

Alcohol and Tobacco Tax and Trade Bureau

Network Infrastructure GSS

Privacy Impact Assessment

Information Collected and Purpose

TTB's Network Infrastructure GSS provides TTB users with the infrastructure and office applications required to conduct daily business. The Network Infrastructure GSS includes all of the network routing and storage hardware, windows servers, word processing and email applications, and other assorted hardware and software required for TTB employees to perform their duties. The Network Infrastructure GSS only stores Personally Identifiable Information (PII) that has been submitted by TTB users for contact information purposes.

Information Use and Sharing

The Network Infrastructure GSS stores names, email addresses, addresses, the last four digits of user's social security number, and phone numbers of TTB employees. All TTB employees have limited access to some of the contact information stored, but only designated and approved TTB employees have direct access to the Network Infrastructure GSS. All TTB employees receive different rights to access data in the Network Infrastructure according to their job roles and needs.

Information Consent

For an individual's PII to be in Network Infrastructure GSS, he or she must have willingly and intentionally filled out and submitted a TTB 7200.1 form with that information.

Information Protection

TTB will take appropriate security measures to safeguard PII and other sensitive data stored in Network Infrastructure GSS. 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 Network Infrastructure GSS PII will be limited according to job function. TTB will control access privileges according to least privilege, with the most sensitive data, accessible only to one or more system administrator as necessary.

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
- Systems are routinely scanned to ensure that they are configured correctly and have up-to-date patches and virus definitions