Alcohol and Tobacco Tax and Trade Bureau

TTBDocs

Privacy Impact Assessment

Information Collected and Purpose

TTBDocs is a document management system based on COTS software from ZyLabs. In its initial release, TTBDocs will servce the Office of Chief Counsel (OCC) and the Office of the Chief Information Officer (OCIO). The OCC uses the system to store, archive and retrieve legal memoranda, advisory opinions, regulatory and administrative rulings, and other precedential material. The OCIO uses the system to store and retrieve filings of Form 7200.1, which are used for Information Systems Access. TTBDocs only stores Personally Identifiable Information (PII) in the form of contact information that has been included as a part of legal memoranda, advisory opinions, and 7200.1 forms.

For individuals with direct access to TTBDocs, TTB also collects necessary PII to authenticate users and restrict permissions. TTBDocs associates these individuals with user-created user IDs and passwords.

Information Use and Sharing

As an archival document program, TTBDocs stores contact information which includes names and phone numbers. Designated and approved TTB employees have direct access to TTB data, however all individuals receive different rights in TTBDocs according to their job roles and needs. Additionally, all users with access to TTBDocs are required to enter a username and password in order to access the system.

Information Consent

For an individual’s PII to be in TTBDocs, he or she must have willingly and intentionally provided their contact information.

Information Protection

TTB will take appropriate security measures to safeguard PII and other sensitive data stored in TTBDocs. 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 TTBDocs 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