Transportation Security Administration

Office of Transportation Vetting and Credentialing Screening Gateway and Document Management System Privacy Impact Assessment

January 14, 2005

Contact Point:

Lisa S. Dean
Privacy Officer
Transportation Security Administration

Reviewing Official:

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security

OTVC Screening Gateway and Document Management System
Privacy Impact Assessment

1. Introduction

This Privacy Impact Assessment (PIA) pertains to the hardware, software and communications infrastructure systems that are used by the Transportation Security Administration (TSA) to conduct security threat assessments on various transportation worker and other populations related to transportation. Specifically, this PIA relates to the TSA Office of Transportation Vetting and Credentialing (OTVC) Screening Gateway (Screening Gateway) and the OTVC Document Management Systems (DMS). In this PIA, the Screening Gateway and the DMS will be referred to collectively as "the Gateway Infrastructure" or "the Gateway."

This PIA analyzes the privacy risks presented by the Gateway Infrastructure and describes the steps that TSA has taken to mitigate those risks.

The Gateway is comprised of various hardware platforms and software systems that are used to host system applications that support various OTVC security threat assessment programs. These programs include the Hazardous Materials Endorsement (HME) security threat assessment program, the Registered Traveler (RT) program, and the Transportation Workers Identification Credential (TWIC) program. Other OTVC programs will also use the Gateway Infrastructure as the technological foundation upon which their program-specific software will operate; however, not all such programs will be specifically identified in this PIA. TSA will provide, upon request, a list of all OTVC programs that use the Gateway Infrastructure.

Because this PIA discusses aspects of information technology that may not be well known to the average person, definitions of technical terms have been provided in Section 2.

What does the OTVC Screening Gateway do? The Screening Gateway provides for aggregation of data relevant to security threat assessments of individuals. Applicant data[1] is sent to the Gateway where queries are created and sent out to other systems that contain criminal, citizenship and terrorist-related data. Any data these systems have on the applicant is returned to the Gateway where it is aggregated and presented to TSA personnel for their review and action.

[1] Applicant data means information about individuals who are required to undergo a security threat assessment under an OTVC program; for example, applicants to the Registered Traveler program or commercial drivers who hold or seek to obtain a hazardous materials endorsement for their commercial drivers license.

What does the OTVC Document Management System do? The DMS is the companion system to the Screening Gateway and facilitates the tasks of notifying individuals of the results of their security threat assessment and processing any appeals or waivers that might be submitted by the individuals. The DMS will also facilitate notification to the individuals of the results of their appeal or waiver request.

It is important to note that the Screening Gateway and DMS do not in and of themselves require the collection or processing of personally identifiable information (PII). The sole purpose of these systems is to provide the physical platforms and environment to house the software that services individual OTVC programs. These programs establish the requirements for the collection, processing and dissemination of PII and other data.

2. Definitions

Portions of the definitions below were obtained from webopedia.com, an online encyclopedia dedicated to computer technology.

Advanced Encryption Standard. A block cipher adopted as an encryption standard by the US government, and is expected to be used worldwide and analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES).

Audit trail. A record showing who has accessed a network device and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining and for recovering lost transactions.

Database. A collection of information organized in such a way that a computer program can quickly select desired pieces of data. You can think of a database as an electronic filing system.

Encryption. The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

File Transfer Protocol (FTP). The protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).

Firewall. A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Hardware. Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips. In contrast, software is untouchable. Software exists as ideas, concepts, and symbols, but it has no substance. Books provide a useful analogy. The pages and the ink are the hardware, while the words, sentences, paragraphs, and the overall meaning are the software. A computer without software is like a book full of blank pages -- you need software to make the computer useful just as you need words to make a book meaningful.

Host. To provide the infrastructure for a computer service. For example, there are many companies that host Web servers. This means that they provide the hardware, software, and communications lines required by the server, but the content on the server may be controlled by someone else.

Intrusion detection. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Network. A local area network (LAN), such as the Gateway infrastructure, is a data communications network that resides in a single location, has a specific user group and has a specific topology, or shape.

Password. A secret word or phrase that gives a user access to a particular program or system.

Router. A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts. Very little filtering of data is done through routers.

Secure Sockets Layer (SSL). A protocol for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Web addresses that require an SSL connection start with "https" instead of "http."

Security. In the computer industry, refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most security measures involve data encryption and passwords.

Server. A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer

can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Software. Computer instructions or data. Anything that can be stored electronically is software. The storage devices and display devices are hardware.

> Systems software. Includes the operating system and all the utilities that enable the computer to function.
>
> Applications software. Includes programs that do real work for users. For example, word processors, spreadsheets, and database management systems fall under the category of applications software.

Structured Query Language (SQL). A standardized query language for requesting information from a database.

Switch. In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

Unix. A computer operating system (the basic software running on a computer, underneath things like word processors and spreadsheets). UNIX is designed to be used by many people at the same time (it is "multi-user"). It is the most common operating system for servers on the Internet.

3. Legislative and Rulemaking Overview

In response to the September 11, 2001 terrorist attacks, Congress passed several statutory mandates including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, the Safe Explosives Act (SEA), the Maritime Transportation Security Act (MTSA) and the Aviation Transportation Security Act (ATSA).[2] These Acts provide the basis for performing security threat assessments on various individuals within the transportation sector and those who are applicants for TSA programs. To facilitate these threat assessments, OTVC is establishing the Gateway as a common information technology (IT) infrastructure to support the various OTVC programs that perform these assessments.

[2] P. L. 107-56 (October 25, 2001), 115 Stat. 272, codified at 49 U.S.C. § 5103a(a)(1): P.L. 107-296, November 5, 2002, 116 Stat.2280; P.L. 107-295, November 25, 2002, 116 Stat. 2064.; P. L. 017-71, November 19, 2001, 115 Stat. 597.

4. System Overview

4.1 What personally identifiable information will be collected?

The Gateway will not collect any personally identifiable information (PII). The Gateway is part of the IT infrastructure that exists to support the electronic collection, transmission, analysis, and storage of PII used by individual OTVC programs (such as TWIC and Registered Traveler). The individual software applications for those OTVC programs reside on the Gateway.

The Gateway provides the physical media for storage of information (hard drives) and a method for formatting, operating, and storage of databases (Oracle Database Management System); however, the collection, processing and dissemination of PII are solely governed by the individual OTVC programs and are discussed in the PIAs for those programs. Each program that uses the Gateway Infrastructure has completed its own PIA that describes the PII collected and the reasons for collection. Please refer to the PIA for the specific OTVC program you are interested in to learn what PII that program collects. All TSA PIAs are available on the Department of Homeland Security's website at www.dhs.gov/privacy (click on "Privacy Impact Assessments").

4.2 Why is this personally identifiable information being collected?

The individual OTVC programs that use the Gateway collect data to conduct security threat assessments. Please refer to the PIA for the specific OTVC program you are interested in to learn why that program is collecting PII.

3.3 Who is affected by the collection of this data?

Individuals who are submitting to the security threat assessment programs using the Gateway are affected. Please refer to the PIA for the specific OTVC program you are interested in to learn which individuals are affected.

4.3 What information technology system(s) will be used for this program and what is the step-by-step process for obtaining and processing data?

The Gateway will use a variety of information technologies to provide a secure IT infrastructure for the individual OTVC program software applications. These technologies are the standard components found in most networks and include routers, switches, firewalls, servers, and specialized security software for intrusion detection and data encryption. (See attachment 1 for a general diagram of the infrastructure and the location of these components within the overall design.) This infrastructure is intended to meet the needs of multiple OTVC programs that perform security threat assessments on individuals. By establishing a common IT infrastructure to support these programs, TSA is maximizing the efficient use of taxpayer dollars by avoiding the need for each program to provide its own infrastructure. This approach is consistent with the Office of

Management and Budget's requirements to maximize efficiency in the development of new IT systems and saves the government significant resources and funds that would otherwise be required for planning, design, reviews, documentation, audits and support of multiple infrastructure systems.

The overall design of the Gateway is a layer of devices that begins at the outermost and most vulnerable point of the Gateway network, which is the part that faces the Internet, and proceeds to the most secure and heavily defended area of the network where the program data is stored. As you progress down each layer of the network, additional safeguards are in place that add to the overall security of the systems and data. Below are descriptions of the specific information technologies used in the operation of the Gateway.

Routers: At the outer edge of the Gateway network are the routers, which connect the system to external networks. In this instance, the routers connect the Gateway to the Internet and to other entities that electronically provide information to TSA for OTVC programs. These routers serve as the first line of defense for security. They protect the network from many types of attacks that are commonly used by persons or entities attempting to infiltrate or gain control of the network, or to deny others use of the network. The routers use access control lists to prevent access by any computer that does not originate from an authorized location (e.g., TSA network or an authorized contractor's network).

Switches and Firewalls: Network switches are also part of the Gateway Infrastructure. The switches connect all of the component pieces (such as routers, firewalls and servers) together and allow them to communicate. The Gateway also makes use of firewalls to enhance the security of the system. The firewalls control the types of communications that are allowed to come into the network. They also control the communications between the servers that can be accessed from the Internet (a less secure area also called the demilitarized zone (DMZ)) and the servers that cannot be accessed from the Internet (our most secure area in the network). PII and other sensitive data are stored primarily on the servers that are in the most secure area of the Gateway network.

Servers: All of the servers in the Gateway infrastructure are run by Unix operating systems. In developing the Gateway, TSA considered the use of two other operating systems. TSA ultimately chose Unix for reasons of reliability and security, particularly because the software applications that use the Gateway will be processing PII. Other common operating systems were considered, including one other version of Unix, however, a popular version of Unix was chosen because it is widely used, has an excellent support base and Unix platforms in general have fewer vulnerabilities than many other operating systems and therefore provides a more secure environment.

Software: We are also using specialized software that enhances the security of the Gateway design and provides additional layers of protection for the PII that will be processed on the Gateway. This software consists of:

- Antivirus software to protect the systems against viruses, worms and other malicious forms of software.

- Network Intrusion Detection Software to identify and alert TSA system administrators of any threats that are detected in network traffic as it passes through the network switches.

- Host Intrusion Detection Software to identify and alert system administrators of any threats or suspicious activities (e.g. attempted breaches) that are detected on the servers themselves.

Backup Hardware/Software: The Gateway also uses backup hardware and software to perform daily/weekly/monthly backups of data that is stored on the Gateway. TSA will store the backup tapes at another location to ensure that key data is recoverable in the event that any original data is lost through system or human error (e.g., hard drive crashes, inadvertent deletions).

Databases: Each OTVC program that uses the Gateway infrastructure will have its own database(s) that is only accessible by TSA-authorized persons who have an official need for that program's data. Access will be limited to such persons by technological means, namely by controlling the systems and data that can be accessed by a particular person's logon ID. Databases for the individual OTVC programs will also be logically, and in some cases physically, separated. For example, the Hazmat, TWIC and RT databases will reside on the same physical server; however, they will each be a separate database within the database management structure. Therefore, the data for one program will not be co-mingled with data from other OTVC programs.

4.4 What notice or opportunities for consent are provided to individuals regarding the information collected and how that information is shared?

Notice of the intended use and collection and sharing of personal information is governed by the individual OTVC programs that use the Gateway. Please refer to the PIA for the specific OTVC program you are interested in to learn more about notice and consent, and how PII in that program is shared.

4.5 Does this program create a new system of records under the Privacy Act?

No, but the protections of the Privacy Act apply to the Gateway because it maintains and transmits Privacy Act-protected PII. Because the Gateway is an IT infrastructure system and not an agency program, it does not independently collect or maintain PII; therefore, it does not create a new system of records. However, many (if not all) of the OTVC programs that use the Gateway collect and maintain PII that are subject to the Privacy Act. The data for these programs are part of existing TSA Privacy Act systems of records and each program's PIA identifies which system of records applies to that

program's data. Please refer to the PIA for the specific OTVC program you are interested in to learn whether its data is part of a Privacy Act system of records.

4.6 What is the intended use of the information collected?

The OTVC programs that use the Gateway collect information to conduct security threat assessments. The Gateway does not itself collect information. Please refer to the PIA for the specific OTVC program you are interested in to learn what the intended use is for PII collected by that program.

4.7 With whom will the collected information be shared?

The Screening Gateway is an IT infrastructure system that does not dictate with whom PII will be shared. Instead, each OTVC program that uses the Gateway decides how and with whom information from their program will be shared. The role of the Gateway in information sharing is to permit the program to retrieve information and to facilitate any electronic sharing of that information with other IT systems. Please refer to the PIA for the specific OTVC program you are interested in to learn how PII collected by that program may be shared with others.

4.8 How will the information be secured against unauthorized use?

The Gateway Infrastructure uses the following safeguards for protecting information, including PII, that is stored within the system: physical security, data security, network security, and operations security.

Physical Security. The Gateway hardware/software is located in a secure TSA facility to ensure the physical security of the data in the system, as well as the components of the system that support technological security measures, like the routers. The secure facility limits access to only those individuals who have the proper credentials (badges). Anyone who requires access to these facilities, but does not have the proper credentials, must be escorted and accompanied at all times by someone who does have the requisite credentials. Backup data is stored at off-site contractor facilities, which are also secured.

Data Security. Because the Gateway uses public communication circuits (the Internet) to transmit information, data security was a prime concern in the design of the Gateway. For example, personal data that is transmitted to other government agencies to facilitate criminal, terrorist or immigration checks is encrypted using the Advanced Encryption Standard (AES) and sent via secure file transfer protocol (SFTP), or data can be sent over a virtual private network (VPN) connection, to prevent tampering or access by unauthorized persons; similarly the results of these checks are encrypted before they are returned to the Screening Gateway. Other secure data transmission methods are also used to prevent unauthorized access, including password-protected e-mail for sending files between sources used to conduct the security threat assessment. Users of the systems are required to logon using unique user IDs and passwords and their on-line sessions with the software applications are encrypted using secure sockets layer

(SSL). In addition access to all Gateway network resources (including routers, servers, switches, and firewalls) require correct user IDs and passwords to gain access. Only TSA employees and contractors who have an operational need to access specific data for an OTVC program will be granted these access privileges.

Network security is another of the layers in the overall security of the Gateway. The routers and firewalls control access to the Gateway network itself and prevent intrusion into the network by unauthorized persons. They use access control lists and rules to limit who may gain access to the Gateway network and, for those authorized access, what parts of the network they can use. Firewalls also control which device(s) can access the database servers and also serve to segregate the database servers from the rest of the network. This segregation allows TSA to keep the personal data in the most secure and least accessible segments of the network. Access to the network devices themselves requires the use of unique logon IDs and passwords to limit access to only authorized personnel. We will limit traffic to our web (internet accessible) servers[3] to only secure methods (as can be seen in figure 1, we'll use secure file transfer protocol for data file transfers and secure sockets layer for users connecting to the Gateway). We will take the added precaution of allowing only certain types of traffic[4] (structured query language traffic in this case) between the web servers and the database servers which contain the personal data. No other server(s) will be able to talk with the database servers. This is accomplished by firewall rules that only allow the database server to talk with a specific web server and that allow only specific traffic types to be communicated between the two servers.

We also incorporated Intrusion Detection Systems and security auditing tools into our overall network security. These Intrusion Detection Systems look for abnormal activities and/or known attacks on the network and either shut them down or notify system administrators of these activities. The audit logs will be reviewed regularly to identify anomalies or suspicious or abnormal activity so that TSA may take appropriate action against any person who may be attempting to access the system without authorization or abusing their access privileges.

[3] Non-secure traffic, such as normal "http" web surfing traffic, will be blocked at the firewall as a security best practice.

[4] As a security best practice, only a single type of traffic will be allowed between the web server and the database server. This significantly limits the potential vulnerabilities to the database server, which is where the sensitive information is maintained.

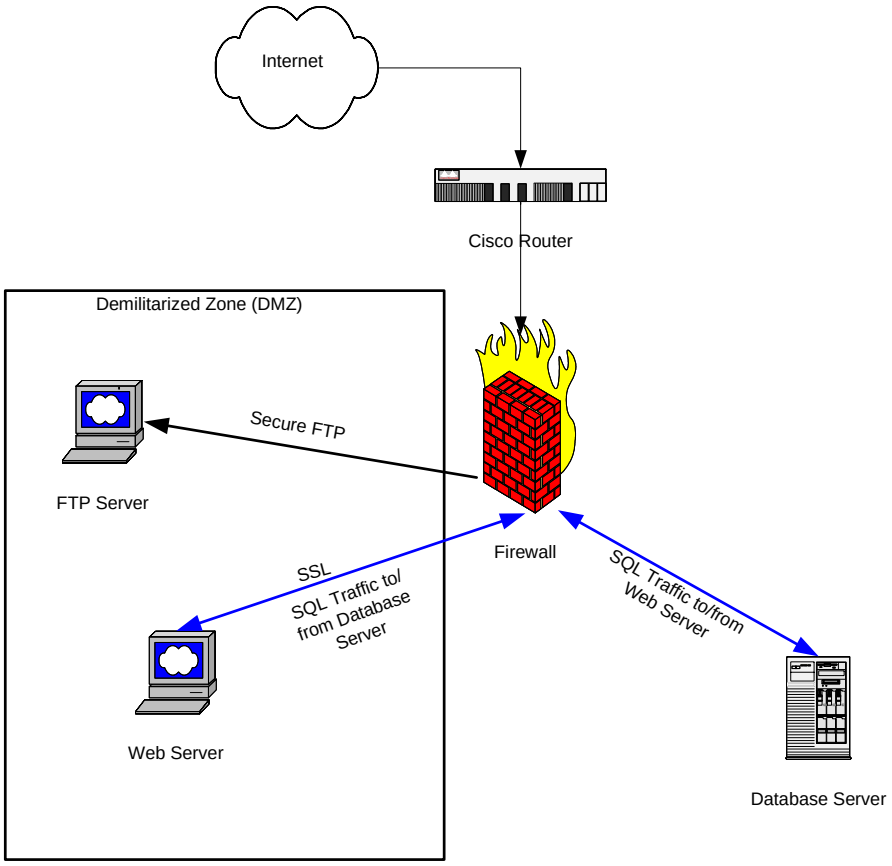

Figure 1.

Operations Security. Operations security for the Gateway is implemented by:

- Strict adherence to Federal Government security and information assurance policies, rules, and regulations
- Strict adherence to TSA security and information assurance policies, rules, and regulations
- Approval of security processes through TSA's formal System Security Accreditation process. This process is formally documented in a Systems and Security Guide for the Gateway Infrastructure.
- Inclusion of a Security Review Board as part of the normal configuration management process for managing changes that are implemented on the Gateway Infrastructure.

In addition, all data is handled under the guidelines of the following Federal laws, regulations and standards:

- *The Privacy Act of 1974*, which requires Federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of information protected by the Act.

- *Federal Information Security Management Act of 2002,* which establishes minimum acceptable security practices for Federal computer systems.

- *49 CFR Part 1520 - Protection of Sensitive Security Information*, which defines and requires the protection of "Sensitive Security Information" (SSI). SSI is sensitive but unclassified information that would be detrimental to the transportation security if publicly released. SSI is often provided to entities in the transportation sector on a need-to-know basis so that they may carry out their security obligations.

- *Federal Information Processing Standard (FIPS) 46-2 - Data Encryption Standard (DES)*, which defines the technical requirements for transmitting encrypted data at minimal acceptable levels of security (i.e., 56 bit encryption).

- *FIPS 197 - Advanced Encryption Standard (AES)*, which defines the technical requirements for transmitting encrypted data at extremely high levels of security (i.e., 128 bit encryption and higher).

- *FIPS 188 - Standard Security Label for Information Transfer*, which defines the technical requirements for transmitting encrypted data across the World Wide Web using Secure Socket Layer (SSL). SSL is the accepted industry standard.

The Gateway implements the aforementioned security requirements and technologies to ensure that the storage and transmission of data is safeguarded at appropriate levels of security. No classified information will be processed or stored by the Gateway.

Only TSA employees and contractors with proper access privileges are allowed access to the Gateway. They will also receive appropriate privacy and security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities. In order to obtain access to TSA secure facilities or the Gateway, TSA personnel and contractors must be vetted by the TSA Office of Security and be subject to a risk assessment. TSA employees and contractors will also be subject to the Gateway Rules of Behavior, which define the responsibilities and expected behavior of individuals accessing the system. Employees who do not comply with the Rules of Behavior will potentially be subject to disciplinary action. Contractors will be subject to remedies provided for under the governing contract.

4.9 What technological mechanisms will be used to secure the data?

The technologies and capabilities that are being used to secure the PII that is stored on the Gateway are discussed in detail in Sections 3.3 and 3.8, above. Here is a recap of the major tools and measures used to secure the data and prevent unauthorized access.

- Encryption – Data transmitted between the Gateway and external systems is encrypted for transmission to and from the external systems. In addition, data stored on servers that are accessible from the Internet remains encrypted. Users

(TSA employees or contractors) accessing the various program software applications (e.g., Hazmat or Registered Traveler) will use encrypted sessions to interact with the applications to prevent unauthorized access to the data.

- Network Routers and Firewall – Routers and firewalls are used to prevent intrusion into the Gateway and to protect databases that reside on the infrastructure. The network firewalls are also used to separate the database servers from the Internet-accessible web servers and to limit the types of network traffic that can be used to communicate with the database servers, thus providing further protection for the PII that resides on them.

- Audit Trails and Intrusion Detection Systems – Attempts by unauthorized users to access sensitive data in the system, including PII, will be automatically recorded in an audit trail for forensic purposes. Intrusion Detection Systems (IDS) are also in place to monitor network traffic and identify any anomalies or known attacks on the system. The IDS software will stop the attack and/or notify system administrators so that appropriate protective action can be taken.

- Physical Security – The Gateway Infrastructure has been installed in a secure TSA facility. This facility requires individuals to have the proper credentials (badges) in order to obtain physical access to the facilities. Anyone who requires access to these facilities, but does not have the proper credentials, must be escorted by someone who does have the requisite credentials.

- User Access – System users must have an assigned logon ID and password in order to access the systems. Users are only allowed access to information and features of the systems at a level that TSA has determined is appropriate for their particular job duties. For example, for users who need to access data pertaining to Hazmat drivers but who are not involved with any aspects of the Registered Traveler program, their network logon credentials will only allow them access to Hazmat driver information. The access control system will bar them from accessing any data on Registered Travelers.

4.10 What databases will be used?

The Gateway does not contain any databases in and of itself; however, databases owned by individual OTVC programs that use the Gateway will reside on the Gateway infrastructure. Please refer to the PIA for the specific OTVC program you are interested in to learn what databases are used by that program.

4.11 Will the information be retained, and if so, for what period of time?

The retention period for information that may pass through or reside on the Gateway Infrastructure is established by the individual OTVC programs that use the Gateway, and not by the Gateway itself. Please refer to the PIA for the specific OTVC program you are interested in to learn the retention period established by that program.

4.12 Will the information collected be used for any purpose other than the one intended?

The OTVC programs that use the Gateway collect information to conduct security threat assessments. The Gateway does not collect or use information for any purpose separate from that of the individual OTVC programs. Please refer to the PIA for the specific OTVC program you are interested in to learn whether PII will be used for any purpose other than the one intended for that program.

4.13 How will an individual seek redress?

Individual OTVC programs that use the Gateway Infrastructure have their own redress procedures, such as appeals and waivers. Please refer to the PIA for the specific OTVC program you are interested in to learn what redress procedures may be available for that particular program.

4.14 Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?

All TSA and assigned contractor staff who perform work related to the Gateway are required to complete privacy training on the proper use and handling of PII. In addition, all TSA and contractor staff must hold appropriate credentials for physical access to the sites housing the Gateway and must comply with the guidelines set forth in the Gateway Rules of Behavior. The Gateway does not contain classified information so security clearances are not required for access.

Please refer to the PIA for the specific OTVC programs that use the Screening Gateway for more information about training and security clearance requirements for each particular program.

For questions or comments, please contact:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 202-772-9848

Attachment 1