Privacy Impact Assessment
for the

U.S. Customs and Border Protection Complaint Management System (CMS)

DHS/CBP/PIA-035

September 14, 2016

Contact Point
Barbara Aliño
Office of Public Affairs
U. S. Customs and Border Protection
(202) 325-8000

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

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) Complaint Management System (CMS) is a customer-service system designed to address a broad spectrum of complaints and comments voluntarily submitted by members of the public. Although these complaints and comments may involve any type of interaction with CBP, the majority of complaints and comments focus on travel, such as incidents involving passengers at a checkpoint; or trade, in connection with the entry and examination of goods into the United States. CBP is conducting this Privacy Impact Assessment (PIA) because CMS collects and uses personally identifiable information (PII) from members of the public.

Overview

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Office of Public Affairs (OPA) implemented the CBP Complaint Management System (CMS) in response to Executive Order (E.O.) 12862.[1] This E.O. requires all Executive departments and agencies to meet customer service standards by providing easily accessible information, services, and complaint systems, and by providing a means to address customer complaints. The CBP INFO Center website[2] provides easily accessible information and services via Frequently Asked Questions (FAQs), links, and a portal to CMS where individuals or their representatives can submit a complaint or comment concerning their interactions with CBP. CMS enables CBP to address customer complaints and comments by providing a unified tracking system to follow the life cycle of complaints and comments and analytical tools to measure responsiveness and customer feedback trends.

Through CMS, CBP manages the entire complaint and comment process from initial intake to tracking, referral, and closeout. CMS provides CBP officials with a more comprehensive understanding of CBP's public image, which is necessary to improve interactions with members of the public and to enhance responsiveness to customer concerns.

CBP shares information with appropriate CBP offices, DHS components, or other Federal Government agencies as appropriate to obtain feedback and resolution of complaints. In addition, CMS may refer complaints or comments to other entities when appropriate, as set out in section 6.0 below. For example, if CBP determines that a complaint or comment is more appropriately addressed by the DHS Traveler Redress Inquiry Program (TRIP),[3] CBP provides the individual

[1]Executive Order 12862, "Setting Customer Service Standards" (58 FR 48257), *available at:* http://www.archives.gov/federal-register/executive-orders/pdf/12862.pdf
[2]https://help.cbp.gov/
[3] Department of Homeland Security /ALL/PIA-00(a) - DHS Traveler Redress Inquiry Program (TRIP) June 5, 2013, *available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-dhstrip-20130605.pdf.* Department of Homeland Security/ALL- 005 - Redress and Response System of Records January 18, 2007 (72 FR 2294), *available at:* http://www.gpo.gov/fdsys/pkg/FR-2007-01-18/html/07-190.htm.

with information for filing a redress inquiry with DHS TRIP, and CBP then closes the case within CMS.

Information Collected in CMS:

CMS collects information that generally falls into four broad categories: (1) contact information to enable CBP to communicate with the individual or his/her designated representative; (2) information about the individual's experience to assist CBP in locating the associated information and identifying the office best able to address the issue; (3) additional personally identifiable information (PII) or documentation to verify the identity of the individual (as described in Section 2.2), as necessary; and (4) relevant information derived from appropriate programs and systems that is needed to address and resolve these complaints and comments. Details concerning the types of information collected are set out in section 2.1 below.

Individuals may submit complaints to CBP using one of three different methods: 1) telephone calls; 2) written correspondence (such as, by comment card available at the port of entry (POE), mailed letter, or fax); or 3) electronic submissions into CMS via the CBP INFO Center website. Complaints or concerns received via telephone calls or written correspondence are entered manually by CBP staff into CMS. Written correspondence is currently held in a locked cabinet pending approval of the record retention schedule. Once the schedule is approved, all written correspondence will be destroyed. The processes for the submission and collection of information related to an individual's complaint, or comment are discussed in Section 2.2 of this PIA.

Processing the Complaint or Comment:

Upon intake, all complaints or comments are issued a CBP control number. For complaints or comments made over the phone or in person, CBP staff provide a control (or reference) number to the complainant. For complaints or comments submitted via the online portal, CBP sends an acknowledgement of receipt with a unique control number or case file number to the individual's email. The acknowledgement instructs the individual to reference this unique control number when inquiring on the status of his or her case, whether telephonically or online. An individual may also register for an account in CMS by providing his or her name and email address to track the status of the complaint, using his or her complaint reference number.

After CBP assigns a reference number, CBP staff either assign the case to the appropriate CBP office (for example, Office of Field Operations for complaints arising at Ports of Entry) or refer the matter to the appropriate DHS component for review and resolution (for example, DHS Office of Civil Rights and Civil Liberties (CRCL) for all civil liberties complaints). If the complaint is about an agency outside of DHS, the complainant is advised to contact that agency directly. CBP continues to track all information related to the case (including additional interactions with the individual) such as requests for further information, case status updates, and conclusions and recommendations of the case review. Although CBP logs and tracks complaints and comments in CMS, the assigned CBP office remains responsible for communicating with the

individual. CMS maintains information collected directly from the responding office or agency related to the final disposition of the complaint.

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?

- Executive Order 12862,[4] "Setting Customer Service Standards" provides legal authority for information collected and stored in CMS.
- Executive Order 13571,[5] "Streamlining Service Delivery and Improving Customer Service," expands Executive Order 12862 by requiring agencies to use technology and service delivery systems to enhance customer service.
- Homeland Security Act of 2002.[6]

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

The Complaint Management System is covered by the DHS Correspondence Records System of Records.[7] The DHS Correspondence Records SORN permits the collection of records to manage incoming information and responses to inquiries, comments, or complaints outlines the collection of contact information, the complaint itself, and other related materials.

If CBP relies on additional information – such as travel or enforcement information – to research or resolve a complaint, the source system SORNs provide coverage for the records used for complaint resolution. CMS does not store the official records, or copies of records, from the source system SORNs. CMS may include pointer or reference information back to a source system, such as a TECS (not an acronym)[8] Record ID number. For example, if the complainant submits his or her Global Entry Pass ID as part of his or her complaint, CBP personnel would use that information to verify the individual's identity within the Global Enrollment System, which is covered under the Global Enrollment System.[9]

---

[4] Executive Order 12862, September 11, 1993, "Setting Customer Service Standards" (58 FR 48257), *available at,* http://www.archives.gov/federal-register/executive-orders/pdf/12862.pdf.
[5] Executive Order 13571 "Steamlining Service Delivery and Improving Customer Service (76 FR 24339), *available at,* http://www.gpo.gov/fdsys/pkg/FR-2011-05-02/pdf/2011-10732.pdf.
[6] 6 U.S.C. §§ 101 et seq.
[7] DHS/ALL-016 Department of Homeland Security Correspondence Records (November 10, 2008, 73 FR 66657).
[8] DHS/CBP-011 TECS, December 19, 2008 (73 FR 77778).
[9] DHS/CBP-002 - Global Enrollment System (January 16, 2013, 78 FR 3441).

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

No. The CMS authority to operate (ATO) is pending completion of this PIA.

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

CBP continues to work with the CBP Records Office and NARA to develop a records retention schedule of five years from the date that the complaint is closed. CBP retains these records, to include the case management information within CMS, and all information submitted by the complainant, for a period of up to five years to assist an individual who may have repeated experiences or to reduce the likelihood of repeated experiences, as well as to track historical trends.

To the extent information is used for research from other systems, CMS does not store the official records, or copies of records, within CMS. CMS may include pointer or reference information back to a source system, such as a TECS (not an acronym) Record ID number.

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.

The information collected from persons filing a complaint or comment that CMS maintains is covered by OMB Number: 1651-0136.

Section 2.0 Characterization of the Information

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

Individuals who wish to submit a complaint or comment and receive a response are required to provide sufficient personal information and event details to enable CBP to research the complaint and provide the individual with a response. Individuals who wish to remain anonymous are not required to provide any personal information; however, they also will not receive a response from CBP.

CBP uses pre-determined question paths to minimize the information collected in order to respond to an individual's specific complaint or comment. When individuals submit their complaint or comment through the website portal, they are asked to identify the nature of their complaint or comment from listed categories, such as: 1) Trusted Traveler Programs (e.g.,Global

Entry, NEXUS, SENTRI, GOES);[10] 2) Border Patrol checkpoints or other locations; 3) General aviation facility or marina; 4) Importing/exporting goods or other related international trade issues; or 5) General concerns, such as: the CBP website, the Electronic System for Travel Authorization (ESTA)[11] application, I-94[12] retrieval, service delays/responsiveness (including lost or missing parcels, general practices and procedures, etc.) The selected category is designed to collect the information required to research those types of complaints or comments. Once in the identified path, the information essential to contacting the individual and locating the record is identified with a red asterisk next to each required item. Information without a red asterisk, although helpful to finding the record and expediting the process, is considered optional. When the information is received via telephone, CBP staff are trained to guide the individual's through the same identified questions in order to address the caller's issue. For example, if a complaint involves general CBP practices and procedures, the individual will not be asked for his or her trusted traveler number because it would be irrelevant.

The information collected in CMS falls into four broad categories: (1) contact information to enable CBP to communicate with the individual or his/her designated representative; (2) information about the individual's experience to assist CBP in identifying which office is best able to address the issue; (3) additional PII and/or documentation, to verify the identity of the individual prior to sharing information; and (4) relevant information derived from appropriate programs and systems which is needed to address and resolve these complaints and comments.

1. The following information may be collected directly from the individual or his/her designated representative to enable CBP to communicate with him/her during the lifecycle of the complaint, (asterisks specify the mandatory fields):
    - Email address (required for responses to electronic submissions)*;
    - User ID and password, if complainant wishes to open an "account" with CMS to track the status of his/her case;
    - First and last name*;
    - Middle name;
    - Street address,

[10] DHS/CBP/PIA-002 Global Enrollment System (GES) (January 10, 2013), *available at* www.dhs.gov/privacy.
[11] DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA) (originally published June 2, 2008, and subsequent updates), *available at* www.dhs.gov/privacy.
[12] DHS/CBP/PIA-016 U.S. Customs and Border Protection Form I-94 Automation (February 27, 2013), *available at* www.dhs.gov/privacy.

- City, country, state/province, and postal code*;
- Phone country code number (if not in the United States); and
- Phone number*.

2. The following information may be collected directly from the individual or his/her designated representative to locate information associated with the complaint:
    - Port of entry*;
    - Incident date*;
    - Employee name/badge number;
    - Flight number; and
    - Narrative describing the complaint*.

For commercial trade complaints or comments, the following information may also be collected:

- Entry type*;
- Entry number;
- Cargo location*;
- Problem type*;
- Bill of lading number;
- Container number;
- Booking number; and
- Proprietary trade data.

3. The following optional information may be collected directly from the individual or his/her designated representative to verify the identity of the individual prior to sharing information with them:
    - Date of Birth;
    - Passport Number and Citizenship Country;
    - Passport Card Number;
    - Enhanced Driver's License (EDL) Number and State of Issuance;
    - Alien Registration Number (also known as Lawful Permanent Resident Number, and/or Green card (Permanent Residence));

- Border Crossing Card Number; or
- Trusted Traveler ID number (e.g., FAST, SENTRI, and NEXUS numbers).

4. CBP enters case notes into text fields in CMS as additional information is received during the intake, review, assignment, and resolution stages of the process. CBP staff are trained on the job to only enter PII into CMS that is relevant to the review and possible resolution of the complaint or comment. Training is accomplished through in-house training and mentoring, as well as periodic formal training provided by CBP Internal Affairs staff.

In addition, CBP collects information to verify the identity of requesting individuals and their need to know prior to releasing information. For complaints or comments received telephonically, CMS has a Voice Over Internet Protocol (VOIP) that enables the recording of date, time, and telephone numbers from which the call was made. Calls are downloaded onto external media, entered manually into CMS, and verified for accuracy. The external media are secured and then in accordance with the proposed record schedule, disposed of after five years, unless associated with an enforcement or national security event.

Although CMS covers a broad spectrum of complaints and comments, it does not collect or maintain information concerning redress issues involving traveler entry into or exit out of the United States. These types of complaints are handled by the DHS Traveler Redress Inquiry Program (DHS TRIP). As a result, if CBP determines that a complaint or comment is more appropriately addressed by DHS TRIP, CBP provides the individual with information for filing a redress inquiry with DHS TRIP and CBP closes the case within CMS.

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

There are three sources of information for the CMS system:

1. Members of the public who submit the complaint or comment through the CBP complaint management process in either written or verbal form.
2. Information derived from other Federal Government databases used to research and resolve the complaint such as those accessed through TECS[13] and the Arrival and Departure Information System (ADIS).[14] This source of information is maintained in the case management portion of CMS, either in a narrative field or scanned into CMS. Staff manually enter this type of information into CMS. The

[13] DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (August 5, 2011) and DHS/CBP-011 TECS SORN (December 19, 2008, 73 FR 77778), *available at* www.dhs.gov/privacy.
[14] DHS/CBP/PIA-024(a) Arrival and Departure Information System (ADIS) March 7, 2014, and DHS/USVISIT-001 Arrival and Departure Information System (ADIS) SORN (May 28, 2014, 78 FR 31955), *available at* www.dhs.gov/privacy.

official records themselves are not transferred or copied into CMS.

3. Individuals whose information is included in records that have been provided or referred to CBP during the complaint management process. These individuals may serve as witnesses to, collaborate, or provide additional information concerning the complaint or comment issue, or as subjects of the complaint or comment.

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

CMS does not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

All complaints submitted to CBP are submitted by the individual complainant or by a representative on behalf of the individual complainant. Therefore, because complainants submit information directly to CBP, all contact or personally identifiable information submitted is presumed to be accurate.

The actual details of the complaint may vary based on the facts of the case. CBP CMS retains the original submitted complaint, and then uses other CBP information to research and resolve the case. Due to nature of these complaints, they do not always mirror what is contained in CBP reports or records. The CBP office (Office of Field Operations, Border Patrol, etc.) to which the complaint is directed will do its own individual research, including contacting the officers or agents involved in the incident, to confirm or refute the complaint. In some instances, complaints are referred to the Office of Professional Responsibility (OPR), DHS CRCL, or Office of the Inspector General (OIG) for further research and investigation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information collected may be outdated, inaccurate, irrelevant, or incomplete.

Mitigation: Individuals provide information directly to CBP/CMS or through a representative. They must self-verify the timeliness, accuracy, and completeness of the information they provide. Additionally, individuals who submit a comment or complaint through CMS are given a control number so that they may update, correct, supplement, or even withdraw their submission at any time during the process. All information that CBP uses to verify or research complaints is from internal CBP source systems, as noted in section 2.1. If the complaint indicates an inaccuracy, CBP specialists do additional research and send the complaint for the appropriate

office for redress action (DHS TRIP, OPR, etc.). In addition, CBP gathers witness statements and reviews officer reports to corroborate or confirm complaint details.

Privacy Risk: There is a risk that individuals may provide more information than necessary to review and resolve a particular complaint or concern.

Mitigation: This risk is partially mitigated. Individuals may submit whatever information they believe is relevant to resolve their issue. When CBP staff receives complaints and comments via telephone calls, they are trained via mentoring, in-house training, and formal classes to provide guidance to individuals concerning which information is relevant and necessary to review and resolve a particular issue. However, CBP staff are unable to provide similar guidance to individuals who submit their complaints and comments via correspondence or the online portal. To reduce this risk for online submissions, CBP has streamlined the portal by associating certain questions with certain types of complaints (see section 2.1), and by marking certain fields mandatory but leaving the majority of fields as optional.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CMS addresses a broad spectrum of complaints and comments involving interactions with CBP. To address and resolve these complaints, information is collected from individuals submitting the complaint or their representatives, and appropriate programs and systems. The information is used to: 1) maintain contact with the individual submitting the complaint during the complaint process; 2) verify the identity of the individual; 3) locate and retrieve records associated with the complaint or concern; and 4) refer the issue to the correct office for adjudication/resolution. CMS maintains case notes for each complaint, recording intake information, case referrals, updates, and resolutions.

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. Only CBP headquarters and field offices/sectors have access to CMS. Information shared with other relevant DHS components or other federal offices usually is shared via telephone calls when additional information is needed to process and/or resolve a complaint or comment if more facts are needed to research the issue.

CBP may share information with the DHS U.S. Immigration and Customs Enforcement (ICE) FALCON Tipline[15] for further vetting when there appears to be a specific violation or potential violation of law or identified threat or potential threat to national or international security, such as criminal or terrorist activities, based on individual records in this system. For example, when the information provided by the individual or discovered in review of the complaint indicates some sort of violation of law or potential violation of law or identified threat or potential threat to national or international security, CBP may share the information with ICE. In lieu of contacting the CBP CMS, individuals also may report these activities directly to ICE using the Homeland Security Investigations (HSI) Tip Form located on the ICE public website.[16]

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information collected may not be necessary or directly relevant to the purpose of the complaint or comment and CBP's review and resolution of the inquiry.

Mitigation: This risk is partially mitigated. CMS covers the entire spectrum of possible complaints and comments with the exception of entry issues submitted or referred to DHS TRIP for redress. As a result, CBP cannot always anticipate the information needed to properly locate required records for a particular complaint or concern. To mitigate this risk, the website identifies what information is required and by default, which information is optional. If the information is received in person or over the phone, trained CBP staff will advise the submitter about what information is necessary for submission.

Privacy Risk: There is a risk that information collected as part of a complaint or comment may be used inappropriately or may be used for purposes beyond the intent of this document.

Mitigation: All system users are trained to use information strictly to collect comments and complaints, track case progress and final resolution, and compile statistics. CMS uses auditing to track individual record access to ensure users are not accessing information inappropriately. Additionally, CBP revokes access for any employees who query records in CMS without a need to know. Individuals with access to CMS are required to take the annual "General Privacy Awareness Course" training. Privacy training must be completed for new users before access to CMS is granted and annually for continued use by currently approved users.

[15] DHS/ICE/PIA-033 FALCON Tipline (FALCON-TL) (November 2, 2012), *available at* www.dhs.gov/privacy.
[16] https://www.ice.gov/webform/hsi-tip-form.

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.

The CBP INFO Center online portal is available on the public-facing www.cbp.gov website, along with instructions for how to submit a complaint or comment to CBP. Consistent with 5 U.S.C. § 552a(e)(3), all web intake forms requesting data contain a Privacy Act Statement. The individual seeking complaint resolution acknowledges that he or she is voluntarily submitting PII for complaint resolution purposes and that the information provided is accurate. Individuals making their submissions by letter, phone, or in-person who have privacy concerns are directed to the website to view CBP's online Privacy Act Statement. Individuals making submissions by phone are informed that the calls are recorded for quality purposes. In addition, this PIA provides public notice of the collection, use, sharing, and maintenance of this information.

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

The complaint process is voluntary, so individuals have the right to decline to provide information by either opting out of the process or by limiting the information they provide for review. However, providing less information than requested may make resolution of the issue more difficult. Individuals also have the option to register a complaint or comment anonymously; however, the lack of sufficient information may prevent the complaint or comment from being fully investigated or resolved. For example, an individual may call from a pay phone or other non-attributable phone number to remain anonymous. As a result, CBP has no way to contact the individual with follow-up questions. As a third option, individuals retain the ability to withdraw their submission(s) after the complaint or comment is entered into CMS. In these situations, the case is closed in CMS and retained in accordance with the record retention schedule.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is the risk that the individual may receive inadequate notice regarding the use of his or her information.

Mitigation: This risk is partially mitigated. CBP provides a Privacy Act Statement on the website, however CBP does not read a Privacy Act Statement over the phone or in-person at Ports of Entry or checkpoints. Providing an oral Privacy Act Statement is often impracticable in the travel and border management environment. Individuals are often in a hurry to reach their final destinations or are agitated about an encounter with CBP. CBP finds that it is better to direct individuals to a website, or provide a tear-sheet, with a Privacy Act Statement so they may take it with them. Typically complaints are filed after an individual leaves a CBP facility.

For the online portal, individuals must confirm that they have read and understood the Privacy Act Statement before submitting their information. The Privacy Act Statement reminds individuals of the opportunity to decline to provide information and that the information is provided voluntarily.[17] Individuals who submit complaints by phone are informed that the calls are recorded for quality purposes and directed to the Privacy Act Statement on the website.

Lastly, CBP has a robust amount of information on its public-facing www.cbp.gov website regarding how to file a complaint or comment, and has published this PIA to increase transparency regarding its operations.

Section 5.0 Data Retention by the project

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

CBP continues to work with the CBP Records Office and NARA to finalize the retention schedule. The proposed retention schedule is as follows: All information contained in CMS, which includes: information collected from individuals in support of their requests, the current status of those requests, and supporting information about the resolution of the request, will be retained for up to five years from the date of closure and the complaint response. This retention period enables CBP to: a) assist individuals who may have repeated experiences or 2) reduce the likelihood of repeated experiences, and 3) track historical trends.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CMS retains information longer than needed to resolve a complaint.

Mitigation: Information is retained in compliance with the established retention schedule. An approved NARA retention schedule enables CBP to provide better customer service by: 1) assisting individuals who have repeated experiences; 2) reducing the likelihood of repeated experiences; and 3) identifying historical trends for management. To mitigate the risk associated with retaining records longer than needed to process the request, the data will be protected in databases continuously certified to meet FISMA medium level security standards until disposition. CMS automatically archives cases once the retention limit has been reached.

[17] See Appendix A.

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 may disclose the information within CMS pursuant to the routine uses identified in the DHS Correspondence Records System of Records,[18] and as otherwise authorized under the Privacy Act.[19] The information collected and retained in CMS may be shared under certain circumstances with other Federal Government agencies via telephone calls or email when it is necessary to address an individual's complaint that cannot be resolved within CBP or DHS.

Other examples of when CBP may share the CMS information include but are not limited to the following circumstances:

(1) With the Department of State (DOS) when the complaint request pertains to visa issuance or a passport program;

(2) With authorized contractors or service providers who are not CBP employees but have an agency relationship with CBP to accomplish CBP responsibilities concerning complaint and comment resolution. Contractors are required to sign a non-disclosure agreement prior to being granted access to CBP systems.

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

External sharing is compatible with the purposes for which the original information is collected – to research and resolve complaints or comments. All external sharing is done pursuant to subsection (b)(3) of the Privacy Act and with the routine uses identified in the DHS Correspondence Records System of Records. External sharing purposes are compatible with the original purpose because CBP needs to refer the complaint or comment to the federal agency that has the information germane to research and resolve the complaint or comment, or to address the law enforcement response aspect in the case of potential violation of law or national security threat.

6.3 Does the project place limitations on re-dissemination?

Yes. CBP places limits on the re-dissemination of information shared with other federal agencies, including through the use of a Memorandum of Agreement (MOA) or a letter of authorization. These documents contain provisions that ensure compliance with the Privacy Act and authorize disclosure via the routine uses contained within the SORN.

[18] DHS/ALL-016 Department of Homeland Security Correspondence Records (November 10, 2008, 73 FR 66657).
[19] 5 U.S.C. 552a.

Contractors or service providers that receive or handle information to accomplish CBP responsibilities concerning complaint and comment resolution must comply with the same limitations on re-dissemination and protections as federal employees.

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

CBP tracks any sharing of records from CMS with external agencies using the Form DHS-191 Privacy Act Disclosure Record. The CBP Info Center retains copies of these forms.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that CMS information may be shared inappropriately with other Federal Government agencies.

Mitigation: CBP mitigates this risk by only sharing data with other Federal Government agencies in accordance with an established MOA or letter of authorization and as authorized by the Correspondence Records SORN. CBP transmits this information in a secure manner and the receiving agency is required to handle it in accordance with the Privacy Act and federal information security requirements.

Privacy Risk: There is a risk that CMS information may be shared inappropriately by employees, contractors, or service providers with access to CMS.

Mitigation: CBP mitigates this risk by requiring contractors and service providers (who are responsible for maintenance of the servers) to sign a non-disclosure agreement, undergo background checks, take the same privacy training as CBP employees, and comply with the same limitations on re-dissemination and protections as federal employees.

Section 7.0 Redress

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

CMS provides individuals with the option of setting up a password-protected account at the time they register a complaint through the CBP complaint portal. This account contains their initial complaint as well as the status and resolution of the complaint. Complaints received by mail or telephone are manually entered into CMS by CBP staff, and information regarding online access is provided to the individual in the response letter or phone call. Individuals who contact CBP through the mail are able to create an account in CMS and access the status of their complaint or comment by providing the control number.

If an individual wants to access records about him or herself maintained by CMS without creating an account, he/she may file a Freedom of Information Act (FOIA) request or Privacy Act

request with CBP's FOIA Division for a copy of his/her records. Individuals seeking notification of and access to any record contained in CMS, or seeking to contest its content, may gain access to certain information, subject to application exemptions, by filing a FOIA or Privacy Act request with CBP at https://foia/cbp.gov/palMain.aspx or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, D.C. 20229
Fax Number: (202) 315-0230

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

CBP receives initial information directly from individuals submitting a complaint or comment or from their designated representative. CBP instructs staff collecting information via telephone calls to confirm the information with the individual prior to entering the information into CMS. If the information is collected via the website portal, an individual is required to certify that the information is true and accurate. In addition, all complaints are provided a unique identifier (control number) that allows the individual to review his/her complaint through the website and check the complaint for accuracy and submit corrections. Individuals who open an account in CMS can update their information at any time during the process.

Individuals may also file a Privacy Act request with the CBP FOIA office for a copy of their records, subject to any applicable exemptions. Lastly, individuals may request amendment of inaccurate records that CMS has collected from them.

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

Individuals are notified about the procedures to correct their information in several ways:

- The CBP public website at www.cbp.gov;
- CBP FOIA website at http://www.cbp.gov/site-policy-notices/foia/faq-foia;
- FAQs posted on the website at https://help.cbp.gov/app/home;
- Final response letter; and
- This PIA provides notice on how to correct information pertaining to an individual.

7.4 Privacy Impact Analysis: Related to Redress

There is no privacy risk to redress. All information is submitted directly by the individuals, and they are able to update their information at any time via the online portal. CBP provides substantial notice via the public-facing website and Privacy Act Statements. If individuals are not satisfied with their ability to update their information within CMS, they may file a Privacy Act Request.

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?

CMS has an audit trail feature with the capability of tracking individual record access and modifications by user name as well as time/date stamp. CMS Information Security Systems Officer (ISSO) regularly reviews the audit system logs.

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

CBP employees and contractor personnel with access to CMS receive privacy training to ensure that they are using the information in CMS consistent with the purpose of its original collection. Privacy training is included in the formal CMS training and reinforced with on-the-job training, experience, and in-house mentoring.

In addition, individuals with access to CMS take the annual "General Privacy Awareness Course" training. Privacy training must be completed for new users before access to CMS is granted and annually for continued use by currently approved users. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting PII. Compliance with these training requirements are subject to auditing. CBP employees who also must access TECS to obtain information related to developing a response to a complaint or comment must take and pass the TECS Privacy Awareness Course on an annual basis.

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

CMS users must be designated in writing by CBP supervisors or other DHS management personnel with supervisory authority. Role-based access controls are used to control access to CMS using the Policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles. Employees or contractors are assigned roles for accessing CMS based on their job functions. The CMS administrator will grant access on a need-to-know basis and ensures compliance to policy and

manages the activation or deactivation of accounts and privileges as required or when expired. CBP ensures personnel accessing CMS have security training commensurate with their duties and responsibilities.

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?

CMS does not have any MOUs in place for access to CMS or CMS data. However, if an MOU is required as a part of the complaint management business process, the CBP Office of Public Affairs will coordinate with the CBP Privacy and Diversity Office to ensure that the MOU is developed and reviewed by the program manager, CBP Privacy Officer, and the Office of Chief Counsel.

Responsible Officials

Barbara Aliño
Program Manager
Office of Public Affairs
U.S. Customs and Border Protection
(202) 325-8000

Debra L. Danisek
Acting CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
(202) 344-1610

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

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

Appendix A: Website Privacy Act Statement

Pursuant to 5 U.S.C. § 552a(e)(3), this Privacy Act Statement serves to inform you of the following concerning the collection of the information on this form.

AUTHORITY: Executive Order 12862, September 11, 1993, "Setting Customer Service Standards" (58 FR 48257) provides the legal authority for collecting information in CMS. Executive Order 13571, April 27, 2011 "Streamlining Service Delivery and Improving Customer Service" expands upon that authority by requiring agencies to use technology and service delivery systems to enhance customer service. 6 U.S.C. §§ 101 et seq. of the Homeland Security Act of 2002 provides the legal authority for sharing information with law enforcement and national security agencies for the purpose of protecting the United States from terrorists and natural disasters, and to safeguard the overall economic security of the United States.

PURPOSE: The purpose for soliciting this information is to: (1) collect and store information voluntarily submitted by you or your representative(s) that enables CBP to review your complaints or comments concerning CBP and reach a resolution, when possible, and (2) analyze performance metrics for the customer management program and historical customer treatment trends to improve customer service.

DISCLOSURE: The information solicited on this form may be made available as a "routine use" to other Government agencies to assist the Department of Homeland Security in making determinations about your complaint or comment and for law enforcement and administration purposes. A complete list of the routine uses can be found in the system of records notice associated with this form, DHS/ALL-016 Department of Homeland Security Correspondence Records (November 10, 2008, 73 FR 66657). The Department's system of records notices can be found on the Department's website at http://www.dhs.gov/system-records-notices-sorns.

CONSEQUENCES OF FAILURE TO PROVIDE INFORMATION: The information collected from you through this form is voluntary. You may choose to submit information for all applicable fields, some fields, or not to submit information at all. However, if you provide insufficient information, it may impede CBP's ability to contact you, thoroughly review your complaint or comment, or reach a fair resolution.

What are your rights under the Privacy Act of 1974?

The Privacy Act of 1974 (5 U.S.C. 552a) protects the personal information the Federal Government keeps on United States citizens and lawful permanent residents in "systems of records" (SOR). A SOR is information an agency controls that can be retrieved by name or some other personal identifier. The Privacy Act controls how the Government can disclose, share,

provide access to, and maintain the personal information that it collects. DHS, as a matter of policy, extends the administrative rights of the Privacy Act, including the rights of access and amendment, to aliens when dealing with mixed-use systems (systems containing information about both U.S. citizens and foreign nationals). Not all information collected online is covered by the Privacy Act. The Act's major provisions require agencies to:

- Publish a System of Records Notice (SORN) in the Federal Register explaining the existence, character, and uses of a new or revised SOR;
- Keep information about citizens and lawful permanent residents accurate, relevant, timely, and complete to assure fairness in dealing with you; and
- Allow citizens and legal permanent residents to, upon request, access and review their information held in a SOR except when exempted from disclosure in the SORN for law enforcement or national security reasons.

An overview of the Privacy Act can be viewed at the following web site: http://www.justice.gov/opcl/1974privacyact-overview.htm