Privacy Impact Assessment Update for the

REMEDY Enterprise Services Management System

DHS/CBP/PIA-029(a)

May 28, 2020

Contact Point

Marshall Nolan
Border Enforcement and Management Systems Directorate
Office of Information and Technology
(571) 468-6862

Reviewing Official

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Office of Information and Technology's (OIT) REMEDY Enterprise Services Management serves as an intake tool for CBP technical support and customer service personnel supporting non-CBP persons from other Government agencies, state, local and federal law enforcement entities, as well as trade-related organizations requiring access to CBP-owned information technology systems. CBP previously published a Privacy Impact Assessment (PIA) discussing the use of REMEDY, both as an internal intake tool for CBP technical support as well as customer service for members of the public to submit queries related to various agency programs. CBP is updating the PIA to provide notice that REMEDY has been updated to only provide support for individuals requiring access to CBP systems or information. CBP has created various public programmatic websites to provide direct customer service support to members of the public and has removed these services from the REMEDY tool.

Overview

CBP OIT's REMEDY Enterprise Services Management System (REMEDY) is a technology services suite that manages: 1) information technology (IT) help desk service requests; 2) system maintenance activities and system and hardware outage support; 3) new IT system testing and evaluations; and 4) technology asset and property tracking. Originally, REMEDY served as an intake tool for CBP technical support and customer service personnel supporting non-CBP persons from other Government agencies, state, local and federal law enforcement entities, as well as trade-related organizations requiring access to CBP-owned IT systems.

CBP OIT uses REMEDY to manage Information Technology (IT) help desk service requests and create support "ticket numbers" for various technology incidents involving outages, software vulnerabilities, system access issues, patch management, hardware issues, and other IT enterprise management activities. It also serves as a tool to track and manage some CBP technology assets and/or property (e.g., laptops, desktops, circuits, and cameras). REMEDY allows the agency to maintain a working knowledge-base of help desk support information.

Reason for the PIA Update

Previously, REMEDY was used as an intake tool for CBP technical support as well as for managing queries submitted by members of the public related to benefit status, traveler redress, travel and port of entry policies, as well as agency programs. CBP is updating this PIA to provide notice that REMEDY no longer serves as an intake tool to track queries and requests from the general public via the following public-facing websites:

- CBP Customer Service (Contact Us) website;[1]
- CBP Information Center (help.CBP.gov);[2]
- Global Online Enrollment System (GOES) web portals,[3] and
- The toll-free CBP Inquiries telephone line.

CBP is developing a Redress PIA, which will provide notice of the various programs through which members of the public may request information and redress from CBP. In addition, CBP is also drafting a CBP Compliments, Questions, Complaints and Comments Management System (CQC2MS) PIA to provide additional notice for a customer-service system designed to address a broad spectrum of questions, complaints, and comments voluntarily submitted by members of the public.

However, REMEDY continues to serve as an intake tool for external federal, state, local, tribal agencies or trade organizations and stakeholders seeking technical support to access various CBP managed law enforcement, trade and/or travel information technology systems. These systems include, but are not limited to, the Automated Targeting System (ATS),[4] TECS,[5] and the Automated Commercial Environment (ACE).[6]

Current Uses of REMEDY to support CBP IT System Users

CBP uses REMEDY to track and manage CBP internal IT and asset management activities, such as:

- IT Help Desk requests;
- IT system access requests;
- Technology incidents involving system or hardware outages;
- Software vulnerabilities and patch management;
- Hardware distribution and management;
- New IT system testing and evaluations;
- IT Technician work order assignments; and

[1] *See*: http://www.cbp.gov/contact.
[2] *See*: https://help.cbp.gov/.
[3] CBP no longer uses GOES, however all inquiries and information collected about trusted travelers that was stored in REMEDY was collected via GOES.
[4] DHS/CBP/PIA-006 Automated Targeting System; *See:* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf.
[5] DHS/CBP/PIA-021 TECS System: Platform; *See:* https://www.dhs.gov/sites/default/files/publications/DHS-PIA-ALL-021%20TECS%20System%20Platform.pdf.
[6] DHS/CBP/PIA-003 Automated Commercial Environment (ACE); *See:* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_aceitds.pdf.

- Technology asset and property life cycle management (including laptop and desktop computers, and mobiles devices).

CBP technical support personnel use REMEDY when they receive a call or email to the CBP Help Desk from CBP personnel requesting IT support. Technical support personnel initiate an incident ticket and request the individual's name and CBP identification number (HashID) to verify the requestor's identity. CBP uses HashID to verify identity prior to granting access to certain CBP IT systems or providing technical support. Those individuals who either do not have a HashID or do not remember their information are given an identifier based on their first and last names. No Social Security numbers (SSNs) are collected or retained in the REMEDY system.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authorities and other requirements associated with CBP's collection, use, maintenance, and dissemination of information within REMEDY have not changed since the original PIA was published in 2016, with the exception of authorities specific to the Trusted Traveler Programs indicated in the previous PIA.[7] REMEDY no longer collects information regarding the Trusted Traveler Programs and the aforementioned authority no longer applies.

The SORN that governs maintenance, use and dissemination of REMEDY-related data is DHS/ALL-004 General Information Technology Access Account Records System of Records.[8]

An updated system security plan is available as part of the authority to operate (ATO), which now expires on August 29, 2021.

The records retention schedules approved by the National Archives and Records Administration (NARA) that apply to the remaining types of REMEDY records will be revised to meet the current business needs as defined in the Data Retention by Project section of this PIA.

REMEDY is not covered by the Paperwork Reduction Act (PRA).

Characterization of the Information

CBP continues to collect information directly from CBP employees and contractors seeking IT technology support, in addition to information directly from non-CBP persons seeking

[7] *See* Homeland Security Act of 2002, as amended, Section 402.6; 44 U.S. Code § 3534 - Federal agency responsibilities; E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA); Executive Order 9397 (SSN), as amended by E.O. 13478; and DHS Sensitive Systems Policy Directive 4300A.

[8] *See* DHS/ALL-004 General Information Technology Access Account Records System of Records, 77 FR 70792 (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

access to CBP-owned law enforcement, trade, or travel-related IT systems for official business. The information being collected on employees, contractors, and non-CBP persons seeking IT support or access to a CBP-owned system for official business purposes will remain the same.

Employees, contractors, and non-CBP persons seeking IT support or access to a CBP-owned System for Official Business Purposes:

- Full name;
- HashID (CBP employees only);
- Agency or business entity name;
- Business location/address;
- Work or mobile telephone number;
- Email address;
- Business, mobile, or home telephone number (for teleworkers);
- Login or password information;
- Name of IT system attempting to access (if applicable);
- Device name or number; and
- Ticket number (for existing support requests).

Although the previous PIA stated that REMEDY collected SSNs from non-CBP persons who require access to CBP-owned systems for official business purposes, CBP does not actually collect SSNs in this system.

REMEDY will no longer collect the following information about members of the public who seek assistance in accessing or creating online accounts to manage their trusted traveler program memberships:

- Full name;
- Trusted Traveler identification number;
- Login or password information (for access to a trusted traveler system);
- Email address;
- Home address;
- Home or mobile telephone number; and
- Ticket number (for existing support requests).

REMEDY does not use information from commercial sources or publicly available data.

The accuracy of the data maintained in REMEDY is ensured by collecting the information directly from the individuals seeking support.

Privacy Risk: CBP does not have clear legal authority to collect SSNs from CBP employees, contractors, and non-CBP personnel in order to generate the HashID number that is used to provide system account access.

Mitigation: This risk is mitigated. The REMEDY system continues to use HashID as the means to identify CBP users in order to track their tickets. While the HashID is derived using an individual's SSN, CBP does not collect or use the actual SSN in the REMEDY system. If an individual does not have or know their HashID, their tickets are tracked by first and last name (or something similar).

Uses of the Information

The uses of the REMEDY information remain the same with the exception of information related to individuals seeking assistance with access to online accounts and publicly available websites such as the CBP trusted traveler programs. The data on these individuals that will no longer be collected or used includes: name, trusted traveler identification number, home address, CBP program requiring support, contact information, and incident ticket number (for existing incidents).

REMEDY does not use technology to conduct electronic searches, queries, or analyses. There are no other DHS components with assigned roles and responsibilities within the REMEDY system.

Privacy Risk: There is a risk of identity theft or harm to individuals in the event of a breach or unauthorized access to information within REMEDY due to the use of SSN to generate the HashID.

Mitigation: This risk is fully mitigated. The REMEDY system continues to use HashID and access controls to restrict access to data but it does not collect or use the actual SSN in the system. CBP will research options to issue user log-in credentials that do not rely on the SSN in the future.

Notice

Given the change in the customer support for REMEDY, there will no longer be REMEDY-related notices provided through general privacy policy statements on the Trusted Traveler Program public-facing websites. To the extent users create an account to access another type of CBP system, such as users from other Government agencies, state, local and federal law enforcement entities, as well as trade-related organizations requiring access to CBP-owned IT systems, notice is provided at the time of account creation.

Individuals still have the right to withhold consent to provide information to address their IT or customer service matters, but doing so will prevent technical support and customer service personnel from addressing the individual's matter in an efficient and effective manner.

Privacy Risk: There is a risk that individuals who access CBP systems may not know exactly how CBP uses SSNs and HashIDs during the identity verification process or whether the agency retains that information within the REMEDY system or other agency systems or databases.

Mitigation: This risk is mitigated. CBP uses HashID as a unique identifier for CBP employees and some combination of first and last names to authenticate other individuals needing help desk support. No SSN is ever solicited from customers calling into the Help Desk as there is an alternative identity verification process.

Data Retention by the project

CBP Records and Information Management (RIM) is working with NARA and the REMEDY team to develop a revised records retention schedule. To meet this business need, RIM will create a CBP-specific retention schedule that based on General Records Schedule (GRS) 5.8, Item 010, Technical and Administrative Help desk Operational Records, and GRS 6.5, Item 010, Public Customer Service Records. At the time of publication of this PIA, all system records will remain active for three years, be archived for two years, and be deleted at the end of the five-year period.

GRS 3.1, Item 030 allows CBP to retain configuration and change management records for five years, but longer retention is authorized if needed for business use.

According to GRS 3.2, Item 031, CBP employee system access records maintained for REMEDY will be destroyed or deleted 6 years after the user account is terminated or when no longer needed for business use, whichever is later.

Privacy Risk: There is a risk that PII may be retained for longer than necessary to fulfill the specified purposes.

Mitigation: This risk is mitigated. CBP mitigates this risk by deleting IT customer service files when no longer needed for review and analysis pursuant to the NARA-approved retention schedules. The risk is further mitigated by security measures that render PII used for IT or customer service support unusable in other CBP systems that require PIV cards for access purposes.

Privacy Risk: There is a risk that the REMEDY system will continue to store the inquiries related to trusted traveler account issues despite no longer needing it for business purposes.

Mitigation: This risk is mitigated. The REMEDY system has purged all previously collected trusted traveler inquiry information prior to the publication of this PIA.

Information Sharing

CBP still does not share information contained in REMEDY outside of DHS. There is no privacy risk to information sharing.

Redress

There are no changes to the redress procedures for the REMEDY system. The privacy risks and mitigation related to redress remain the same.

Auditing and Accountability

There are no changes to how REMEDY ensures that information is used in accordance with stated practices in this PIA Update. There are no changes to the annual or role-based training offered in relation to the REMEDY system. There are no changes to the access granting procedures for REMEDY. There are no changes to the review and approval of information sharing agreements, uses of the information or new access to REMEDY by organizations within DHS and outside.

Responsible Official

Debra L. Danisek
CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Mario Travi
Director
Mission Support Branch
Border Enforcement and Management Systems Division
Office of Information Technology
U.S. Customs and Border Protection

Approval Signature

[Original signed copy completed and on file with the DHS Privacy Office]

____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security