U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

FMCSA PORTAL

Responsible Official

Barbara Baker
Application Development Team Lead | IT Development Division
USDOT |Federal Motor Carrier Safety Administration
(202) 493-0215
Barbara.Baker@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

8/4/2014

X Claire W. Barrett

Claire W. Barrett
DOT Chief Privacy & Information Asset Officer
Signed by: CLAIRE W BARRETT

Executive Summary

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration within the U.S. Department of Transportation (DOT) with a core mission to reduce commercial motor vehicle-related crashes and fatalities. The FMCSA Portal provides the industry motor carriers, federal government employees, state and local employees, and contractors with single sign-on capability to several critical FMCSA information systems via the web. The FMCSA Portal was initiated by FMCSA to integrate new technologies with FMCSA business practices and allows FMCSA to quickly and efficiently respond to evolving business requirements, significantly expand IT delivery capabilities, and reduce IT operation and maintenance costs. This Privacy Impact Assessment (PIA) is necessary to provide information regarding the system and the necessity to collect PII.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

By optimizing FMCSA's business processes and improving IT functionality, the FMCSA Portal provides FMCSA and State enforcement personnel and the motor carrier industry with resources needed to improve the safety of U.S. roadways.

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

The FMCSA Portal was initiated by FMCSA to transform the way it does business by integrating the Agency's information technologies with its business practices. Through the FMCSA Portal, FMCSA responds quickly to evolving business requirements, significantly expands IT delivery capabilities, and reduces IT operation and maintenance costs. The FMCSA Portal provides a single entry point to multiple FMCSA information systems for internal and external users in compliance with the E-Government Act of 2002[2]. The FMCSA Portal is located in the Volpe Center, which is owned and operated by DOT.

The FMCSA Portal allows individuals to request a FMCSA Portal account, as well as make modifications to these requests, via the FMCSA Portal website. Motor carriers can use the FMCSA Portal to access crash, inspection, reviews, and census information contained on them in various FMCSA IT systems through a single location. The FMCSA Portal also allows authorized federal and state users to perform the following functions:

- Make assignments (i.e., compliance reviews and safety audits) without exiting the FMCSA Portal
- Manage user accounts (i.e., request forgotten user identifiers, unlock accounts, and change passwords)
- View motor carrier safety information on a single screen
- Execute privileged functions (i.e., run advanced user searches, disable or enable users, and transfer administrative roles) if assigned administrator roles

As part of its security authentication framework, the FMCSA Portal also collects answers to user-chosen personal questions. This information is used only to identify the user later in the event the primary credentials are corrupt or unavailable.
Besides providing single sign-on access to the systems referenced above, the FMCSA Portal also delivers:

- Direct access via the Web - Anyone who can access the Web can access the FMCSA Portal allowing FMCSA enforcement users[3] to access crucial data during roadside inspections and when working from other remote locations.
- Ability to make assignments directly from the FMCSA Portal – Provide FMCSA enforcement users with the proper roles the ability to make assignments for compliance reviews, safety audits and corrective action plans to federal and state field personnel. Assignments can be viewed and managed by enforcement users via the Portal or from Excel spreadsheet reports downloaded from the portal.
- Accounts management - Users can request FMCSA Portal accounts and modify requests directly from the FMCSA Portal. Users were previously required to submit paper-based forms to the Technical Support Hotline in order to request and modify accounts. Administrative users can run advanced user searches, disable or enable users, verify user accounts annually and transfer administrative roles. Individual users can request a forgotten

[2] The systems and applications accessible via the FMCSA Portal are; Motor Carrier Management Information System (MCMIS), Enforcement Management Information System (EMIS), Licensing and Insurance (L&I) System, DataQs, Query Central (QC), Analysis and Information (A&I) Online, Safety and Fitness Electronic Records (SAFER), Electronic Document Management System (EDMS), Hazardous Materials Package Inspection Program (HMPIP), National Consumer Complaint Database (NCCDB), Compliance, Safety, Accountability (CSA) Outreach, Safety Measurement System Preview, North American Standard Driver/Vehicle Inspection, and FMCSA Information Systems Website (InfoSys).
[3] FMCSA enforcement users - Field Safety Investigators, Safety Auditors, Division personnel, Service Center Personnel, HQ and State partners

User ID, unlock a locked account, and receive automatic notifications when their passwords are getting ready to expire.

- Presentation of motor carrier safety data on a single screen - Enforcement users have access to all company data in the same format as that seen by companies.

The FMCSA Portal is an aggregated information management system created with the express purpose of allowing law enforcement and motor carriers to manage carrier safety information and address safety concerns. As a result, one of the portal's primary purposes is to make this information available to the user in a very clear manner. The FMCSA Portal fundamentally contains three types of information:

1. Information provided directly from the individual or motor carrier company
2. Information acquired from external sources pertaining to safety compliance
3. Information on the road safety performance of motor carriers so that FMCSA can identify unsafe carriers, prioritize them for intervention, and monitor if a motor carrier's safety and compliance problem is improving.

This PIA is addressing only the "FMCSA Portal" and not all of the underlying FMCSA IT systems that are accessible via the FMCSA Portal. If those systems contain PII or create privacy risk they will be addressed under separate system PIAs and published on the DOT privacy website (www.dot.gov/privacy.)

Personally Identifiable Information (PII) and the FMCSA Portal

The FMCSA Portal only collects and stores the necessary PII to enable authorized users to sign into the Portal. Through the electronic registration process users submit specific information, including PII, to complete the process of signing up for an account. As a result, the FMCSA Portal contains PII on employees of industry motor carriers, federal government employees and contractors, and state and local employees and contractors. The following information is collected from users through the electronic registration process:

- Username;
- Password;
- First Name;
- Middle Name;
- Last Name;
- Email Address; and
- User-chosen personal security questions and responses

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the

Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[4]*, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*[5]*.*

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

FMCSA does not secretly collect or store PII and clearly discloses its' policies and practices concerning the PII collected and held associated with the FMCSA Portal discussed in this PIA. Information collected directly from the user is done with the user's clear and explicit participation and consent. Data provided by the user is not submitted until the user has read and consented to the FMCSA Rules of Behavior document (See Appendix A) which includes a specific section on expected and accepted privacy related behavior. Authorized users of the FMCSA Portal have access to the information that they submitted about themselves as part of the user registration process.

Information collected from external sources, such as a safety inspection report, or calculated information such as carrier safety scores, are made available in several places within the FMCSA Portal for users to review. The FMCSA Portal provides/displays information that is stored in other systems. For example, the FMCSA Portal displays inspection data that is stored in MCMIS. Crash information is also available to motor carriers when they log into the portal. Enforcement users can see information in the Portal on inspections and then drill down to MCMIS for additional information.

FMCSA published a new information collection (IC) request in the Federal Register at 71 FR 61824 (Docket# FMCSA-2006-25853, December 19, 2006)[6] to notify the public about the new data collection activities. FMCSA also invited public comments over a two month period. Once received the comments were posted for public review. The FMCSA Portal also provides users with a training that is designed to inform the user of how the FMCSA Portal operates and the individual user's responsibilities when accessing the system. In addition, the FMCSA Portal provides clear links to the DOT privacy policy at http://www.dot.gov/privacy.html.

DOT has provided generalized notice to the public of its use of login/access records through the DOT/ALL – 13 (67 FR 30757 - May 7, 2002) Internet/Intranet Activity and Access Records Systems of Records, System of Records Notice (SORN). FMCSA also informs the public that their PII is collected, stored, and used by the FMCSA Portal through this PIA published on the DOT website. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, and all uses of the PII collected and stored by the FMCSA Portal.

[4] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf
[6] The term "COMPASS" used in the notice was the related technology in 2009-2010. This system is now the FMCSA Portal.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

FMCSA ensures that an individual has the right to (a) obtain confirmation of whether FMCSA has PII relating to him or her; (b) access the PII related to him or her within a reasonable time, cost, and manner and in a form that is readily intelligible to the individual; (c) obtain an explanation if a request made under (a) and (b) is denied and challenge such denial; and (d) challenge PII relating to him or her and, if the challenge is successful, have the data erased, rectified, completed, or amended. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOT by complying with DOT Privacy Act regulations, 49 CFR Part 10. Privacy Act requests for access to an individual's record must be in writing either handwritten or typed, may be mailed, faxed or emailed. DOT regulations require that the request include; a description of the records sought, the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Additional information and guidance regarding DOT's Privacy program may be found on the DOT website www.dot.gov/privacy.

Privacy Act requests concerning information in the FMCSA Portal may be addressed to:

Federal Motor Carrier Safety Administration
Attn: FOIA Team MC-MMI
1200 New Jersey Avenue SE
Washington, DC 20590

All personal data maintained by the FMCSA Portal is collected directly from the user to establish a user account. Before the user submits the data, they are required to consent to a Rules of Behavior form which addresses both privacy and proper handling of the information contained in the system. At any point of the collection process, the user has the ability to cancel the process if concerns arise. In addition, all information provided by the user is directly accessible and modifiable by the user, so errors in the information may be corrected at any time. Users may also contact the Service Provider Help Desk at FMCtechsup@dot.gov or 617-494-3003 to request that information be corrected or updated.

Statutory Authority and Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

Title II, section 207 of the E-Government Act of 2002 requires Government agencies to improve the methods by which government information, including information on the Internet, is organized, preserved, and made accessible to the public. FMCSA has made a strategic decision to integrate its IT systems with its business processes. Furthermore, FMCSA has consolidated its systems and databases and has launched a modernization initiative under the FMCSA Portal. The FMCSA Portal is the agency wide initiative to improve its business processes, integrate them with the Agency's information systems, and make the business processes more seamless, secure, and supportive of the Agency's mission of saving lives in the years to come.

The PII discussed in the Overview portion of this PIA are used to create a portal account. Information is collected to initially validate against the user name tables in the database to ensure that the username and password match and are valid. The records in this system are used to electronically authenticate and authorize users to prevent unauthorized access to protected FMCSA IT systems. As part of the security authentication framework, the portal also collects answers to user-chosen personal questions. This information is used only to identify the user later in the event the primary credentials are corrupt or unavailable, and are never transmitted to any other part of the system.

User contact information is used to identify the user and to send various messages and alerts to the user as needed. Messages are sent via both postal mail and email. Messaging is a fundamental requirement of the portal to alert the user to critical actions or states, as well as to deliver correspondence necessary to notify and resolve safety issues.

The FMCSA Portal provides single sign-on access to the systems listed above via a single password and user ID.

The FMCSA Portal also provides:

- *Direct access to FMCSA systems via the Web* - Anyone who can access the Web can access the FMCSA Portal. Allowing users access crucial data during roadside inspections and when working from other remote locations.
- *Ability to make assignments directly from the FMCSA Portal* - Users can make assignments such as Compliance Reviews and Safety Audits without exiting the FMCSA Portal. All of the user's customized prioritization lists are available in one location and can be exported into an Excel spreadsheet for additional customization.
- *Accounts management* - Users can request FMCSA Portal accounts and modify requests directly from the FMCSA Portal. Users were previously required to submit paper-based forms to the Technical Support Hotline in order to request and modify accounts. Individual users can request a forgotten User ID, unlock a locked account, and receive automatic notifications when their passwords are getting ready to expire.
- *Access Management* - Administrative users can run advanced user searches, disable or enable users, and transfer administrative roles.
- *Presentation of motor carrier safety data on a single screen* - Enforcement users have access to all company data in the same format as that seen by companies.
- *Carrier access to their own information* - Carriers now have a single location where they can view their data. With the data extracted directly from the authoritative sources MCMIS, EMIS and L&I, carriers have access to more current data than what was previously available to them through A&I or SAFER. The extracted data includes compliance reviews, safety audits, inspections, crashes and closed enforcement case information. It also includes safety performance of a motor carrier, Census information, and operation type. The extracted data does not include PII. Carriers can also generate their own safety profiles within the FMCSA Portal at no cost and designate third-party entities as having online access to their safety and operational data.

The subsequent use of PII is limited to the fulfillment of those purposes, or such other uses that are compatible with those purposes, as stated in this PIA, unless individuals are given written notice of the proposed change in use, and individuals provide written consent for its use for such new purpose. Unless otherwise authorized by applicable law, FMCSA limits its use of PII related to the implementation of the FMCSA Portal to the performance of official responsibilities pertaining to law enforcement and highway and commercial motor vehicle safety.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The FMCSA Portal only collects the information necessary to accomplish the FMCSA Portal's stated purpose. The portal collects basic user contact information, security information, organizational information to establish authorization capacities and provide driver/carrier safety statistics that pertain to the specific goal of the portal.

User contact information is used to identify the user and to send various messages and alerts to the user as needed. Messages are sent via both postal mail and email. Messaging is a fundamental requirement of the portal to alert the user to critical actions or states, as well as to deliver correspondence necessary to notify and resolve safety issues.

As part of the security authentication framework, the portal also collects answers to user-chosen personal questions. This information is used only to identify the user later in the event the primary credentials are corrupt or unavailable, and are never transmitted to any other part of the system.

Organizational information concerning the user's affiliated company or law enforcement office is used to:

a) Establish chains of authority to determine which user(s) can approve certain requests made by the user
b) Determine what information the user can access based on what they have authority over

User profile records in the FMCSA Portal are covered by GRS 24 User Identification, Profiles, Authorizations, and Password Files, http://www.archives.gov/records-mgmt/grs/grs24.html, Item 6c which provides disposition instructions for the User Identification, Profiles, Authorizations, and Password Files. These files may be deleted when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes."

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The FMCSA Portal collects PII from industry motor carrier employees, federal government employees and contractors, and state and local employees and contractors in order to grant Single Sign On access to several critical FMCSA information systems via the web. Information is collected to initially validate against the user name tables in the database to ensure that the username and password match are valid. Personal information on drivers regarding safety inspections is also accessible in the FMCSA Portal. The information is contained to the portal and only used by the system. No PII information is transmitted to any third-party or external systems that might misuse the information.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

The FMCSA Portal has strict input validation checking on all supplied data and will reject all requests that contain invalid data with an appropriate error message. FMCSA Portal users are prohibited from submitting registration information unless all required data fields are completed in a valid format. These controls ensure that user data is accurately collected in a proper format.

Customer and employee information is kept current by allowing users to electronically update their own basic personal information such as address and email. Once a user submits their modified information, the system is immediately updated to reflect these changes. Users can review their personal data and make modifications as necessary. Users may also contact the Service Provider Help Desk to correct inaccurate information. Beyond personal information, the portal also manages driver and carrier incident reports and safety scores. The business model of handling negative events involves direct user interaction through the notification of affected users on the issue and facilitates correspondence between law enforcement and carriers to help resolve the issue. In this manner, affected users are actively engaged in the feedback mechanism to ensure safety information is accurate.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

PII must be protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for Federal information systems under FISMA and are detailed in Federal Information Processing Standards (FIPS) Publication 200*, Minimum Security Requirements for Federal Information and Information Systems* dated March 2006 and NIST Special Publication (SP) 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations* dated April 2013. FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII.
- Protect against unauthorized access to or use of PII.

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records in the FMCSA Portal at the Service Provider's location are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the electronic system is logged and monitored.

In addition to the general FMCSA information security procedures, the FMCSA Portal utilizes specific technologies and procedures to ensure data is safeguarded:

- **Authentication** – System access requires a valid username and password. New accounts require manual approval by an authorized user. Unauthenticated users are not allowed access to restricted resources.
- **Role-based ACL** – Individual actions within the portal require specific roles. Users are only given the roles required by their duties. Role change requests require manual approval by an authorized user. Roles minimize the impact of compromised account.
- **Account Lockout** – Excessive retries on account authentication will result in that account being locked out. This prevents brute-force or dictionary attacks.
- **Account Expiration** – Accounts require periodic forced password changes and use expiration policies to disable unused or old accounts. This reduces the number of accounts that can be used as a threat.
- **Training** – All users are required to read a Rules of Behavior (RoB) upon creating an account, which addresses proper handling of secure data. In addition, the system requires existing users to periodically review the RoB, disabling access until they have completed the requirement.

Identification and Authentication (I&A) safeguards require each user to positively identify themselves by a unique user-identification and password prior to being granted system access. The I&A safeguards serve as the mechanism for associating a specific user with the recorded audit events. The user's password proves proper identity, enabling the trusted system to perform authentication. Access to sensitive information in FMCSA Portal requires a valid user identifier and password combination for all federal, state, and external users. E-authentication assurance level requirements dictate the authentication mechanisms that must be implemented for external users. All authorized users must read and sign a "Rules of Behavior" document (Appendix A) prior to being granted access to FMCSA Portal.

The FMCSA Portal is approved through the Security Authorization Process under the National Institute of Standards and Technology. ~~is currently undergoing a Security Authorization review. A new package is being developed and Authorization of the system is expected by March 2014.~~ After a review of the security and privacy controls, FMCSA Portal was authorized to operate (ATO) for one year on April 24, 2014.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

FMCSA is responsible for identifying, training, and holding FMCSA employees and contractors accountable for adhering to FMCSA privacy and security policies and regulations. FMCSA will follow the Fair Information Practice Principles as best practices for the protection of PII associated with the FMCSA Portal. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records.

Federal and contract employees will be given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance will be provided in the form of mandatory annual Security and privacy awareness training as well as the DOT/FMCSA Rules of Behavior. The FMCSA Information System Security Officer and FMCSA Privacy Officer will conduct periodic security and privacy compliance reviews of the National

Registry System consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

Responsible Official

Barbara Baker
Requirements Team Lead | IT Development Division
USDOT |Federal Motor Carrier Safety Administration
(202) 366-3397
Barbara.Baker@dot.gov

DOT Privacy Office Approval

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
(202) 366-8135
privacy@dot.gov

Appendix A

U. S. Department of Transportation
Federal Motor Carrier Safety Administration

Rules of Behavior
Federal Motor Carrier Safety Administration (FMCSA) Information Technology Systems

My signature below indicates that I have read, understand, and will comply with the below-stated requirements as a condition of maintaining an active account with access to FMCSA IT systems. I also understand that failure to comply with these requirements may result in disciplinary action and/or loss of access privileges.

First Name		**MI**		**Last Name**	
Title					
Phone		**Email**			
Supervisor Name					
Phone					
Organization				**State**	
Office Symbol or Org. Code					
Signature				**Date**	

As a user of the Federal Motor Carrier Safety Administration (FMCSA) Information Technology (IT) systems, I understand that I am personally responsible for the use and any misuse of my system account and password. I also understand that by accessing a U.S. Government information system, I must comply with the following requirements:

General:

1. FMCSA IT systems are authorized for official Government use only and, in limited cases, for personal use. Limited personal use may only be permitted if (i) it does not directly or indirectly interfere with DOT/FMCSA email services; (ii) burden DOT with noticeable, incremental cost; or (iii)

interfere with the FMCSA user's employment or other obligations to the Government. Limited personal use is subject to a supervisor's approval.

2. FMCSA IT systems may not be used (i) for a purpose that violates any Federal law; (ii) for mass mailings of personal messages/statements; (iii) for commercial purposes, financial gain, or to support "for profit" non-Government activities; or (iv) to engage in any activities that would discredit DOT or FMCSA (gambling, viewing of adult content, etc.). "FMCSA-discrediting activities" also include seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or materials.
3. FMCSA reserves the right to monitor the activity of any machine connected to its infrastructure.
4. FMCSA IT systems are the property of the Federal Government. FMCSA owns the data stored on these systems, including all email messages and information, even those deemed personal.
5. Non-public information that was obtained via FMCSA IT systems may not be divulged outside of Government channels without the express permission of the owner of that information.
6. Any activity that violates Federal laws for information protection (hacking, spamming, etc.) is prohibited.
7. Telecommuters are required to review and adhere to the DOT Remote Access Policy and any new requirements issued by the Administrator's Office.
8. FMCSA contractors using non-FMCSA furnished equipment to access FMCSA IT systems must install and maintain antivirus and anti-spyware tools on said equipment.
9. Users of FMCSA IT systems may not communicate FMCSA information to external news groups, bulletin boards, or other public forums without permission from their supervisors.
10. Users must lock their computers if they are away from their desk and use a password-protected screensaver to automatically lock the computer.
11. Password authentication must be enabled on all FMCSA devices under all circumstances.

Email:

12. Personal email accounts must not be used for FMCSA work-related correspondence.

Government Equipment:

13. Users of FMCSA IT systems are prohibited from modifying their systems by (i) installing unapproved hardware; (ii) installing additional operating systems; (iii) installing unapproved software applications; or (iv) altering approved configuration settings.
14. Users of FMCSA IT systems may not access services with the potential to degrade network performance. This includes use of a program or Internet site that provides continuous data streams [continuous stock quotes, headline news updates, peer to peer (p2p) file sharing, etc.].
15. Users may not connect unauthorized devices (non-FMCSA-issued) to the network without approval as documented in the Network Access Policy.

Mobile Devices:

16. Mobile computers/devices with FMCSA data must be appropriately secured at all times to prevent loss or theft and should not be left in unattended vehicles.
17. Users in possession of an FMCSA-issued BlackBerry must sign an additional DOT Rules of Behavior document specific to the use of their BlackBerry.
18. Laptop locks must be used to secure FMCSA laptops to a permanent or immovable object.

19. Laptop users must never tamper or attempt to circumvent the purpose or implementation of standard security controls including, but not limited to, host-based firewall and antivirus software.

Password:

20. FMCSA IT system accounts are provided solely for the use of the individual for whom they were created. Passwords or any other authentication mechanisms must **never** be shared or stored in **printed form** in any accessible place. If stored digitally, a password must not be stored in a cleartext or readable format.
21. Each FMCSA IT system has password format requirements and a password expiration policy. Although there are variations between systems, passwords that are at least eight alphanumeric characters in length and contain at least two letters and three numbers or special characters (@, $, #, etc.) will normally meet the requirement. Typically, passwords must be changed every 90 days (every 30 days for Administrator accounts).
22. Any security problems or password compromises must be reported immediately to the supervisor, who will then contact the FMCSA Information System Security Officer (ISSO).

Privacy:

23. Users may only send sensitive and privacy information to systems and personnel that have been approved for this level of information. Consult the FMCSA Information System Security Officer for what is considered to be "sensitive" and "privacy" information, and what FMCSA systems are approved to receive this information.
24. Users must only use Sensitive Personally Identifiable Information (SPII) on encrypted laptops, mobile devices, and storage media devices. SPII data is any piece of information that can potentially be used to uniquely identify, contact, or locate a single person (home address, date of birth, social security number, driver's license number, etc.).
25. Users must protect all FMCSA confidential/sensitive and privacy information from disclosure.
26. Hard copies of confidential/sensitive and privacy information must be shredded and destroyed.

I understand that Federal law provides for punishment under Title 18 of the U.S. Code, including a fine and up to 10 years in prison, for the first offense for anyone who:

a) Intentionally accesses a Government information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.

b) Intentionally accesses a Government information system without authorization, or exceeds authorized access, and impacts the Government's operation, including availability of that system.

c) Intentionally accesses a Government information system without authorization, or exceeds authorized access, and alters, damages, or destroys information therein.

d) Intentionally accesses a Government information system without authorization, or exceeds authorized access, and obtains anything of value.

e) Prevents authorized use of a Government information system.