Privacy Impact Assessment Update
for the

TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative

DHS/CBP/PIA-009(a)

August 5, 2011

Contact Point
Jacqueline Russell-Taylor
Office of Intelligence and Investigative Liaison
Customs and Border Protection
202-344-1276

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

Abstract

U.S. Customs and Border Protection (CBP) is publishing this update to the Privacy Impact Assessment (PIA) for DHS/CBP/PIA-009 the TECS System: Primary and Secondary Processing (TECS), dated December 22, 2010.[1] TECS (not an acronym) is the updated and modified version of the former Treasury Enforcement Communications System. TECS is owned and managed by the U.S. Department of Homeland Security's (DHS) component U.S. Customs and Border Protection (CBP). TECS is the principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons. This update will evaluate the privacy impacts of identifying certain of the operational records maintained in TECS as Suspicious Activity Reports (SARs) for inclusion in the National SAR Initiative (NSI), which is led by the Department of Justice on behalf of the entire federal government.

Introduction

TECS is an information-sharing platform, which allows users to access different databases that may be maintained on the platform or accessed through the platform, and the name of a system of records that include temporary and permanent enforcement, inspection, and operational records relevant to the anti-terrorism and law enforcement mission of CBP and numerous other federal agencies that it supports. TECS not only provides a platform for interaction between these databases and defined TECS users, but also serves as a data repository to support law enforcement "lookouts," border screening, and reporting for CBP's primary and secondary inspection processes.

As part of their mission responsibilities, CBP officers and Border Patrol agents may enter free-form text reports based upon their observations and interactions with the public at the border. These reports are maintained in TECS as Memoranda of Information Received (MOIRs). CBP officers and Border Patrol agents create MOIRs, when using TECS, to document an observation relating to an encounter with a traveler, a memorable event, or noteworthy item of information particularly when they observe behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention. Additionally, Border Patrol agents create Field Intelligence Reports (FIRs), when they are using the Intelligence Records System (IRS)[2] operated by U.S. Immigration and Customs Enforcement (ICE), also to document noteworthy incidents or observed activities.

---

[1] DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing PIA, (Dec. 23, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_tecs.pdf

[2] DHS/ICE-006 – Intelligence Records System (75 F.R. 9233) http://edocket.access.gpo.gov/2010/2010-4102.htm

In its role as an information sharing platform, TECS ingests the FIRs from IRS. Once in TECS, the FIRs are converted to MOIRs. These narrative reports are accessible to all users of TECS to provide broader information regarding the context of a record or activity being reported. The MOIRs also serve to provide information that may be associated with other data in TECS to permit identification of related incidents. This information is available to Border Patrol agents, CBP officers, and to those authorized to use TECS.

Reason for the PIA Update

DHS/CBP is updating the existing DHS/CBP/PIA – 009 TECS, published on December 22, 2010, to identify its use of the MOIRs in TECS (both MOIRs and FIRs from IRS) as CBP's source records for review, consideration, and nomination as Suspicious Activity Reports (SARs) for the Departments Information Sharing Environment (ISE) - SAR Initiative.[3] The Office of Intelligence and Investigative Liaison (OIIL) within CBP uses the MOIRs (and converted FIRs) from the CBP officers and Border Patrol agents as the source reporting for submissions of SARs to the DHS SAR Vetting Tool that meet the Nationwide Suspicious Activity Reporting Initiative (NSI) criteria established by the Department of Justice .[4] Those MOIRs that are submitted to the NSI are referred to as ISE-SARs. A team of OIIL analysts routinely performs a manual review of MOIRs in TECS to identify those reports. An OIIL analyst will nominate a MOIR (or converted FIR) to the SAR Vetting Tool, and subsequently an OIIL supervisor will review and approve it to become an ISE-SAR before it is released to the larger federal, state, and local law enforcement community.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

This update is providing additional transparency around the description of free-form text described currently in the TECS PIA. During the course of their duties, CBP Officers and Border Patrol Agents will create MOIRs and/or FIRs which become ingested into TECS as MOIRs as part of the free-form text reports that are currently recorded in TECS by authorized users. The existing TECS PIA does not explicitly call out these reports, and so with this update CBP is describing the process for the collection of an observation relating to an encounter with a traveler, a memorable event, or noteworthy item of information. As a general matter, these types

[3] DHS/All/PIA-032 Department of Homeland Security Information Sharing Environment Suspicious Activity Reporting Initiative, (Nov. 17, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-ise.pdf

[4] See DHS/ALL/PIA-032 for more details on the ISE-SAR Functional Standard Version 1.5 and the Department-wide approach.

of reports are created after an interaction at the Port of Entry (POE) or between the POEs. The MOIRs are a subset of the data collected by CBP and maintained in TECS as described in the existing PIA and does not change the nature of the information collected and stored within TECS.

Uses of the System and the Information

This update does represent an expansion of the use of certain information contained in TECS. The nomination of certain MOIRs to be cross designated as ISE-SARs for use in the NSI is a further use of TECS information. This cross designation does not change the information maintained in TECS. The identification of certain MOIRs as ISE-SARs is a further use and sharing of those records with another DHS system, the DHS SAR Vetting Tool.

While the use of MOIRs that are cross designated as ISE-SARs expands the use of that information from TECS, it does not represent a change with respect to the nature of the use of that information. TECS presently uses MOIRs to inform its own user community of federal, state, local, and foreign law enforcement officers about noteworthy events and activities occurring under CBP observation or incidental to CBP enforcement activities. Inclusion of certain MOIRs as ISE-SARs will broaden the scope of dissemination of that information, but it will not change the purpose for which the records were intended. This use of MOIRs as SARs is entirely consistent with the purpose of the MOIR. As such, there is no qualitative change to the privacy risks associated with MOIRs through this further use of a subset of these records as SARs. Persons identified in MOIRs may be associated with other law enforcement incidents similar to the manner in which persons identified in SARs may become associated with law enforcement incidents. This risk is mitigated through investigatory procedures designed to validate leads through cross referencing with independently obtained information and officer/agent training.

Retention

There is no change to the TECS retention schedule posed by this update.

Internal Sharing and Disclosure

This update causes a change to internal sharing within DHS because those TECS MOIRs identified as ISE-SARs will be shared through the DHS SAR Vetting Tool with DHS's ISE-SAR (Information Sharing Environment – Suspicious Activity Report) server. This sharing amounts to a copying of certain MOIRs from TECS and nominating them to be submitted and stored as SARs in the DHS ISE-SAR sever. The main privacy risk presented by this sharing of MOIRs with the ISE-SAR server is that an MOIR may be mistakenly nominated as meeting the NSI criteria. This privacy risk is mitigated in two ways: first, through the specialized training provided to the SAR nominating team from OIIL that submits MOIRs to become SARs; and secondly, through supervisory review of all nominated SARs. Additionally, there is a risk that

since the information is being manually entered by the OIIL analysts, that the information could be inaccurately entered. Similar to the above, this risk is mitigated by the training and the supervisory review.

External Sharing and Disclosure

This update discusses a change to external sharing in that information that is currently available as MOIRs within TECS to a limited number of federal partner agencies with authorized TECS access. A portion of those MOIRS will now also be available to a larger federal, state, and local law enforcement community as a ISE-SAR from the DHS ISE-SAR server. The main risk posed by this larger dissemination of certain information from TECS is that information misidentified as an ISE-SAR may result in other law enforcement activities occurring in mistaken reliance upon the information. This risk is mitigated through standard investigatory practices by the receiving officers, and by supervisory review of SARs prior to their being release to the larger law enforcement community.

Notice

The DHS/CBP-011 - U.S. Customs and Border Protection TECS SORN was last published in the *Federal Register* on December 19, 2008, 73 FR 77778, and remains accurate and current. Routine Use G covers this sharing.

Individual Access, Redress, and Correction

No changes have been made to access, redress, and correction. The Secretary of Homeland Security has exempted TECS from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, CBP will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in TECS, or seeking to contest its content may gain access to certain information in TECS about themselves by filing a Freedom of Information Act (FOIA) request with CBP at:

U.S. Customs and Border Protection

FOIA Division

799 9th Street NW, Mint Annex

Washington, DC 20229-1177

Technical Access and Security

The expanded sharing of information with the DHS ISE-SAR server will be conducted in conformance with existing information technology security protocols, including encryption.

Technology

No Changes.

Responsible Officials

Jacqueline Russell-Taylor, Director, Policy
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection
Department of Homeland Security

Laurence E. Castelli, Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Final signed version on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security