHS/ICE/PIA-017(a)

August 28, 2013

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

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Child Exploitation Tracking System (ICE-CETS), owned and operated by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), is a centralized information repository that assists law enforcement in conducting child exploitation investigations. The ICE-CETS database aggregates tips and lead information about Internet-facilitated child sexual exploitation crimes in a single repository allowing investigators to identify links in otherwise unrelated matters to reduce redundant investigative work. The original Privacy Impact Assessment (PIA) for ICE-CETS was published on January 19, 2010.[1] With this update to the PIA, ICE is expanding the use of ICE-CETS within DHS to permit select U.S. Customs and Border Protection (CBP) personnel to access and directly query data within the system.

Introduction

The ICE-CETS database contains investigative information related to Internet-facilitated child sexual exploitation crimes, including the possession, distribution, and manufacturing of child sexual exploitation images and videos (i.e., child pornography) and child sex tourism. The primary purpose of the system is to consolidate information (hereinafter, tips) related to these crimes into a single database; to track, link, and deconflict the tips; and to prioritize and refer the tips to HSI agents for investigation. By aggregating tips and lead information about Internet-facilitated child exploitation crimes in a single repository, the ICE-CETS database allows investigators to identify links in otherwise unrelated matters to reduce redundant investigative work. ICE-CETS is not a case management system for these investigations, but rather a repository and tool that facilitates the efficient use of investigative resources by ensuring related tips are identified and assigned for proper follow up.

The Child Exploitation Investigations Unit (CEIU)[2] at the HSI Cyber Crimes Center uses ICE-CETS to store tips submitted by various sources. Examples of such sources include ICE domestic and foreign field offices, the public (through the DHS public tip line), local law enforcement agencies, foreign law enforcement agencies, the International Criminal Police Organization (INTERPOL), and non-governmental organizations involved in preventing and detecting child sexual exploitation. These tips usually consist of Internet-related data that is somehow connected to the child sexual exploitation crime, which law enforcement may be able to use to identify persons involved in the criminal activity and/or to connect related crimes. ICE and other law enforcement agencies may obtain this information through a seizure of evidence during a criminal investigation or from other sources, such as suspects, witnesses, informants, and members of the public.

---

[1] *See* DHS/ICE/PIA-017 ICE-CETS PIA (January 19, 2010), at www.dhs.gov/privacy.

[2] The Child Exploitation Investigations Unit was formerly known as the Child Exploitation Section.

Once received, tips are entered or uploaded into ICE-CETS and reviewed by CEIU personnel to determine if they are actionable. Actionable tips are those that contain plausible information that can be verified through investigatory means and that, if verified, may constitute illegal conduct. Actionable tips then go through an intake process that allows CEIU personnel to link tips, generate specific leads, and send those leads as an investigative referral to the appropriate HSI field office.

As part of the tip intake process, CEIU personnel research the tips to enhance the initial information received using standard investigative techniques, such as administrative summonses or subpoenas and searches of government, public, and commercial databases. While the investigative research is not performed in ICE-CETS itself, the results of such research are manually inputted into the system by CEIU personnel. In cases in which administrative summonses or subpoenas are issued, they are typically served on entities, such as Internet Service Providers and corporations, which may have records pertaining to online access and use.

With this update to the ICE-CETS PIA, ICE is expanding the use of ICE-CETS to include as system users personnel working for the Advanced Targeting Team (ATT) at the CBP National Targeting Center. CBP ATT responsibilities include the identification of persons who are of targeting interest to CBP, including individuals with criminal backgrounds who may be attempting to enter or exit the United States contrary to U.S. laws. CBP ATT will use ICE-CETS to interdict Traveling Child Sex Offenders (TCSO), who are U.S. citizens or lawful permanent residents who travel to foreign countries with the intention of engaging in illicit sexual conduct with minors.

Currently, CEIU and CBP ATT use a manual process to coordinate their law enforcement activities to better detect TCSOs who may be preparing to exit the United States or are reentering the United States after leaving the country undetected. For example, CBP's Automated Targeting System[3] alerts the ATT that a traveler flagged as a registered sex offender will be boarding an outbound flight from the United States. CBP ATT personnel request that CEIU query the traveler's identifying data in ICE-CETS to see if the data is relevant to a developing HSI investigation. CEIU sends back the results, and CBP ATT personnel develop a risk assessment for the traveler and compare data from ICE-CETS and other law enforcement databases against lookouts and patterns of suspicious activity identified through past investigations and intelligence. Ultimately, the ICE-CETS data enhances CBP ATT's ability to make a decision about whether the traveler should receive additional screening prior to arrival at a port of entry (POE) or be referred to secondary at a POE.

Providing CBP ATT personnel with direct access to ICE-CETS will improve the efficiency of these law enforcement operations by eliminating the manual transmission of ICE-CETS data between ICE and CBP and allowing authorized CBP ATT personnel to query data

[3] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS) PIA, at www.dhs.gov/privacy.

within ICE-CETS directly when pursuing TCSO traveler targeting leads. For example, in the course of conducting research prior to a traveler's arrival at an airport, CBP ATT personnel may query in ICE-CETS a name that appears on an airline passenger list days before the scheduled flight in order to resolve any issues before the traveler arrives at the airport. Similarly, CBP ATT may query ICE-CETS after a traveler's arrival at an airport and use the data to enhance its decision-making on whether the traveler should be referred to secondary.

Reason for the PIA Update

This PIA is being updated to reflect that CBP ATT personnel will be granted user privileges to ICE-CETS and to specify what uses will be made of the data by CBP ATT personnel.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There are no changes to the information collected and stored within ICE-CETS, as the data maintained in the system will continue to be investigative information related to Internet-facilitated child sexual exploitation crimes as described in Section 1.1 of the DHS/ICE/PIA-017 ICE-CETS PIA (January 19, 2010). Note: The investigative information may now include notes of any relevant CBP targeting data made in ICE-CETS by CBP ATT users. For example, CBP ATT personnel may note a subject's flight number and date, or that the subject received additional screening.

Uses of the System and the Information

ICE is expanding the use of ICE-CETS by granting select CBP ATT personnel direct user access to the system. These personnel work in conjunction with CEIU to identify registered sex offenders and suspected TCSOs who travel from the United States to foreign destinations with the intention of engaging in illicit sexual conduct with minors. To assist CBP ATT with culling data on targeting leads, CEIU began manually sharing ICE-CETS data with CBP ATT upon receiving the ICE-CETS Authority to Operate on August 19, 2011.

The manual process by which CEIU shares select ICE-CETS data with CBP ATT works as follows. First, CBP ATT personnel request ICE-CETS data by emailing their requests along with relevant traveler targeting data to CEIU. CBP ATT requests typically contain a traveler's personal identifiers (e.g., name, email, Internet-based username). CEIU personnel then query ICE-CETS using the data provided by CBP ATT, generate the results of the query (i.e., whether the traveler is relevant to a developing HSI investigation and any associated information, if available), and return the results to CBP ATT via email. CBP ATT uses ICE-CETS data to enhance its decision-making on whether the traveler should receive additional screening or be referred to secondary. This manual process proves time-consuming and burdensome, and does

not allow for automated tracking, follow up, or statistical reporting of the data provided to CBP ATT.

Direct ICE-CETS user access for CBP ATT personnel will eliminate the manual transmission of data from CEIU to CBP. The ICE-CETS users within CBP ATT will be granted permissions to conduct queries, view query results, and make notes in the ICE-CETS record, including the notation of any relevant CBP targeting data. CBP ATT users will incorporate the relevant query results from ICE-CETS into the CBP risk assessment and forward to the appropriate CBP office for comparison against lookouts and patterns of suspicious activity identified through past investigations and intelligence. If CBP does not have an officer assigned as a liaison to a foreign customs or law enforcement office, then CBP ATT will contact the local HSI office for additional data analysis.

Granting CBP ATT personnel user privileges to ICE-CETS will accelerate data distribution to and by CBP ATT and better facilitate intradepartmental lead sharing and deconfliction. In addition, CBP ATT access to ICE-CETS will automate system research and tracking for CBP traveler targeting leads and will allow for trend analysis and general statistical reporting by both ICE and CBP.

The expansion of ICE-CETS to include CBP ATT personnel presents the risk that CBP ATT users may have access to information in ICE-CETS that is in excess of what they need-to-know in order to perform their duties. This risk was considered and mitigated by system auditing and user training. All user actions conducted on ICE-CETS are logged and auditable. The system logs user ID, login time, login attempts, logoff time, failed login attempts, and any changes to data records. In addition, in completing required ICE-CETS application training, all users are reminded of the restricted access to and limited use of the system. Users must also take mandatory annual privacy and security trainings, which stress the importance of authorized use of data in government systems.

Retention

There are no changes to the retention period of the data. The ICE-CETS records retention schedule was approved by the National Archives and Records Administration on March 26, 2010 (N1-567-10-014).

Internal Sharing and Disclosure

As described above, ICE is expanding the use of ICE-CETS by granting select CBP ATT personnel direct user access to the system. These personnel work in conjunction with CEIU to identify TCSOs and use ICE-CETS data to enhance their decision-making on whether the traveler should receive additional screening or be referred to secondary. Direct CBP ATT user access will eliminate the current method of manual transmission of lead data, and instead retain the data in a limited access, secure, and audited database, which improves the security of that

information. CBP ATT users access the ICE-CETS system via IRMnet, the secure ICE Network.

CBP ATT's direct access to ICE-CETS presents the risk that CBP ATT users may further share ICE-CETS data with unauthorized parties. This risk has been mitigated as CBP's re-dissemination of ICE-CETS data is not permitted unless CBP has received ICE's express authorization. CBP ATT users are trained on this restriction.

External Sharing and Disclosure

There are no changes to the external sharing of ICE-CETS data.

Notice

There are no changes to the notice required or provided to individuals whose information may be maintained in the system. General notice about the information maintained in the system, its uses, and how that information is shared is provided by the DHS/ICE/PIA-017 ICE-CETS PIA (January 19, 2010) and this update.

Individual Access, Redress, and Correction

Individuals who believe they have been improperly identified for additional screening by CBP as a result of ICE-CETS data may seek redress through the DHS Traveler Redress Program ("TRIP").[4] TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports and train stations or crossing U.S. borders. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 S. 12th Street, TSA-901, Arlington, VA 20598-6901 or online at www.dhs.gov/trip.

There are no other changes to individual access, redress, and correction.

Technical Access and Security

CBP ATT users access the ICE-CETS system via IRMnet, the secure ICE Network. Direct access to ICE-CETS is strictly controlled by the ICE-CETS program manager in cooperation with the system administrator, both of whom are CEIU personnel. ICE restricts the CBP ATT user's privileges in ICE-CETS based on his or her job responsibilities, and user privileges are reviewed regularly to ensure that users who no longer require access are removed from accessing the system. CBP ATT users will be granted "investigator" user privileges, which provide users with read-write access but prevents them from deleting records.[5] Thus, CBP ATT users will be able to conduct lead queries, view query results, and add notes to the records, but will not be able to otherwise edit or delete existing records and create new records. All CBP

[4] *See* DHS/ALL-005 DHS Redress and Response Records System SORN (72 FR 2294, January 18, 2007).
[5] *See* Section 8.1 of the ICE-CETS PIA (January 19, 2010) for additional information about the Investigator user role.

ATT queries will be logged in the system in the same manner as ICE user queries. Periodic audits on system usage are conducted by the system administrator in coordination with the ICE-CETS program manager.

Before being granted access to ICE-CETS, CBP ATT users will be required to complete an ICE-supervised familiarization period on the ICE-CETS test system. Once nominated for ICE-CETS access by a CBP supervisory officer, the CBP ATT user will be trained and certified on the system by CEIU personnel. CBP ATT users will be required to be in compliance with the standard DHS IT system tests and reviews as well as demonstrate that they have sufficient knowledge of the system. The ICE-CETS system administrator will review for compliance all CBP ATT users, and the program manager will grant CBP ATT users final approval for access to the system. After being granted access to the system, all CBP ATT users will be bound by DHS Rules of Behavior and will be under the scope and authority of their CBP chain of command. All CBP ATT users are also required to complete annual privacy and security trainings, which stress the importance of authorized use of data in government systems.

In the event of future changes concerning information in ICE-CETS, new users of ICE-CETS, or intended uses of the information collected and maintained in the system, CEIU will engage the ICE Privacy Office to discuss the intended expanded users and/or uses of this information and update the relevant privacy compliance documentation (including the ICE-CETS PIA) as appropriate.

Technology

There are no changes to the ICE-CETS technology.

Responsible Official

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

Approval Signature

Original signed copy on file with the DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security