Alcohol and Tobacco Tax and Trade Bureau

Automated Commercial System (ACS)

Privacy Impact Assessment

Information Collected and Purpose

The Automated Commercial System (ACS) is the primary tool by which TTB retrieves data collected on the Customs Form from the U.S. Customs Service and utilizes the information to track, audit and investigate the entry/import of alcohol, tobacco, and firearms. ACS receives regular (once every week) data updates related to imports of alcohol, tobacco and firearms from the Bureau of Customs and Boarder Protection via batch interface.

ACS only stores Personally Identifiable Information (PII) that has been included in submitted Customs forms by individuals. For individuals with direct access to ACS, TTB also collects necessary PII to authenticate users and restrict permissions. ACS associates these individuals with user-created user IDs and passwords.

Information Use and Sharing

ACS stores names, email addresses, and phone numbers of those individuals who have provided that information on Customs forms. Designated and approved TTB employees have direct access to ACS, and are authenticated to the system via a username and password. All individuals receive different rights in ACS according to their job roles and needs.

Information Consent

For an individual’s PII to be in ACS, he or she must have willingly and intentionally filled out and submitted a customs form with that information.

Information Protection

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