



Privacy Impact Assessment
for the

REMEDY Enterprise Services Management System

DHS/CBP/PIA-029

April 28, 2016

Contact Point

Marshall Nolan

Border Enforcement and Management Systems Division

Office of Information Technology

U.S. Customs & Border Protection

(571) 468-6862

Reviewing Official

Karen L. Neuman

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 Technology's (OIT) REMEDY Enterprise Services Management System is a technology services suite that manages: 1) information technology (IT) help desk service requests, 2) maintenance activities, system, and hardware outage support, 3) new IT system testing and evaluations, and 4) technology asset and property tracking. REMEDY also 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 IT systems. Additionally, REMEDY allows members of the public to obtain customer service assistance and submit inquiries related to benefit status, traveler redress, travel and port of entry policies, as well as agency programs. CBP is conducting this Privacy Impact Assessment because this system collects personally identifiable information (PII) about members of the public.

Overview

REMEDY is a modified suite of commercial-off-the-shelf (COTS) software applications used to manage technical support and other service-oriented activities throughout CBP's technology enterprise. CBP technical support and customer service personnel use REMEDY to create and track numerical incident "tickets" to manage: 1) information technology (IT) help desk service requests; 2) maintenance activities, system, and hardware outage support; 3) new IT system testing and evaluations; and 4) technology asset and property tracking. Customer service inquiries may be submitted by three types of individuals: from CBP employees and contractors; non-CBP persons who have access to CBP systems for official business; or members of the public who have voluntarily applied for trusted traveler programs.

The types of information that REMEDY collects vary based on the whether the individual submitting a support request requires access to CBP systems for official business purposes, or if the individual is a trusted traveler trying to access his or her own profile within the Global Online Enrollment System (GOES).

Access to CBP IT Systems for Official Business

Generally, CBP uses REMEDY to track and manage CBP internal information technology (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
- Technology asset and property management (including but not limited to laptop and desktop computers, mobile devices, and/or smartphones).

CBP technical support personnel use REMEDY when they receive a call or email to the CBP Help Desk from CBP personnel requesting IT support. CBP converts employee and contractor Social Security numbers (SSN) into CBP identification numbers, also known as a “HashID” and uses the information to verify identity prior to granting access to certain CBP IT systems or providing technical 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. Almost all CBP IT systems run on the TECS platform, which is a legacy mainframe and required users to use their SSN for log-in. To deviate from using the SSN as a log-in identifier, CBP instead issues a HashID. All CBP employees and contractors have a HashID, whether or not they require access to TECS.

In addition to managing internal IT support requests, CBP technical support and customer service personnel use REMEDY to manage external requests from non-CBP persons seeking technical support to access various CBP-owned law enforcement, trade, or travel-related IT systems for official business. These systems include the Automated Targeting System (ATS), TECS, Electronic System for Travel Authorization (ESTA), and the Automated Commercial Environment (ACE).¹

To gain access to CBP-owned IT systems (pursuant to their official duties), non-CBP persons that work for other DHS components or local, state, or federal law enforcement entities, must first seek approval through their agency’s approving official and the CBP authorizing official for access to the system requested. Following the approval process, non-CBP persons contact the CBP Technical Service Desk and present their full name and Social Security number (SSN) verbally to technical support personnel who converts the SSN through CBP’s mainframe IT system (TECS) into a HashID that the individual uses to access the requested system. CBP does not retain the individual’s SSN in REMEDY but stores it in the Mainframe IT system to facilitate access for individuals that cannot recall their HashID.

Trusted Traveler Assistance

CBP technical support and customer service personnel also use REMEDY as a workflow management tool to assist members of the public seeking eligibility information or application

¹ See: <http://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



status updates on various CBP trusted traveler programs² or seeking access to the associated trusted traveler system(s) for which they have applied or been accepted. These individuals do not have access to the CBP trusted traveler systems (beyond access to their own application or profile), but rather are requesting assistance with their specific record or application.

CBP also uses REMEDY to support individuals accessing public-facing websites such as CBP Customer Service (Contact Us) website,³ CBP Information Center (help.CBP.gov),⁴ Global Online Enrollment System (GOES) web portals,⁵ and the toll-free CBP Inquiries telephone line. CBP may request contact information in order to direct the individual to the correct point of contact for traveler/border crossing matters, access to CBP IT systems used for law enforcement, trade, or travel purposes, or access to U.S. entry or exit records.

CBP does not generate a HashID, nor collect SSN, for any individual who contacts the CBP Help Desk as an individual needing assistance with a trusted traveler program.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CBP may collect and maintain records pursuant to:

- Homeland Security Act of 2002, as amended, Section 402.⁶
- 44 U.S. Code § 3534 - Federal agency responsibilities.⁷
- E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA).⁸
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 7208.⁹
- DHS Immigration Regulations on Inspection of Persons Applying for Admission into the United States.¹⁰

² See: <http://www.cbp.gov/travel/trusted-traveler-programs>.

³ See: <http://www.cbp.gov/contact>.

⁴ See: <https://help.cbp.gov/>.

⁵ See: <https://goes-app.cbp.dhs.gov/main/goes>.

⁶ See: Pub.L. 107-296.

⁷ See: [44 U.S.C. § 3534](#)

⁸ See: Pub.L. 107-347.

⁹ See: Pub.L. 108-458.

¹⁰ See: 8 CFR Part 235.1.



- Executive Order 9397 (SSN), as amended by E.O. 13478.¹¹
- DHS Sensitive Systems Policy Directive 4300A.¹²

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The SORNs that govern maintenance, use, and dissemination of REMEDY-related data include:

- DHS/ALL-004 General Information Technology Access Account Records System of Records.¹³

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. CBP completed the System Security Plan for REMEDY on May 19, 2015. A new Authority to Operate (ATO) is pending publication of this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. NARA approved the following retention schedules in September 2015:

In accordance with DAA-GRS-2013-0005-0004 (IT Operation and Maintenance Records), CBP retains these records for 3 years after the agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded.

In accordance with DAA-GRS-2013-0005-0007 (IT System Development Records), CBP will destroy the records 5 years after the system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes.

In accordance with N1-GRS-03-1 item 10b (IT Customer Service Files), CBP will destroy or delete the records after 1 year or when no longer needed for review and analysis.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

REMEDY is not covered by the PRA. However, individuals who submit trusted traveler

¹¹ Executive Order (E.O.) 9397, as amended by E.O. 13478, 73 FR 70239 (November 20, 2008).

¹² See: http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf

¹³ 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>.



applications are provided notice, and OMB reviews the forms at the original point of collection (for example, the online ESTA application). These trusted traveler systems, while supported by REMEDY, have their own information collection requirements and/or Office of Management and Budget (OMB) control numbers when applicable.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Depending on the individual submitting a request or seeking IT support, CBP collects different information. In addition to IT system, software, or technology-related information, CBP collects the following information from the following individuals:

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

- Full name;
- HashID;
- SSN (used to convert into a HashID for non-CBP persons who require access to CBP-owned systems for official business purposes);
- 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).

Members of the public who seek trusted traveler program assistance:

- 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).

2.2 What are the sources of the information and how is the information collected for the project?

CBP collects information directly from CBP employees and contractors seeking IT technology support. CBP also collects information directly from non-CBP persons seeking access to CBP-owned law enforcement, trade, or travel-related IT systems for official business. In addition, CBP collects information directly from members of the public requesting information about, or assistance with, CBP trusted-traveler or other agency programs.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

Data is collected directly from the CBP employee or contractor, non-CBP persons, or members of the public seeking IT support, system access, or information on CBP trusted-traveler or other programs. Additionally, REMEDY automates IT help desk accuracy by mapping CBP employees' and contractor's HashID to their CBP network active directory to ensure that technical support reaches the assigned technician and the appropriate individual seeking support.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

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 not mitigated. There is no existing clear legal authority to collect SSNs from CBP employees, contractors, and non-CBP personnel for the purpose of granting



account access. The only means by which this risk can be mitigated is for CBP to move away from the use of SSN-derived personnel identifiers (HashID) in order to provide users with access to systems.

CBP must develop a centralized, enterprise-level identity management system to replace the HashID.

Privacy Risk: There is a risk of over-collection because CBP requires the collection of SSNs to create a system identifier. SSNs are not necessary to provide IT support but are required to assign unique identifiers to non-CBP persons seeking access to CBP-owned IT systems.

Mitigation: This risk is partially mitigated. CBP deletes the SSNs from the mainframe system when they are no longer needed to verify identities of non-CBP persons – however, this is typically after an individual has not logged into their account for some time. CBP disables the accounts of individuals that fail to access CBP systems within 30 days, or if they fail to timely retake required annual privacy training. If they fail to reapply for access, CBP archives the account in the mainframe system until it conducts its annual user authentication review. If the user no longer requires access to the system, CBP deletes the account and the SSN from the mainframe system.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP technical support and customer service personnel use the data listed in Section 2 to provide technical support and other service-oriented activities throughout CBP's technology enterprise. This information allows technical support personnel to create and track numerical incident "tickets" that are used to (1) manage help desk requests, (2) technology maintenance incidents, (3) assign work orders, (4) manage IT assets, (5) test and evaluate new IT systems, and (6) customer service inquiries throughout the lifecycle of the activity. CBP uses REMEDY to manage work order processing, maintenance, asset and property management, and overall IT enterprise management.

CBP Employees & Contractors:

Technical support personnel use employee and contractor information such as name, HashID, work location, device name/number, contact information, and incident ticket number (for existing incidents) in order to provide support for CBP IT systems, assets, and property.

Other Individuals with Access to CBP Systems:

CBP technical support personnel use the individual's information such as name, SSN (used to convert the SSN into a HashID for non-CBP persons), agency, business location, system or



program requiring support, contact information, and incident ticket number (for existing incidents) to provide support to entities seeking access to CBP-owned law enforcement, trade, or travel-related IT systems.

Trusted Travelers:

Technical support and customer service personnel use the individual's information such as name, trusted traveler number, home address, CBP program requiring support, contact information, and incident ticket number (for existing incidents). This information allows CBP to provide assistance to individuals seeking information on, or assistance with, trusted traveler programs.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that REMEDY-related PII could be used for purposes outside the scope of IT support or activities associated with other CBP programs.

Mitigation: CBP uses distinct login-password procedures, including personal identity verification (PIV) smart cards to access various systems and/or databases. These safeguards render PII obtained during the REMEDY IT support and customer service process unusable in other agency systems. The risk is further mitigated through role-based access rules governing technical support personnel usage.

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

Mitigation: This risk is partially mitigated by CBP's use of access controls within REMEDY. This risk cannot be fully mitigated until CBP ends its reliance on SSN to generate HashIDs for CBP system access.

The DHS Privacy Office recommends that CBP adopt a new, updated process for issuing user log-in credentials that does not rely on the SSN.



Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBP provides notice through general privacy policy statements on all public facing websites such as CBP's Customer Service (Contact Us) Internet Site, CBP Information Center (help.CBP.Gov), and Global Online Enrollment System (GOES) web portals. This PIA also serves as notice of how CBP manages PII associated with IT support or customer service activities.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

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

4.3 Privacy Impact Analysis: Related to Notice

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: CBP mitigates this risk by notifying non-CBP persons and members of the public verbally about the reason for soliciting the individual's SSN, HashID, contact information, or trusted traveler number in order to provide appropriate support. CBP plans to further mitigate this risk by enhancing the privacy notices on CBP customer service websites by including Privacy Act statements per the Privacy Act.¹⁴ See Appendix A.

¹⁴ 5 U.S.C. § 552(a)(e)(3); available at <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf>.



Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

Per DAA-GRS-2013-0005-0004 (IT Operations and Maintenance Records) approved in September 2014, CBP will destroy IT operations and maintenance records 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded.

Per N1-GRS-03-1 item 10a and 10b (IT Customer Service Files) approved in August 2015, CBP will destroy or delete the records after 1 year or when no longer needed for review and analysis.

These schedules authorize longer retention if required for business use.

5.2 Privacy Impact Analysis: Related to Retention

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 by the retention schedules. CBP mitigates this risk by deleting IT customer service files after 1 year or 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 may require PIV cards for access purposes. CBP also mitigates this risk by deleting the SSN and associated HashID from its secure Mainframe system following an annual user authentication review that confirms whether or not the user requires access to CBP-owned IT systems.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP does not share information contained in REMEDY outside of DHS.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CBP does not share information contained in REMEDY outside of DHS.

6.3 Does the project place limitations on re-dissemination?

CBP does not share PII contained in REMEDY with external entities.



6.4 Describe how the project maintains a record of any disclosures outside of the Department.

CBP does not share PII contained in REMEDY with external entities.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy risk to information sharing.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Although individuals submit the information maintained in REMEDY voluntarily to request IT support, system access, or information on CBP-owned programs or initiatives, they may request information about their REMEDY records or to seek corrections, pursuant to procedures provided by the Freedom of Information Act (FOIA)¹⁵ and the access provisions of the Privacy Act of 1974, and by writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
90 K Street, NE
Washington, DC 20229

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information.¹⁶ You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury,¹⁷ a law that permits statements to be made under penalty of perjury as a substitute for notarization. While your inquiry requires no specific form, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;

¹⁵ 5 U.S.C. § 552.

¹⁶ 6 CFR Part 5.

¹⁷ 28 U.S.C. § 1746; available at <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title28/pdf/USCODE-2011-title28-partV-chap115-sec1746.pdf>.



- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Non-CBP-persons may access, review, and correct inaccurate information in their user profile or records contained in CBP-owned IT systems.

Trusted traveler participants may access their GOES account to review and correct inaccurate information contained in their profile or in their records.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals have an opportunity to correct his/her information at the time of collection by IT technical support and customer service personnel. They may also submit a Privacy Act request as described in Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA explains how an individual may correct his/her information once obtained by the REMEDY system. In addition, CBP provides notice to individuals via the applicable SORNs in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is minimal risk that individuals may submit inaccurate information that might prolong or prevent technical or customer service support.

Mitigation: The individual mitigates any risk by providing accurate information to allow IT support or customer service personnel to address their matter or concern. They also have the option of using the process in Section 7.1 to address matters pertaining to systems supported by REMEDY.



Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CBP deploys extensive security measures to protect all collected information from inappropriate use and/or disclosure through both access controls and CBP employee information security and privacy training. REMEDY logs system access and OIT personnel conduct periodic compliance reviews of all REMEDY users.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS employees and contractors receive annual privacy awareness training. CBP requires REMEDY users to take separate role-based Security Awareness Training prior to granting access to the system. CBP OIT Account Management staff designate Master Administrators that manage role-based access. Individuals serviced through REMEDY incident tickets do not receive access to the system.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

CBP OIT Account Management staff identifies and selects REMEDY System Administrators that receive full access to the entire application. System Administrators may designate additional “master administrators” that maintain access to all of the application’s administrative tools. Master Administrators may designate REMEDY Developers and Administrators that maintain the right to create users based on an individual’s IT or customer service support role, need to know, and completed background investigation.

REMEDY access control procedures adhere strictly to the DHS Sensitive Systems Policy Directive 4300A. REMEDY employs an automated auditing tool that monitors account creation, modification, enabling, disabling, and removal actions and notifies System Administrators as needed.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All information sharing and MOUs concerning PII sharing, including those related to REMEDY, are created by the operational owner of the system and are sent to the CBP Privacy Officer and Office of Chief Counsel for review. Upon the review’s completion, CBP sends the



information to the DHS Privacy Office for final concurrence before approval and signing.

Responsible Officials

Marshall Nolan
Border Enforcement and Management Systems Division
Office of Information Technology
U.S. Customs and Border Protection

John Connors
Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security



APPENDIX A

Privacy Act Statement

Authority: CBP collects this information pursuant to Pub.L. 108-458, 8 CFR Part 235.1, and E.O. 9397 (SSN), as amended by E.O. 13478

Purpose: The information is used to provide support to individuals that request IT support, access to CBP-owned IT systems, or information on CBP programs or initiatives.

Routine Uses: CBP may share this information in accordance with the Privacy Act, 5 U.S.C. § 552(a) or pursuant to the Routine Uses in the System of Records Notices associated with the REMEDY System: DHS/ALL-004, General Information Technology Access Account Records System of Records.

Disclosure: Furnishing this information, including your Social Security number (SSN) or HashID, is voluntary. However, failure to provide the information may prevent CBP from verifying your identity in order to address your matter or concern. Your SSN will be used to convert the SSN into a HashID that you may use to access a CBP system or database. CBP may seek the SSN verbally to complete the conversion. CBP will store the SSN and HashID in a secure database until they are no longer needed to access CBP-owned IT systems.