



Privacy Impact Assessment
for the

CBPnet

DHS/CBP/PIA-043

May 10, 2017

Contact Point

Michael D. George

Director, Border Enforcement and Management Systems Division

Office of Information Technology

U.S. Customs and Border Protection

(202) 344-1680

Reviewing Official

Jonathan 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) provides private network services to CBP users on the CBP Intranet through CBPnet. CBPnet provides a wide range of CBP information and services that are not generally available to the public through the Internet. CBPnet allows users to obtain general CBP news and information, access applications relevant to their roles and responsibilities, communicate and collaborate with other users within CBP, and access internal and external resources. In addition, CBPnet contains a limited number of applications: 1) Chief Counsel Tracking System (CCTS), 2) Quality and Uniformity Information Control System (QUICS), 3) Regulations & Rulings Tracking System (RRTS), and 4) WebTele. CBP is conducting this privacy impact assessment (PIA) because, although CBPnet itself is internal and only maintains information about CBP employees, contractors, or detailees, the CBPnet subsystems collect and maintain personally identifiable information (PII) about members of the public.

Overview

CBPnet serves as the official U.S. Customs and Border Protection (CBP) Intranet and is used exclusively by CBP employees and contractors. As the official Intranet, CBPnet provides a myriad of information and functions, such as CBP news and information, general Department of Homeland Security (DHS) business contact information, the CBP telephone directory, applications relevant to user roles and responsibilities, communication and collaboration tools, and internal and external resources. Additionally, users can access video and audio files, photo galleries, and official internal CBP forms, policies, and guidance to support operational activities. Authorized users with an official need to know can access trade regulations and rulings and legal cases impacting CBP and DHS.

The CBPnet homepage is organized by divisions and program offices (*e.g.*, Border Patrol, Air and Marine) with links that address relevant topics such as employee services, training, and technology support. Depending on the webpage, some subsystems and websites are available to all CBP users, while others are restricted to those users with a business need to know.

CBPnet provides many benefits to CBP, including:

- **Workforce Flexibility:** CBPnet provides flexibility in the workplace by allowing users to locate and view information from any CBP workstation connected to the network.
- **Increased Security:** Given that access to CBPnet is limited to authorized CBP users, intrusion security risks are greatly reduced.
- **Convenience:** CBPnet provides convenient links to the more commonly used webpages.



- **Time:** CBPnet distributes information to CBP users on a timely and as-needed basis, including up-to-the-minute alerts, when necessary.
- **Communication:** CBPnet allows users to keep up-to-date with the latest and most accurate CBP information.
- **Information Access:** CBPnet provides component-wide access to CBP organizational knowledge through employee manuals, benefits documents, component policies, business standards, news feeds, and even training. Because webpages and documents can be updated online, the most recent version is usually available to CBPnet users.
- **Cost-effective:** CBP users can view and bookmark information on CBPnet rather than maintaining physical documents such as procedure manuals, internal phone lists, and requisition forms.
- **Enhance collaboration:** Information is easily accessible by all authorized CBP users, which encourages collaboration and teamwork.
- **Promote common CBP culture:** Every CBP user views the same information within the Intranet, thus sharing a common knowledge base.

CBPnet Subsystems

The vast majority of information on CBPnet remains available to all CBPnet users. However, a limited number of applications or websites, called subsystems, restrict access in part or in total to those users with an official need to know. These applications also collect and maintain information about members of the public. As a result, the remaining portion of this privacy impact assessment (PIA) will focus primarily on these CBPnet subsystems:

- 1) Chief Counsel Tracking System (CCTS);
- 2) Quality and Uniformity Information Control System (QUICS);
- 3) Regulations & Rulings Tracking System (RRTS); and
- 4) WebTele.

These are standalone systems with databases that reside on CBPnet servers, thus making them a part of the CBPnet system infrastructure. While WebTele and QUICS are accessible to (and searchable by) all CBP users, CCTS and RRTS are restricted and require special permissions for access capabilities.

1. Chief Counsel Tracking System (CCTS)

CCTS provides web-based case management and repository capabilities to the CBP Office of Chief Counsel (OCC). OCC serves as CBP's in-house legal counsel and provides legal advice, review, and representation to CBP officials on a broad range of legal matters affecting the agency.



CBP legal matters, also known as cases, cover all areas of the practice of law, including: labor, employment, enforcement, operations, contracts, procurement, appropriations and fiscal, immigration, customs, ethics, real property, environmental, and agriculture. OCC represents CBP in offensive and defensive litigation in all federal courts, as well as in all third-party administrative hearings. OCC ensures compliance of proposed agency actions and policies with legal requirements, trains CBP officials in a myriad of law enforcement, trade, and ethics matters both at the academies and post-academy, and prepares and reviews legislative and regulatory proposals. CCTS provides the necessary tools to document case data information. OCC utilizes CCTS to: 1) document case progression, and 2) generate workload and performance statistical reports and queries in a real-time, online, enterprise-wide environment. CCTS is a permissions-based system, and is accessible only by OCC employees with a need to know. For example, OCC attorneys may be granted standard access, which allows the attorney to document information in CCTS cases to which the attorney is assigned. OCC supervisory attorneys are granted the level of access that allows the supervisory attorney to document information in CCTS cases to which the supervisory attorney is assigned and to those cases assigned to attorneys who report to the supervisory attorney. CCTS can mark cases as “confidential” or “sensitive,” further limiting the individuals who can view a case and its attachments. As of the end of 2016, OCC employed approximately 350 attorneys and business management staff in 30 offices nationwide. CCTS serves as the legal case management system for OCC personnel in performance of their legal and ethics duties on behalf of the agency.

CCTS does not connect to any other systems except for interfacing with WebTele to validate CCTS user information (*e.g.*, government email address and government phone number), and the CCTS data fields are completed manually by OCC personnel with the necessary permissions. The CCTS data fields that capture personally identifiable information (PII) include: the assigned OCC attorney and judge name if applicable to the case. In addition, names of plaintiffs, claimants, and defendants may be included in some CCTS cases, extracted from legal records associated with the case, including for example pleadings filed by a plaintiff, and in documentation submitted by claimants in support of their claim under the Federal Tort Claims Act¹ or other claim against the government.

In addition to the manual data fields, documents may be uploaded to the case in CCTS that may contain additional PII such as: names, dates of birth, Social Security numbers (in limited situations), Alien Registration Numbers (A-Number), mailing addresses, email addresses, phone numbers, other relevant contact information, attorney contact information, personnel information, security clearance information, relevant medical information, pictures, videos, intellectual property data, agency or Department investigative reports (in limited instances), and other relevant data associated with a given case. The content of documents attached to a case record is not

¹ 28 U.S.C. §§ 2671-2680.



keyword-searchable and is accessible only to OCC employees with permissions to access the case. Documents uploaded to case records can be created by OCC or provided to OCC by the client. A significant amount of information contained within CCTS is covered by various privileges, including, but not limited to, attorney-client privilege, attorney work-product privilege, law enforcement privilege, and the deliberative process privilege, given the role of OCC in advising agency decision-makers and in handling litigation.

2. *Quality and Uniformity Information Control System (QUICS)*

QUICS is an online inquiry/response system that assists the CBP Office of Trade (OT) National Commodity Specialist Division (NCSO) in making uniform trade decisions on merchandise classification, value, country of origin, marking requirements, and other product-specific issues, as well as the application of tariff laws. QUICS consists of the following two functions: 1) Query and Response, and 2) Search.

The QUICS “Query and Response” function is capable of sending and responding to inquiries, and disseminating product-related alerts. The system allows authorized officers/inspectors to send inquiries to the National Import Specialists within the NCSO, Office of Trade, Regulations and Rulings (OTRR). These messages can include uploaded product documentation and images, thus reducing the need to email samples for review. The only PII permissible in these attachments, images, or messages is contact name and information (*i.e.*, email address, phone number, and work address) for respective importers and manufacturers of goods. Data is not retrievable by personal identifier. QUICS also enables OTRR offices to initiate “OTRR Alerts” on specific issues of interest to CBP field offices. QUICS permanently records these alerts and makes them easily available for search by all interested CBP officers and inspectors and general agency personnel. The “Query and Response” function is only available to authorized users.

The QUICS “Search” function is available to anyone in CBP who has access to the Intranet; no password is required. This tool enables keyword searches of all QUICS fields, or selected fields by filtering on “Message Type,” “Field,” or a specific “Subject.” The search tool does not search any upload, attachment, or image.

3. *Regulations & Rulings Tracking System (RRTS)*

RRTS is a web-based case-management system that supports OTRR. The system tracks trade-related workload and case activity by assigned attorney name and automatically-generated attorney number. Attorney information consists of the assigned attorney’s name, attorney number, and branch information. Case information is limited to the name of the trade client, protest number, if applicable, and a brief description of the issue. This information is used primarily for tracking purposes related to attorney caseload, and for general tracking of cases for the office. The reports



generated from RRTS reflect attorney activity with regard to case lifecycle management. Similar to CCTS, RRTS is a permission-based system limited to OTRR staff with a need to know.

A legacy component within RRTS had been used to manually track check payments related to property rights recordations. This component was used to capture the following financial data: payor name, bank account number, bank routing number, check amount, and date. This function has since been transferred to the CBP Intellectual Property Rights e-Recordation and Search Systems (IPRRSS),² and OTRR has discontinued the use of this functionality in RRTS.

4. *WebTele*

WebTele is the CBP telephone directory used by employees to obtain phone numbers and email addresses of other CBP employees. It is also used by supervisors to: 1) reach employees at home in the aftermath of large-scale disasters, 2) offer assistance to employees and family members, and 3) reach employees' contact persons in the event of personal emergencies. The employee data captured in the system includes employee name, work and home addresses, work and home telephone numbers (mobile numbers, if appropriate), government email address, CBP organization, supervisor's name, CBP employee status, and emergency contact information. CBP employees are required to complete all mandatory fields in both the "Public" tab (fields accessible to all authorized CBPnet users), and the "Personal" tab (fields accessible by the employee's direct chain of command). HASH ID³ and mainframe password are required to log in to the site. This tool is a web-based interface of the legacy mainframe application "TELE."

In addition, WebTele is the primary interface system used by the CBP Emergency Notification System (ENS), which serves as the official means of emergency alert notifications to personnel in the event of an emergency or national crisis. ENS is used by CBP management to maintain the safety and accountability of staff during emergency events. ENS alerts use multiple notification methods such as desktop pop-ups and phone, email, and text messages. The contact information is imported from WebTele into ENS for notification purposes. Data may be retrieved by an individual's first or last name.

² See DHS/CBP/PIA-011 Intellectual Property Rights e-Recordation and Search Systems (December 11, 2012), available at www.dhs.gov/privacy.

³ The HASH ID is an internal identification number created using an algorithm and is based on the employee's Social Security number.



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?

The following legal authorities permit the collection of information within *RRTS* and *CCTS*: 5 U.S.C. § 301; the Federal Records Act, 44 U.S.C. § 3101; the Homeland Security Act of 2002, Public Law 107-296; and the Aviation and Transportation Security Act, Public Law 107-71.

The collection of information from the public for trade-related cases is authorized by 49 CFR parts 176 and 177.

The data collection and upkeep of the data in *WebTele* are mandated by the following two directives: CBP Directive No. 51332-016A, Residency Requirement for U.S. Customs and Border Protection (CBP) Employees, and CBP Directive No. 5290-020, U.S. Customs and Border Protection (CBP) Emergency Notification System (CBP-ENS). The latter directive applies to CBP personnel, as well as to anyone working in an official capacity for the agency, such as contractors and temporary employees.

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

To permit the collection of various types of records, CBPnet relies on the following SORNs:

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System⁴ provides coverage for general lists and contact information in *WebTele*.
- DHS/ALL-004 General Information Technology Access Account Records System of Records (GITAARS)⁵ provides coverage for collection of data in order to create and maintain user profiles in the various systems.
- DHS/ALL-008 Accounts Receivable System of Records⁶ provides coverage for the legacy manual payment tracking related to property rights management in *RRTS*.
- DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records System of Records⁷ provides coverage for emergency contact information in *WebTele*.

⁴ See DHS/ALL-002 DHS Mailing and Other Lists, 73 FR 71659 (November 25, 2008).

⁵ See DHS/ALL-004 General Information Technology Access Account Records System of Records (GITAARS), 77 FR 228 (November 27, 2002).

⁶ See DHS/ALL-008 Accounts Receivable System of Records, 80 FR 58289 (September 28, 2015).

⁷ See DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records, 73 FR 61888 (October 17, 2008).



- DHS/ALL-017 Department of Homeland Security General Legal Records⁸ provides coverage for the legal records contained in *CCTS*.
- DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records⁹ provides coverage for employee (including contractors and detailed federal employees) work and personal data in *WebTele*.
- DHS/CBP-001 Import Information System¹⁰ allows CBP to collect and maintain importer/manufacture information and to assist in targeting illicit goods.

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

A system security plan was completed for CBPnet in November 2016. The Authority to Operate (ATO) expired on February 12, 2015, and is pending reauthorization following publication of this PIA.

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

CBP Records Management is in the process of scheduling these systems for records purposes. They will work with the respective program offices to establish appropriate schedules.

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 major subsystems residing on CBPnet do not collect data directly from members of the public, and therefore are not subject to the Paperwork Reduction Act (PRA). In addition, any application residing on CBPnet is only accessible by CBP employees and contractors and cannot be used as a vehicle to collect information from members of the public; therefore, it is not subject to the PRA.

⁸ See DHS/ALL-017 Department of Homeland Security General Legal Records, 76 FR 72428 (November 23, 2011).

⁹ See DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records, 80 FR 58283 (September 28, 2015).

¹⁰ See DHS/CBP-001 Import Information System, 81 FR 48826 (July 26, 2016).



Section 2.0 Characterization of the Information

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

CBPnet collects, uses, disseminates, and/or maintains the following information in these four major subsystems:

CCTS

CBP Employees:

Attorney name and automatically-generated attorney number.

Members of the Public:

In addition to the name of the judge, information may be captured from within the text of relevant documents (*i.e.*, pleadings and claim forms filed by plaintiffs/claimants with the court or the agency) uploaded to the case file. This information includes notes/comments pertaining to the case, names, dates of birth, Social Security numbers (in limited situations), alien registration numbers, mailing addresses, email addresses, phone numbers, other contact information, attorney contact information, witness contact information, agency or Department investigative reports (in limited instances), personnel information, security clearance information, relevant medical information, pictures, videos, intellectual property data, and any other relevant data associated with a given case. The content of documents attached to a case record are not keyword-searchable and are accessible only to OCC employees with permissions to access the case.

QUICS

Members of the Public:

Importer/manufacture contact name and information (*i.e.*, email address, phone number, work address).

Shipping Information and Related Correspondence:

Shipping information/correspondence may include: message, subject, specific issue, entry number, initiating office/port, primary and secondary Harmonized Tariff Schedule (HTS) numbers entered by the field personnel, as well as OTRR unit price, quantity, currency, total value, country of origin, manufacturer name, consignee name, carrier name, description, field officer and OTRR remarks, rulings, and QUICS number.

RRTS

CBP Employees:

Attorney name and automatically-generated attorney number.



Non-PII Information:

The data entered into RRTS includes fields such as: incoming reference, port, protest number, and docket number. While there is a free text field for issue/keyword description, the process dictates that attorneys exclude PII input to the extent possible. That said, there may be occasions in which attorneys deem it necessary to include contact or other information that may contain PII.

Members of the Public:

Tracking/documentation of property rights-related financial payments including payor name, bank account number, bank routing number, check amount, and date. As noted earlier, as this functionality is now officially tracked and accounted for in IPRRSS, these fields are no longer populated and data will be archived in the near future.

WebTele

CBP Employees and Contractors:

Name (first, middle, last, alternate first name), home address (street, city, state, zip code, country), home phone number, government employment status, active status, title, government email, work phone, location (name, room number, room or cube number, street, city, state, zip code, country), organization (name, code), manager name (first, last, middle initial), mobile phone number, radio call sign, secure telephone (STU-III) number, alternate fax number, secure fax number, TECS email site code, TECS email, and building number.

Members of the Public:

For emergency contact information: name, relationship, and phone number (primary and alternate contacts).

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

CCTS receives information from agency documentation, case pleadings and documents, and email. The agency documentation can potentially be provided by any office or third-party as relevant to the case. These records are sent to OCC at various stages in the decision-making or litigation process, and are utilized by OCC in resolving the matter at issue in the record. All cases are assigned to in-house OCC attorneys and cases/records are created in *CCTS* for case tracking, workflow, and work management purposes. OCC attorneys may upload source documents on a case-by-case basis. This data is needed to handle and/or litigate the various matters given to OCC.

QUICS is an online search tool, intended to support field inspectors and officers regarding product classifications and markings. Any documents that are uploaded directly by CBP personnel



pertain to the products in question and are obtained from trade and shipping manifests submitted to CBP.

RRTS receives information from inquiries received from CBP personnel and trade partners. While complete information is included in these files specifically related to importers and any individuals involved in product rulings or protests, the system only captures minimal information needed to track attorney output and workload.

WebTele receives information directly from employees, contractors, and detailed federal employees. These CBPnet users have the ability to view and update their information as needed. The emergency contact information is provided by agency personnel as required for emergency notification and contact purposes.

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

There is no direct link from the subsections in CBPnet to any public or commercial sources of data. However, much of the data in *QUICS* and *RRTS* also reside on public platforms given the data relates to litigation or trade/shipping matters.

For example, the LexisNexis database will contain information from *RRTS* if it was published in the Customs Rulings Online Search System (CROSS) database, which is a sortable index containing CBP legal rulings available on CBP.gov. No PII is maintained or made available through CROSS.

2.4 Discuss how accuracy of the data is ensured.

CCTS grants various user roles and permissions to review and update information in cases. Attorney supervisors have the ability to review all case information and deadlines, assess the quality of case information, and oversee their respective team case load. Supervisory attorneys have the ability to resolve any inaccuracies that are identified.

QUICS data is provided through trade and shipping manifests originally provided by importers and manufactures, and used for product classification and marking purposes. After receiving the data from the trade and shipping manifests, CBP personnel then upload into *QUICS*.

RRTS has various levels of user roles and permissions in the system such as data entry staff, attorney, branch chief/manager, and director. At each level, the accuracy of information in each case can be viewed and revised as needed. At a minimum, the attorney working on a case record created by data entry staff will update details as appropriate. The staff attorneys can only add their labor time, which indicates where they are on each case (for example, drafting a decision).



In addition, property rights payment information is sourced directly from manual checks mailed to CBP, so data errors are minimized or nonexistent.

WebTele allows CBPnet users, employees, contractors, detailed federal employees, and their respective CBP supervisors to enter, update, and correct their own information. As a result, information from these data sources is considered highly accurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of data inaccuracy due to manual data entry for many of the CBPnet source systems.

Mitigation: This risk is mitigated since each subsystem compensates for inaccurate data input by adopting its own method of checks and balances to remedy any inaccuracies/discrepancies in its system.

Both *CCTS* and *RRTS* generate data from relevant legal documents/pleadings and information pertaining directly to an individual case. The respective user groups assign attorney supervisors and other senior attorneys appropriate permissions to assess and rectify any inaccuracies with data. The data that is manually entered into *CCTS* contains minimal contact information PII. The payment information captured in *RRTS* is sourced directly from checks mailed in to CBP, thus minimizing data inaccuracies/discrepancies.

In *QUICS*, information is obtained from trade and shipping manifests along with published tariff schedule numbers. This information can be scanned and uploaded, thus minimizing data errors.

WebTele collects information directly from employees, contractors, detailed federal employees, and their respective CBP supervisors and, if updates are needed, each user is required by policy to correct/update his or her own information or that of their subordinates. All users are required periodically to check and verify that their information is up-to-date and accurate.

Privacy Risk: Specific subsystems within CBPnet may collect more information than is needed to meet business needs.

Mitigation: The four subsystems limit the collection of information in several different ways.

CCTS limits collected information to content provided in source documents and directly related to a specific case or matter. Manually input data fields for litigation are limited, and many fields are completed by choosing among pre-populated drop down menus to ensure consistency. Although uploaded attachments to cases may contain personal information, these documents are uploaded as needed and the contents are not searchable within *CCTS*.



QUICS only collects information specific to questions on product classifications, markings, and trade rulings as appropriate. The tool pulls information from industry sources, such as tariff schedules, as needed to adequately respond to queries. The only public PII is the business contact information for manufacturers/importers.

RRTS focuses on attorney workloads and case tracking. As a result, *RRTS* collects minimal information on actual cases. The individual information in the system is limited to the attorneys assigned to particular cases. The over-collection of financial information originally collected and stored in the legacy component will be disabled as it is now collected through a different source.

WebTele limits information collection to the contact information and location of CBP employees, contractors, detailees, and emergency contacts. *WebTele* serves as the component telephone directory, and the information is needed for operational communication and location during crises and natural disasters. Minimal emergency contact information is required for all CBP users to address any potential emergency/crisis situations.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBPnet provides universal access to all CBP employees, contractors, and detailees. Through CBPnet authorized users can access a myriad of information and functions such as CBP news, events, and resources; general DHS business contact information and the CBP telephone directory; and trade regulations and rulings. A limited number of users, all within OCC, may access CCTS and information on legal cases impacting CBP. Depending on site content, some subsystems and sites are available to all CBP users, while others are restricted to those users with a need to know.

In *CCTS* and *RRTS*, authorized users access these systems to track, manage, and resolve various legal, ethics, and trade-related cases, as well as determine caseload metrics. The manual tracking of property rights payments is a legacy functionality in *RRTS* that will be disabled and archived in the future.

In *QUICS*, there is guidance provided to field inspectors and officers regarding product classifications and markings to ensure that CBP officers and inspectors make uniform trade decisions. This information, along with trade ruling updates, is vital to supporting the field and protecting trade between the United States and other nations. The information is only available to agency personnel and not external facing to the public.

In *WebTele*, users can access contact information of their colleagues for operational and emergency purposes. This information can be used for routine communication between staff, as well as contacting personnel or their families during crisis situations. Access to emergency contact information is limited to the individual's direct chain of command.



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 technology is used to conduct searches or queries to discover predictive patterns or anomalies.

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

No, CBPnet is internal facing, so access to CBPnet is limited to CBP users consisting of CBP employees, contractors, and individuals detailed to CBP. However, not all CBP users can access each subsystem as each user must be authorized to access based on need to know.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information within CBPnet may be used for a purpose that is inconsistent with the original purpose of collection.

Mitigation: CBPnet is the agency's intranet website and is only available to agency personnel and detailed federal employees at the agency. The risk is partially mitigated as each of the subsystems maintains restricted access to that system, and is for internal use only. The only data available to all agency personnel is the employee directory in WebTele and searches conducted in QUICS. CCTS and RRTS are case management tools and only accessible to authorized CBP users.

In *CCTS*, OCC users access the system to document, manage, and resolve various legal cases and ethics matters, as well as determine caseload metrics. The data collected in CCTS comes from documentation and information directly related to the respective CCTS cases. Any documentation from legal filings uploaded into the system are to support case management and ultimate resolution. The information uploaded into CCTS is based on business purpose.

For *QUICS*, the information captured relates to product markings and classifications. Any PII would typically include contact information for trade and likely be found in attachments, which are not searchable. The communication between field and headquarters staff involve the use of industry documentation, such as tariff schedules, needed to resolve queries. Upon resolution, these queries become searchable by CBP staff who may have a need to know of the outcomes and decisions related to importation of goods. In addition, registered users are trained and required to abide by and agree to follow the instructions outlined in the QUICS Access Guide.



With respect to **RRTS**, the information regarding attorneys consists of hours spent on case-related activities. The information is primarily for supervisors and other leadership to track performance and work related to specific cases.

Finally, in **WebTele**, only the “Public” and “Official” tabs are available to all personnel. These tabs primarily serve as the CBP directory for communication purposes and include name, work details, and contact information. Home address and phone number, as well as emergency contact details, are contained in the “Personal” tab, which is only available to restricted individuals with a need to know (*e.g.*, needing to locate personnel during emergency situations, the employee’s supervisor).

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.

Given that CBPnet is an internal website only accessible by CBP users, information is not collected directly from members of the public. Therefore if public notice is required, it becomes the responsibility of the collection source.

In **CCTS**, data documented in a particular case is generated from the documentation and information provided by the parties in litigation or during the administrative matter, and directly relates to the CCTS case. CCTS is not the point of collection for this information, but ingests information from sources such as court filings and internal complaints and lawsuits.

With respect to **RRTS**, importers and others in the trade industry are aware that their information, which is likely not in RRTS, is subject to the Freedom of Information Act (FOIA). If they request confidentiality of specific information, they are made aware that if their information is requested through FOIA, they will be given notice of such.

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

In **CCTS**, data documented in a particular case is generated from the documentation and information provided by the parties in litigation, or during the administrative matter and directly relates to specific CCTS cases.

Per the discussion above, importers and others in trade are aware that their information is subject to FOIA, so they will be notified if their information is ever requested per that process.

Given that CBPnet is not the point of collection for **CCTS**, **QUICS**, and **RRTS**, members of the public are unable to consent to the use of their information or decline or opt out of the use



of their information. The responsibility to inform individuals of the further dissemination of their information lies with the original collection source.

By policy, CBP users are required to maintain updated and accurate information in *WebTele*. Although CBP users can opt to decline to provide the required information, non-compliance to the policy could result in disciplinary actions.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals are unable to consent to the use of their information, decline to provide their information, or opt out of providing their information.

Mitigation: Since CBPnet is not the collection origin for *CCTS*, *QUICS*, and *RRTS* information, this risk cannot be mitigated within CBPnet. The responsibility for mitigation lies with the source of the collection.

However, this PIA provides notice that the subsystems within CBPnet contain the previously discussed data.

Section 5.0 Data Retention by the project

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

The CBP Records Management Program is in the process of establishing record retention schedules for CBPnet and its subsystems. Existing records will be retained until schedules are finalized.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data in the various subsystems is maintained longer than needed for business purposes.

Mitigation: CBP Records Management is in the process of working with the respective program offices to establish appropriate records schedules for these systems. Until a record retention schedule is finalized, all data is retained indefinitely.

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.

Information and metrics generated directly from *CCTS* are not shared outside of the Department. OCC personnel provide litigation support to the Department of Justice (DOJ) in various court proceedings, and OCC may provide information to DOJ to defend the agency. The



litigation support provided is not generated from CCTS, but from other agency documents.

OTRR shares information with DOJ for litigation purposes, but the information is derived directly from the file upon which the record in *RRTS* is based.

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

No information derived from any of the CBPnet subsystems is shared outside of the Department.

6.3 Does the project place limitations on re-dissemination?

No information derived from any of the CBPnet subsystems is shared outside of the Department.

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

No information derived from any of the CBPnet subsystems is shared outside of the Department.

6.5 Privacy Impact Analysis: Related to Information Sharing

No information derived from any of the CBPnet subsystems is shared outside of the Department.

Section 7.0 Redress

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

Individuals seeking notification of and access to any CBP records contained in CBPnet, or seeking corrections, pursuant to procedures provided by the Freedom of Information Act (FOIA) and the access provisions of the Privacy Act of 1974, with CBP can do so by visiting <https://www.cbp.gov/site-policy-notices/foia>, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue, NW, Room 3.3D
Washington, D.C. 20229

When seeking records about one's self from this system of records or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal



regulations regarding Domestic Security and Disclosure of Records and Information.¹¹ One must first verify his or her identity, meaning that one must provide his or her full name, current address, and date and place of birth. One must sign the request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury,¹² a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an individual's inquiry requires no specific form, he or she may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <https://www.dhs.gov/freedom-information-act-foia>. In addition, the request should:

- Explain why the individual believes the Department would have information on him or her;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when he or she believes the records would have been created; and
- Provide any other information that will help FOIA staff determine which DHS component agency may have responsive records.

CCTS stored attorney case files are covered by attorney-client, attorney work-product, law enforcement, deliberative process privilege, and/or other privileges. The documents collected in CCTS are typically obtained from legal documents filed by CBP employees and contractors and members of the public and their attorneys.

QUICS is primarily a messaging tool for communication between National Import Specialists and the Field Import Specialists to determine product classifications and markings. There is minimal information on importers; the information that is contained in QUICS is comprised of importer names and contact information. Data on importers is typically derived from information (*e.g.*, forms) submitted by the importers in order to engage in the trade of goods and services.

RRTS is a case management tool that tracks the work product of individual attorneys in the Office of Trade. As these attorneys have access to the CBP Intranet, they are able to access and amend their information as needed. The practice of tracking payment data related to property rights has ceased, and no new payment data is being collected in this system.

WebTele users have direct access to the CBP Intranet and therefore can access and update their own records at any time. The information collected on members of the public stored in this system is emergency contact information provided by CBP personnel. Agency directives require

¹¹ 6 CFR part 5.

¹² 28 U.S.C. § 1746.



maintenance and update of this information for all personnel (employee, contractor, and detailed federal staff).

While members of the public can request access to or amendment of any records about themselves in these systems, their requests will be considered on a case-by-case basis given attorney-client privilege and other exemptions.

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

Individuals may correct inaccurate or erroneous information in CBPnet by following the procedures described in Section 7.1.

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

CCTS, *QUICS*, and *RRTS* contain minimal individual information sourced from court pleadings and other publicly available documents, or within agency documentation derived from another system of records and related PIAs. The information is collected for case management and handling purposes, trade disputes, and other product specific issues. Any updates to information would be done during the legal or appeals process.

WebTele users have direct access to update their own records. Supervisors encourage and ensure their personnel update contact and other personal information as needed.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of their redress options during trade disputes nor are they aware that their information is stored in these systems.

Mitigation: *QUICS* and *RRTS* collect minimal information about individuals through publicly available documents and public forums like rulings, court pleadings, trade documents, and emails. CBP uses this information to resolve trade disputes and product issues. The individuals, through their attorneys or other personal representatives, have opportunities to access and revise any information about themselves during the dispute process.

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?

CBPnet is available to all CBP users at login. However, the subsystems restrict access by assigning user roles based upon the official need to know. *CCTS* and *RRTS* are primarily case management systems used solely by OCC and OTRR users, respectively. Each of these systems



assign user roles or permissions to restrict access to those with a need to know. For example, the users who are able to create cases in RRTS have different role access than the assigned attorneys, who actually work the cases. Supervisory attorneys who oversee the quality of work performed in CCTS are able to access all the cases assigned to attorneys, who are their subordinates.

QUICS, too, has roles and permissions. For example, some *QUICS* users can access/view existing product-related guidance and rulings, while other users have roles that allow them to, for example, create questions or respond to issues.

All CBP personnel have access to *WebTele* and are required by CBP policy and reminded by supervisors to keep their contact information updated in accordance with directives. Several times a year, CBP users are required to verify their contact information in WebTele is up-to-date and accurate. In addition, supervisors can update information for all of their subordinates in WebTele, if needed.

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

All CBP users are required to take several mandatory courses that address protecting PII, system security, and online rules of behavior. Specific mandatory online training includes:

- CBP IT Security Awareness and Rules of Behavior Training, and
- Privacy at DHS: Protecting Personal Information.

In addition, CBP users with access to additional systems or applications may be required to take additional training courses.

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

User access to information is usually determined by the existing organizational reporting structure and an official need to know. In *CCTS* and *RRTS*, access is restricted to those individuals with an official need to use the system in performance of their job. In both *CCTS* and *RRTS*, there are multiple roles/permissions depending on job function. A user can only view/update/print information that he or she is allowed to handle per his or her profile. An attorney using *RRTS* does not have the same screens as a data entry specialist for the tool or attorneys assigned to other cases.

In *QUICS*, there are specific roles that allow individuals to be able to, for example, post questions or respond to inquiries. These roles are typically delegated to field officers and import specialists who provide guidance and rulings related to product classifications and markings. All CBP Intranet users can access the posted guidance and rulings related to products.



In *WebTele*, supervisors have the need to create the employee/contractor records during the onboarding process, and then, CBP users become responsible for maintenance of their own information. User roles ensure that users can only view/modify their own records. In addition, supervisors also can view/modify the records of their subordinates.

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?

Information contained on CBPnet is not shared outside of CBP. Given that CBPnet serves as the CBP Intranet, no other DHS components nor users outside DHS have access to CBPnet, with the exception of individuals detailed to CBP and registered in WebTele.

Responsible Officials

Michael D. George, Director
Border Enforcement and Management Systems (BEMS)
Division Office of Information Technology
U.S. Customs and Border Protection

Debra L. Danisek, CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

Original, sign copy on file at the DHS Privacy Office.

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