Alcohol and Tobacco Tax and Trade Bureau

Caliber

Privacy Impact Assessment

Information Collected and Purpose

CaliberRM is a requirements management tool used by the Office of the Chief Information Officer personnel to manage requirements for custom application development and maintenance. Caliber supports requirements definition, organization, tracking, traceability, reporting, and requirements document generation. Caliber only stores Personally Identifiable Information (PII) in the form of contact information that has been intentionally provided by users.

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

Information Use and Sharing

In order to facilitate collaboration, impact analysis, and communication when developing custom applications, Caliber stores contact information which includes their names, phone numbers, and email addresses. Designated and approved TTB employees have direct access to Caliber data, however all individuals receive different rights in Caliber according to their job roles and needs. Additionally, all users with access to Caliber are required to enter a username and password in order to access the system.

Information Consent

For an individual's PII to be in Caliber, 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 Caliber. 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 Caliber 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