



U.S. Department of Transportation

Privacy Impact Assessment

Pipelines and Hazardous Materials Safety Administration (PHMSA) PHMSA Portal System (PPS)

Responsible Official

Amit Joshi

Amit.Joshi@dot.gov

(202) 366-7213

Reviewing Official

Claire W. Barrett

Chief Privacy & Information Asset Officer

Office of the Chief Information Officer

privacy@dot.gov



Executive Summary

The Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA), an Operating Administration within the Department of Transportation (DOT), is responsible for protecting people and the environment by advancing the safe transportation of energy and other hazardous materials essential to the daily lives of Americans. To do this, PHMSA establishes national policy, sets and enforces standards, educates, and conducts research to prevent pipeline or hazardous material incidents. To meet these goals, PHMSA must maintain effective communication in order to prepare the public and first responders and reduce the impact if an incident does occur. The PHMSA Portal System (PPS) helps PHMSA accomplish this by automating the sharing of information while protecting privacy by implementing strict safeguards that protect against unauthorized access to and unintentional loss of information. PPS is used to manage access to various PHMSA systems and requires information about authorized users and creates a record of their permissions and access history to provide appropriate levels of access. This Privacy Impact Assessment was conducted because PPS collects personally identifiable information (PII) from members of the public (e.g. State Partners and Pipeline Operators that PHMSA regulates) in order to provide them with access to PHMSA IT systems.

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;*

¹Office 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).

- *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

PPS identifies, authenticates and authorizes users for access to PHMSA applications. It does this through system-generated user IDs and user-supplied passwords for external users, and Personal Identity Verification (PIV)-authentication of DOT employees and contractors.

In order to provide members of the public with access to PHMSA IT systems, PPS collects:

- User Type (e.g. Hazmat, Pipeline, or State Regulator);
- Username;
- Name (first, last, mi);
- Business address;
- Business email; and
- Business phone number.

Users may enroll with PPS by creating an account directly through the PPS web interface <https://portal.phmsa.dot.gov/PHMSAPortal2/>. PPS only shares this information with applications and systems for which PPS manages access. Data collected from PPS users is not directly searchable by name or any other identifier. See Appendix A for an illustration of the information required to be provided access to PPS.

When using PPS to access PHMSA systems and applications, users are provided a message stating: “by clicking “Submit” you agree that your information will be used in accordance with PHMSA’s Privacy Policy.” The privacy policy link is provided and contains all the protection and advisories required by the E-Government Act of 2002.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is 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) v3², 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 Organizations³.

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.

For direct access to PPS, users must agree to the PHMSA Privacy Policy. The PPS website has a link to the DOT Privacy Policy. The Privacy Policy describes DOT information practices related to the online collection and the use of PII as required by the E-Government Act of 2002.

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.

External users provide PII only when they create accounts. Users are aware of the purpose for the collection of their PII, and how it will be used. Users are provided with a Privacy Act statement, which states the purpose for the collection of the information, the authority to collect it, and that the provision of the information is voluntary, but may result in the inability to access the system.

System users can update the PII that they submitted for access to PPS at any time. PHMSA requests identifying information from external users for account creation. The information is not used outside of PPS. External user accounts are set to inactive after 30 days of inactivity. The password is required to be reset to reactivate the account. Individual user accounts are not deleted because individual users and/or business entities have differing system access requirements depending on service or reporting requirement. Some users may access the system on a regular basis whereas others may only require access once a year or even 2-3 years, depending on their reporting requirement.

Internal (DOT) users accounts are managed by the DOT Information Technology Support Services (ITSS) policies regarding account creation, disablement and deletion.

Under the provisions of the Privacy Act, individuals may request searches of PPS to determine if any records have been added that may pertain to them. This is accomplished by sending a written request directly to:

² <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

³ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Pipeline and Hazardous Materials Administration
Attn: FOIA Team or PHMSA Privacy Officer
1200 New Jersey Avenue, SE
Washington, DC 20590

At any time, a PPS user may contact a privacy representative at PHMSAprivacy @dot.gov. The to contact a privacy representative may also be found at www.transportation.gov/privacy.

Purpose Specification

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

PPS was created and is maintained to support PHMSA's mission-critical activities as described in various legislative mandates. These include the Pipeline Safety, Regulatory Certainty, and Job Creation Act of 2011, the Moving Ahead for Progress in the 21st Century (MAP-21) of 2012, the Fixing America's Surface Transportation (FAST) Act of 2015, and the Protecting Our Infrastructure of Pipelines and Enhancing Safety (PIPES) Act of 2016. PPS collects PII to appropriately grant access to various PHMSA systems and applications.

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.

Data collected from PPS users is used only for account creation and authorization. PPS system administrators are bound by the DOT Rules of Behavior for IT Users to only use the information in the system for the purpose it was collected. Users can update the PII that they submitted for access to PPS at any time. Information in PPS is retained permanently until a NARA records schedule is approved. Once the sceheulde is approved the records will be delete/destroyed after data mingratio to PDM. (See DAA-0571-2018-0004-0001)

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.

PHMSA uses PII collected by PPS to identify user access to systems, set access permissions, monitor access, and contact users if required. PHMSA's data collection to those required to meet the legally authorized business purpose and mission of the Agency. PHMSA does not share any PII collected by PPS with PHMSA system other than those that require it for access.

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 PPS System Owner and PHMSA IT Security Team perform an annual review to ensure that the collection, use, and maintenance of information collected for operating PPS is still necessary and restricted to the purposes specified in this document. Additionally, this annual review ensures the access and information is accurate, complete, and timely.

Users may access and make changes to their PII in PPS. However, users may not access or change any log files or other monitoring-related information.

If for business reasons PPS changes the data types that are being collected they must follow the PHMSA IT systems change management process, which requires approval by the PHMSA Information System Security Manager and PHMSA Privacy Officer.

Security

DOT shall implement administrative, technical, and physical measures to 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.

PPS is the access point for PHMSA systems and applications, and is categorized as a FIPS 199 moderate system. PII is 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 the Federal Information System Management Act (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, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

PPS is housed in the DOT HQ Data Center. Physical access to the PPS system is limited to authorized personnel through building key cards and room-access key pads. Personnel with physical access have all undergone DOT security screening and privacy training. All users receive customized Terms and Conditions of Use and/or Rules of Behavior that describe their privacy responsibilities. Access to the system containing the records in the PPS 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 PPS system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the PPS system is logged and monitored.

Logical access controls restricts users of PPS. These controls are guided by the principles of least privilege and need-to-know. Role-based user accounts are created with specific job functions allowing only authorized accesses, which are necessary to accomplish assigned tasks in accordance with compelling operational needs

and business functions of the PPS system. Any changes to user roles required approval of the System Manager.

PPS also maintains an auditing function that tracks all user activities in relation to data including access and modification. Through technical controls including firewalls, intrusion detection, encryption, access control list, and other security methods; FMCSA prevents unauthorized access to data stored in the SAFETYNET system. These controls meet Federally mandated information assurance and privacy requirements.

In the event of a privacy or security breach, PHMSA follows the breach management procedures outlined in DOT Order 1351.19 PII Breach Notification Controls.

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.

PHMSA identifies, trains, and hold employees and contractors accountable for adhering to DOT privacy and security policies and regulations. PHMSA follows the Fair Information Practice Principles as best practices for the protection of PII. In addition to these practices additional policies and procedures are consistently applied, especially as they relate to the protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training as well as the DOT Rules of Behavior. The PHMSA Information System Security Manager and Privacy Officer conduct periodic security and privacy compliance reviews of the PPS system consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Amit Joshi

System Owner

Solutions Architect, PHF-30 Information Resources Division / Office of the CIO

Approving Official

Claire W. Barrett

Chief Privacy & Information Asset Officer

Office of the Chief Information Officer

Appendix A - Enrollment Screens

PHMSA Pipeline and Hazardous Materials Safety Administration **U.S. Department of Transportation**

PHMSA Home | Contact Information

Contact Information Verification Confirmation

Please fill out the following personal information to enroll in the PHMSA Portal.

* Please select the type of user you wish to enroll as: Hazardous Materials

* First Name: John
Middle Initial: D
* Last Name: Doe
Username: John.Doe

* Business Address #1: 123 MAIN STREET
Business Address #2:
* Country: United States
* City: ANYWHERE
* State: District of Columbia
* Zip Code: 11111

* US Work Phone: (555)555-5555
Alt Phone:
Fax:
* Work Email: test@test.gov
* Confirm Email: test@test.gov

Cancel Next

Contact Us | FAQs | Privacy Policy | FOIA | Accessibility | Web Policies | Site Map
Regulations.gov | USA.gov | WhiteHouse.gov | DOT.gov

Figure 1: PPS Initial User Enrolment Page

PHMSA Pipeline and Hazardous Materials Safety Administration **U.S. Department of Transportation**

PHMSA Home | Contact Information

Contact Information **Verification** Confirmation

Verification

Please verify the information below. If the information is correct, please click the Submit button below. If the information is incorrect, please use the Previous button to edit your information.

Enrollment Date: 5/9/2019
First Name: John
Middle Initial: D
Last Name: Doe

Username [John.Doe] is already taken. We recommend you to use [John.Doe5]

* Username: John.Doe Validate Username

Address #1: 123 MAIN STREET
Address #2:
Country: US
City: ANYWHERE
State: DC
Zip Code: 11111

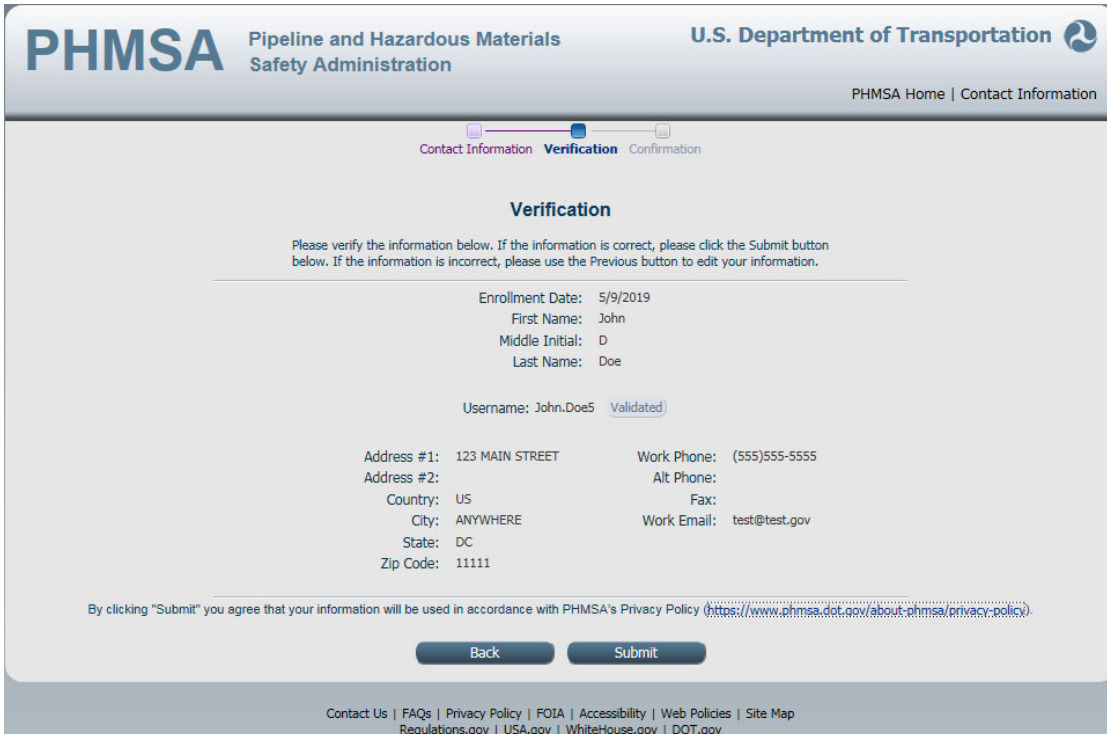
Work Phone: (555)555-5555
Alt Phone:
Fax:
Work Email: test@test.gov

By clicking "Submit" you agree that your information will be used in accordance with PHMSA's Privacy Policy (<https://www.phmsa.dot.gov/about-phmsa/privacy-policy>).

Back

Contact Us | FAQs | Privacy Policy | FOIA | Accessibility | Web Policies | Site Map
Regulations.gov | USA.gov | WhiteHouse.gov | DOT.gov

Figure 2: Username Already Taken



PHMSA Pipeline and Hazardous Materials Safety Administration **U.S. Department of Transportation**

PHMSA Home | Contact Information

Contact Information **Verification** Confirmation

Verification

Please verify the information below. If the information is correct, please click the Submit button below. If the information is incorrect, please use the Previous button to edit your information.

Enrollment Date: 5/9/2019
 First Name: John
 Middle Initial: D
 Last Name: Doe

Username: John.Doe5 Validated

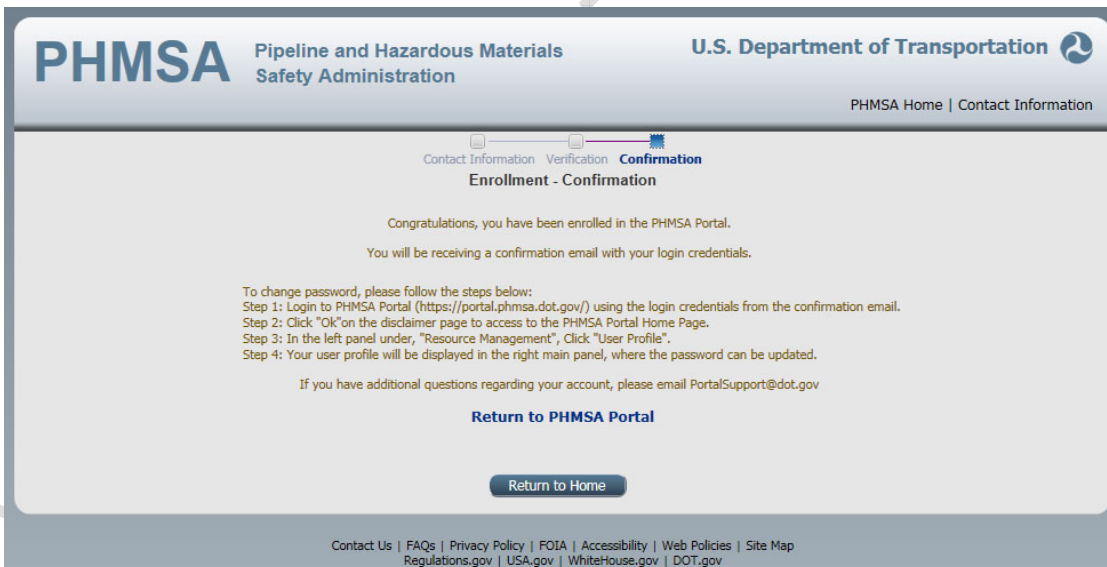
Address #1: 123 MAIN STREET Work Phone: (555)555-5555
 Address #2: Alt Phone:
 Country: US Fax:
 City: ANYWHERE Work Email: test@test.gov
 State: DC
 Zip Code: 11111

By clicking "Submit" you agree that your information will be used in accordance with PHMSA's Privacy Policy (<https://www.phmsa.dot.gov/about-phmsa/privacy-policy>)

[Back](#) [Submit](#)

Contact Us | FAQs | Privacy Policy | FOIA | Accessibility | Web Policies | Site Map
 Regulations.gov | USA.gov | WhiteHouse.gov | DOT.gov

Figure 3: PPS User Enrolment Verification Page



PHMSA Pipeline and Hazardous Materials Safety Administration **U.S. Department of Transportation**

PHMSA Home | Contact Information

Contact Information Verification **Confirmation**

Enrollment - Confirmation

Congratulations, you have been enrolled in the PHMSA Portal.

You will be receiving a confirmation email with your login credentials.

To change password, please follow the steps below:
 Step 1: Login to PHMSA Portal (<https://portal.phmsa.dot.gov/>) using the login credentials from the confirmation email.
 Step 2: Click "OK" on the disclaimer page to access to the PHMSA Portal Home Page.
 Step 3: In the left panel under, "Resource Management", Click "User Profile".
 Step 4: Your user profile will be displayed in the right main panel, where the password can be updated.

If you have additional questions regarding your account, please email PortalSupport@dot.gov

[Return to PHMSA Portal](#)

[Return to Home](#)

Contact Us | FAQs | Privacy Policy | FOIA | Accessibility | Web Policies | Site Map
 Regulations.gov | USA.gov | WhiteHouse.gov | DOT.gov

Figure 4: PPS User Enrolment Confirmation

Appendix B Privacy Policy

PHMSA's privacy policy is available online at <https://www.phmsa.dot.gov/about-phmsa/privacy-policy>.

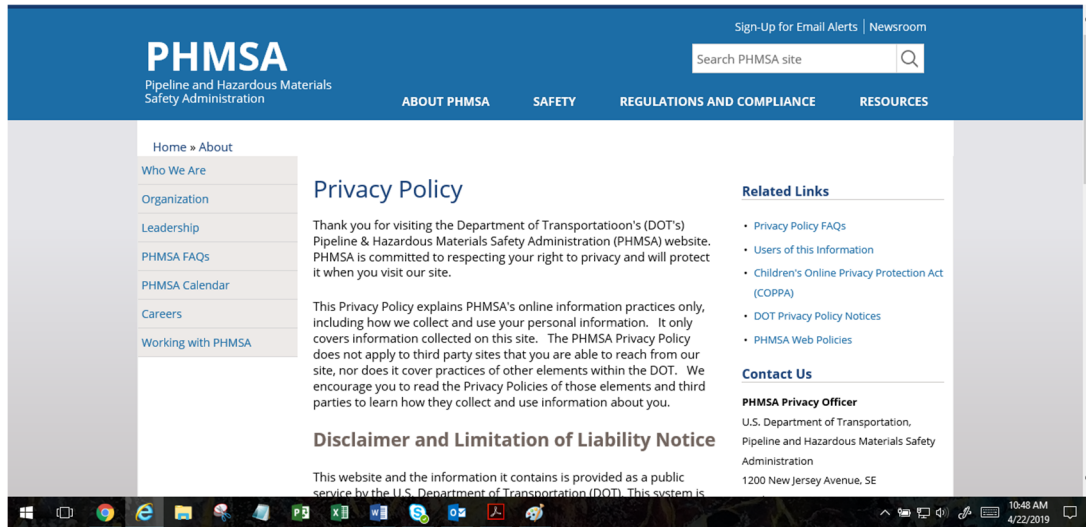


Figure 5: Privacy Policy Screenshot 1

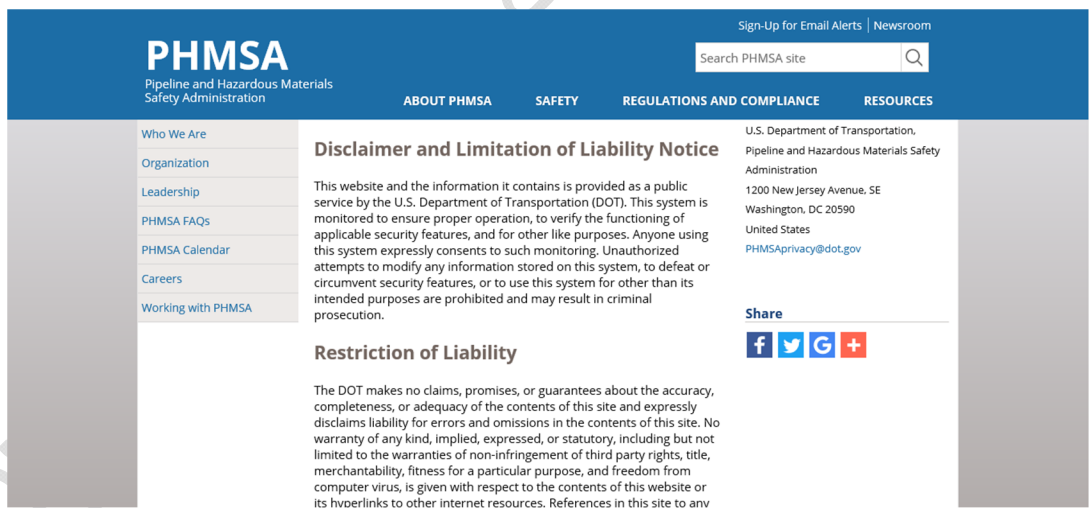


Figure 6: Privacy Policy Screenshot 2

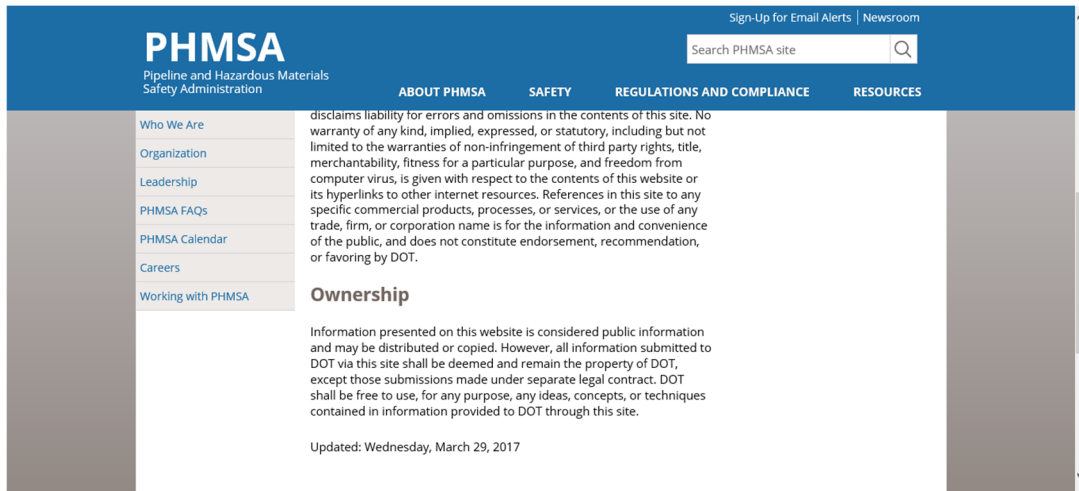


Figure 7: PHMSA Privacy Policy Screenshot 3