U.S. Department of Transportation

Privacy Impact Assessment

Pipelines and Hazardous Materials Safety Administration (PHMSA)

PHMSA Portal System (PPS)

Responsible Official
Liezl Gonzalez (PHMSA)
liezl.gonzalez@dot.gov
202-734-0062

Reviewing Official
Karyn Gorman
Chief Privacy 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 (OA) within the 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 accomplishes 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 (PIA) was conducted because PPS collects Personally Identifiable Information (PII) from members of the public (e.g., State Partners and Pipeline Operators that PHMSA regulates) to provide them with access to PHMSA IT system through the PPS.

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

[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).

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

PPS identifies, authenticates, and authorizes users for access to PHMSA applications. It does this through LOGIN.GOV, which enforces multifactor authentication (MFA) for external users, and MyAccess for DOT employees and contractors.

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, middle);
- Business Name
- Business address;
- Business email; and
- Business phone number.

External users may enroll with PPS by creating an account via LOGIN.GOV through the PPS web interface https://portal.phmsa.dot.gov/PHMSAPortal2/. PPS only shares this information with applications and systems for which PPS manages authorization. Data collected from PPS users is not directly searchable by name or any other identifier. Access control is managed by authenticating through sign in via LOGIN.GOV. See Appendix A for an illustration of the information required to be provided access to PPS.

When enrolling with 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.

PPS has subsystems, which are called applications as described below:

- **Special Permits** - Allows shippers and container manufacturers to submit requests to obtain permission to ship hazardous materials using containers/transport modes that do not have an existing specific approval in the Hazardous Material Regulations.
- **Approvals (multiple modules)** - Allows hazmat shippers, carriers, manufactures, packagers, testers and cylinder Re-qualifiers (testing requirements) to submit Approvals requests. As part of Approvals there are several groups that require independent approval requests. These include Fireworks (Allows OHMS the capability of processing consumer, display and articles for pyrotechnic Fireworks Approvals), Competent Authority, Explosives, Re-qualifiers, M-Numbers (marking symbols numbers), and Visual Inspection.
- **Online CFR** - The Online Code of Federal Regulations (CFR) is PHMSA's enterprise platform to navigate, search, and view CFR regulations.
- **Case Management System (CMS)** - Manages the workflow processes of hazmat enforcement inspections from start to finish. The system coordinates between several different role-based user groups to allow for approval, rejection, and modification of cases as they are worked among Field Operations.
- **Hazardous Materials Incident Communication System (HAZMATICS)** - Manages National Response Center (NRC) data and Unreported Incidents and is a publicly available data entry interface: and workflow automation to collect, validate and manage PHMSA specific hazmat incident report information.
- **Hazardous Materials Emergency Preparedness (HMEP)** - Allows Office of Hazmat Safety (OHMS) to issues 65 to 70 grants to states, territories, and tribes each year for the purposes of hazardous materials emergency preparedness HMEP training of emergency responders in dealing with hazmat incidents.
- **Hazmat Registration** - Allows companies to submit hazmat registrations as required under 49 CFR 107 Subpart G. It also provides capabilities to process registration fees in the form of credit card, ACH and check payments, as well as refunds.
- **Radioactive Material (RAM)** - Certification: Issues Competent Authority Certificates for Type B fissile material radioactive material packages and special form Class 7 materials.
- **Online Search Websites** - These sites are available on the PHMSA website. They allow users to search for details on Special Permits, Approvals, Registrations, and Incidents.
- **Package Testing** - is used to collect testing data of hazmat packages. The data is used by the Office of Hazmat Safety to perform risk analysis.
- **PHMSA Document Search** - Provides PHMSA users with the ability to search the document repository using key words and applying search conditions.
- **Annual Reporting** - Allows pipeline operators to submit their annual reports electronically. Annual reports collect information regarding all regulated system types and specifically collects information regarding pipeline miles and facilities attributes such as pipe diameter, material, location, types of testing conducted annually, and whether the pipe is located in high consequence areas.
- **OPID Management** - Allows pipeline operators to use PHMSA Portal to request Operator IDs. Other specific capabilities that shall be provided include Notification

Management, OMS Reports, OPID Access Request, OPID Association, OPID Contact Management, and OPID Management.

- **Work Management System (WMS)** - Integrates pipeline modules and automatically routes tasks to pipeline inspectors and State partners to manage requests for new operator IDs, changes in operatorship, or safety programs. It also provides a module to manage failure investigations and carry-out enforcement functions. Below describes each of the modules within WMS:
    - **Failure Inspection Module (FIM)** - Allows PHMSA investigators to manage and track pipeline accidents during the Telephonic Investigation phase.
    - **Pipeline Asset Manager (PAM)** - Provides operator and asset management functions, as well as automated notifications submitted by pipeline operators to the States and PHMSA Regions who regulate them.
    - **Pipeline Inspection Investigation and Enforcement (PIIE)** - The system allows pipeline users to manage inspections, investigations, enforcement, program support activities and other functionality for PHMSA's pipeline programs and its state partners.
    - **Inspection Planning Module (IPM)** - Provides users to create, manage, and track work effort for Inspection Planning Activities from start to finish. It allows integration with PIIE to get user and inspection data.
    - **Other WMS Capabilities** - Other features such as support Effort Data, Search Feature, Roles Administration and Management.
- **Federal State Tracking and Reporting (FedSTAR)** - Used to automate, collect, and analyze the State Program processes that State Agencies are required to follow to receive grant funding from, and participate in, the PHMSA State Pipeline Program, in addition to providing back-office program management to the PHMSA Office of State Programs.

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) v3[2], 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[3].

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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.

PHMSA's privacy policy is available online at https://www.phmsa.dot.gov/about-phmsa/privacy-policy. See Appendix B for screenshot of PHMSA's privacy policy website. PPS maintains audit logs and DOT has provided generalized notice to the public of its use of login/access records through the System of Records Notice (SORN), DOT/ALL – 13 (67 FR 30757 - May 7, 2002) Internet/Intranet Activity and Access Records Systems of Records. Additionally, PHMSA informs the public of how their PII is collected, stored, and used by the PPS Portal through this Privacy Impact Assessment (PIA), published on the DOT website.

Individual Participation and Redress

DOT provides 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 they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

PHMSA requests identifying information from external users for account creation. External users provide PII only when they create accounts. The information is not used outside of PPS. System users can update the PII that they submitted for access to PPS at any time. Users are aware of the purpose for the collection of their PII, and how it will be used. Users are provided a link to the PHMSA's privacy policy at https://www.phmsa.dot.gov/about-phmsa/privacy-policy which states the purpose for the collection of the information and use of personal information. In addition, the system displays a disclaimer page to alert users of notice and consent to monitoring while using the system.

Individual external 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:

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. Additional information 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 schedule is approved the records will be delete/destroyed after data migration to PHMSA DataMart (PDM). (See *DAA-0571- 2018-0004-0001).* The PPS Portal maintains user profile records in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 Information Systems Security Records, Item 30 (System Access Records).

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.

PPS and all applications that reside in PPS present a unified umbrella under which PHMSA's internal and external users conduct their Hazmat and Pipeline related work individually or collectively. PPS and its independently managed applications provide for a largely automated environment, reducing costs and human error associated with manual processes. In addition, PPS provides a consolidated "one-stop-shop" environment for internal PHMSA and external users with a standardized look and feel that helps in managing user expectations, ease of use and decreased training time. Internal users are PHMSA employees, contractors and authorized users. External users are non-PHMSA employees such as PHMSA's state partners and pipeline operators that PHMSA regulates.

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.

PPS doesn't create any outputs and/or decisions about individuals. Data in PHMSA DataMart (PDM) collected through PPS enables PHMSA program offices to process information efficiently. A typical transaction within the system is outlined below:

- PPS Enrollment: External user registers with PPS using their LOGIN.GOV account and Internal users use MyAccess to login to PPS.
- PPS Hazmat: Registered Users logs in with login credentials, clicks on one of the PPS Hazmat Integrated Applications, submits the request for approvals of hazmat transport or special permits, Hazmat Office will review the request and provide a disposition (Granted, Denied, etc.)
- PPS Pipeline: Registered Users logs in with login credentials, clicks on one of the PPS Pipeline Application such as Annual Reports, submits the Annual Reports

PPS is used to collect, store, or process information as follows:

- HAZMAT approvals
- HAZMAT incidents
- HAZMAT registrations
- HAZMAT Enforcement (Inspections / Investigations and Chief Counsel)
- HAZMAT Special Permits
- HAZMAT Outreach activities
- Pipeline incidents
- Pipeline inspections
- Pipeline operator registration and statistics/annual reports
- Pipeline Enforcement
- National pipeline map
- Safety-related condition reports

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 Change Management Board (CMB) to include System Owner, PHMSA Data Steward, PHMSA Change Manager, and PHMSA Information System Security Manager.

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 keypads. 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 of 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 restrict 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 require 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; PHMSA prevents unauthorized access to data stored in the PPS 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

Liezl Gonzalez (PHMSA)
System Owner
Office of the PHMSA CIO

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.02.27 09:56:20 -05'00'

1.0 Appendix A – Enrollment Screens

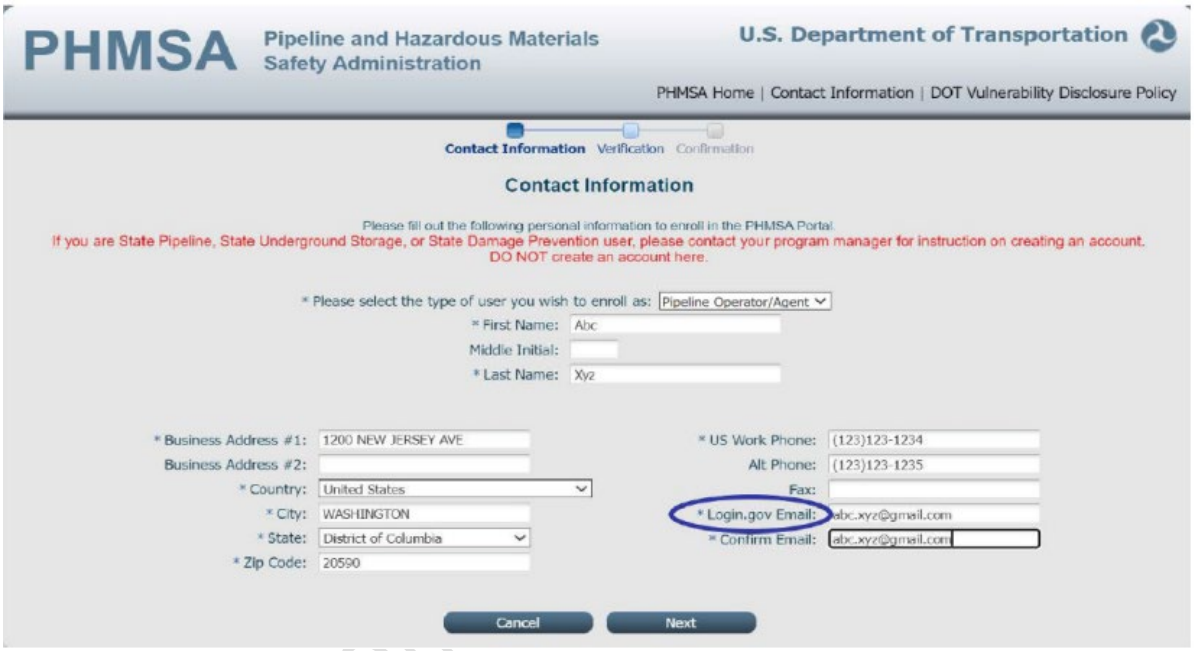

Figure 1: PPS Initial User Enrolment Page

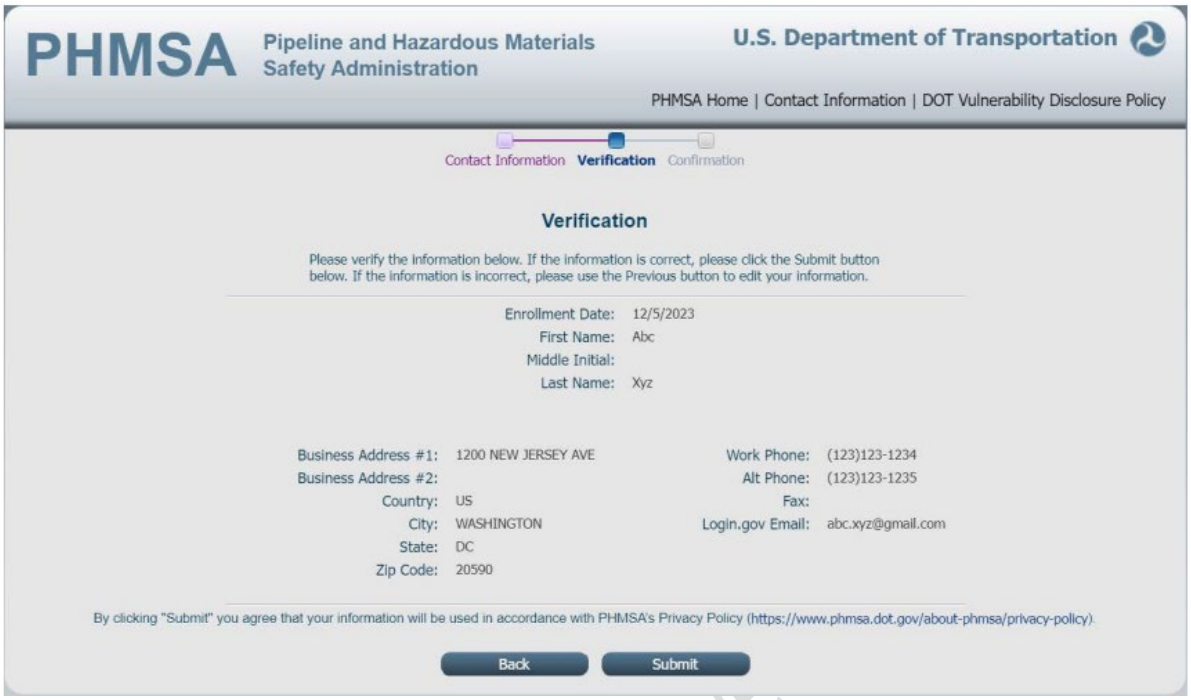

Figure 2: PPS User Enrolment Verification Page

Figure 3: PPS User Enrolment Confirmation

Figure 4: Privacy Disclaimer

2.0 Appendix B Privacy Policy

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

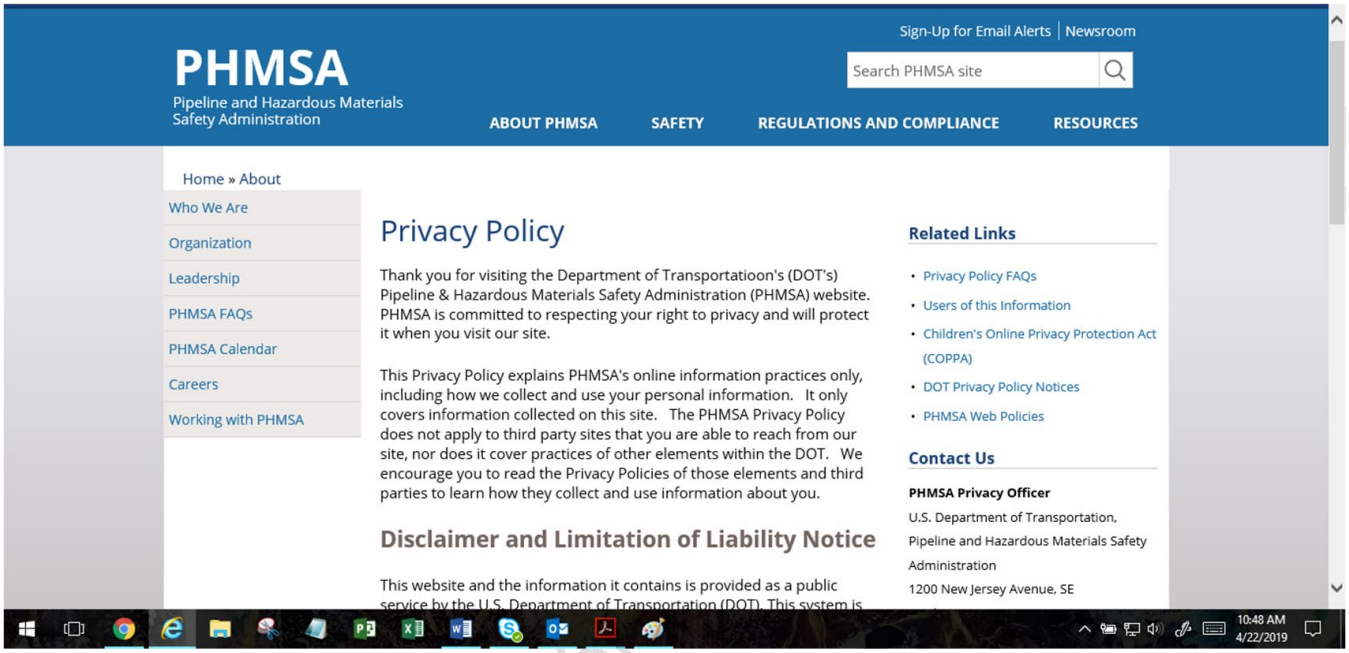

Figure 5: Privacy Policy Screenshot 1

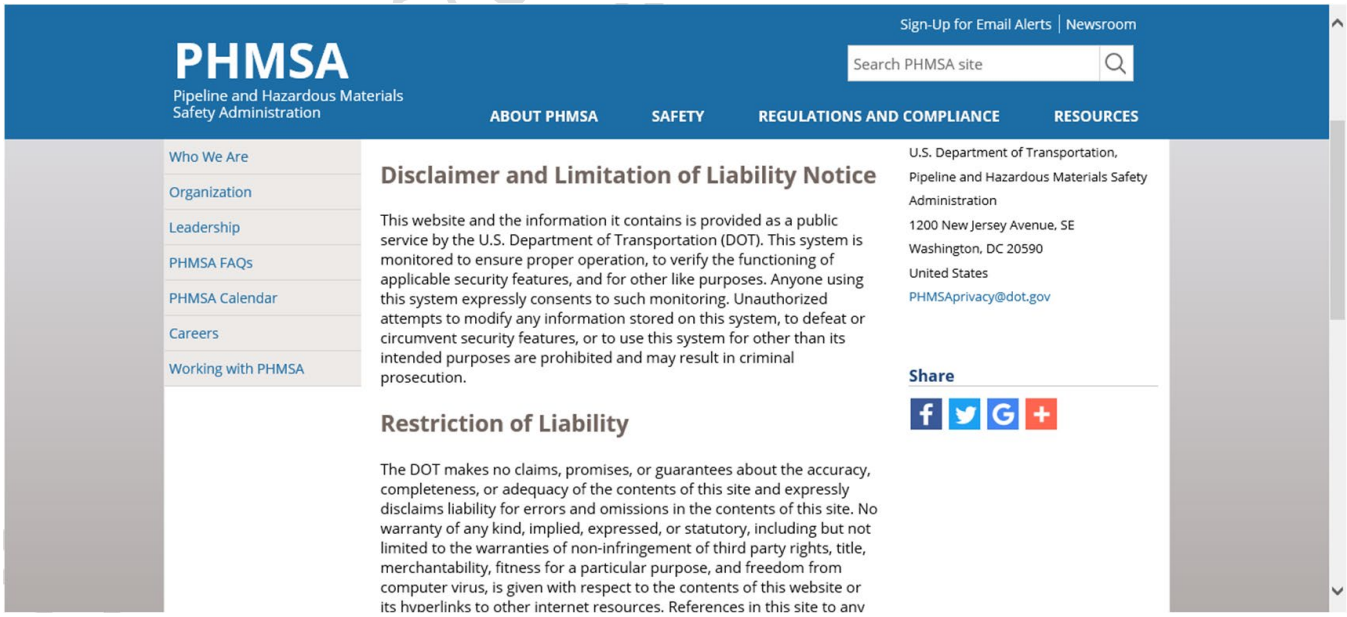

Figure 6: Privacy Policy Screenshot 2

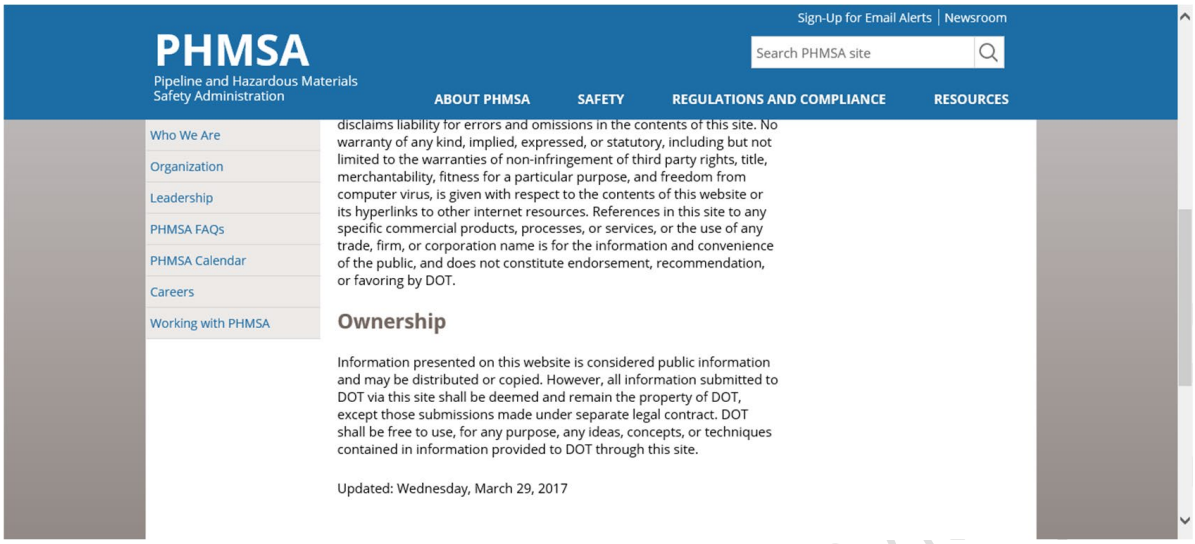

Figure 7: Privacy Policy Screenshot 3