Alcohol and Tobacco Tax and Trade Bureau

Chief Council Management System (CCMS)

Privacy Impact Assessment

Information Collected and Purpose

The Chief Counsel Management System is the Office of Chief Counsel's case management system which tracks legal case files, tracks legal advice provided to TTB client offices, and assures that uniform and accurate legal advice is delivered to all TTB clients.

CCMS only stores Personally Identifiable Information (PII) contact information that is relevant to case files. For individuals with direct access to CCMS, TTB also collects necessary PII to authenticate users and restrict permissions. CCMS associates these individuals with user-created user IDs and passwords.

Information Use and Sharing

CCMS stores names and phone numbers of those individuals who have provided that information for the case file. Staff attorneys nationwide can query case information in CCMS to determine if similar matters have been previously handled by a Counsel office, thus assuring uniformity and consistency of legal advice provided to TTB clients. However, case data related to adverse personnel actions handled by the Counsel eventually can be viewed and edited only by certain attorneys assigned to the Litigation, Disclosure, and Field Operations Divisions.

In some cases, TTB may need to share some case file information in CCMS within other departments of TTB. However, TTB does not share PII from CCMS outside of the federal government. TTB will also provide the minimum information necessary in these data transfers and regulate user access according to job function and business need. TTB evaluates each request on an individual basis and oversees the process to ensure all procedures are followed pursuant to the Privacy Act of 1974.

Information Consent

For an individual's PII to be in CCMS, he or she must have previously provided their contact information when the case file was opened.

Information Protection

TTB will take appropriate security measures to safeguard PII and other sensitive data stored in CCMS. TTB will apply Department of the Treasury security standards, including but not limited to routine scans and monitoring, back-up activities, and background security checks of all TTB employees and contractors.

In addition, access to CCMS PII will be limited according to job function. TTB will control access privileges according to least privilege.

The following access safeguards will also be implemented:

- Passwords expire after a set period
- Accounts are locked after a set period of inactivity
- Minimum length of passwords is eight characters
- Passwords must be a combination of letters and numbers and symbols
- Accounts are locked after a set number of incorrect attempts