Alcohol and Tobacco Tax and Trade Bureau

Certificate of Label Approval Formula Modernization Laboratory (CFM Lab)

Privacy Impact Assessment

Information Collected and Purpose

CFM Lab is the Bureau of Alcohol, Tobacco and Firearms official registry of issued or canceled Certificate of Label Approvals (COLAs). CFM is also the accurate registry of rejected or withdrawn alcohol beverage Label/Bottle/Formula applications. Additionally, it is the primary tool used by the Alcohol Labeling and Formulation Division (ALFD) personnel in tracking key information associated with label and formula applications and other alcohol related work items (correspondence, special projects, etc.). CFM only stores Personally Identifiable Information (PII) contact information that is included with submitted applications. For individuals with direct access to CFM, TTB also collects necessary PII to authenticate users and restrict permissions. CFM associates these individuals with user-created user IDs and passwords.

Information Use and Sharing

CFM stores names and phone numbers of those individuals who have provided that contact information in submitted applications. Designated and approved TTB employees have direct access to CFM. All individuals receive different rights in CFM according to their job roles and needs, and are required to authenticate with proper credentials before being granted access to the system.

Information Consent

For an individual's PII to be in CFM, he or she must have previously provided their contact information in the submitted application.

Information Protection

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