

TESERV SECURITY

1. Personal Data On The Internet

- TEServ uses the industry standard, 128-bit SSL (secure socket layer) to ensure that data transmitted between the user and database is not intercepted. The system has been set so that users can only connect to the server if their browser supports high encryption.
- With the exception of system administrators and group administrators, users will only have access to their own data within the database. Group administrators access will be restricted only to the users that they need to see to do their jobs such as prepare travel orders or voucher for individuals within their own organization.
- TEServ user names are structured so that they are not easily determined or guessed.
- TEServ passwords will be set to expire every 90 days. These passwords are case sensitive, and must include at least one number to decrease the likelihood of someone guessing a password. The system is set to detect intruders by locking user accounts after three unsuccessful login attempts.
- The database itself is housed in at Gelco's secure hosting facility. Physical access to the servers that host the data is restricted to authorized personnel that have been subject to government security investigations. Logical access to the database is also restricted and includes several firewalls and an intrusion detection system. The facility has been inspected by an Information Security Specialist from the Office of the Secretary of Transportation. The Department has issued an interim Security Certificate for the hosting facility and TEServ. It is anticipated that a final security certificate will be issued by July 31, 2002.

2. Selling Personal Data / Personnel Names (Potential Customer Lists) To Other Vendors

- The contract language prevents both PWC and Gelco from giving or selling any data collected by the system to other vendors. Additionally it prevents PWC and Gelco from using this data to sell or create mailing list for their own benefit. Both vendors must turn over to the government all data collected including backups at contract termination.