Privacy Threshold Assessment (PTA)

Maritime Administration
Information Collection
2133-0029
Shipbuilding Orderbook and Shipyard Employment

Privacy Threshold Assessment (PTA)

The Privacy Threshold Assessment (PTA) is an analytical tool used to determine the scope of privacy risk management activities that must be executed to ensure that the Department's initiatives do not create undue privacy risks for individuals.

The Privacy Threat Assessment (PTA) is a privacy risk management tool used by the Department of Transportation (DOT) Chief Privacy Officer (CPO). The PTA determines whether a Department system[1] creates privacy risk for individuals that must be further analyzed, documented, or mitigated, and determines the need for additional privacy compliance documentation. Additional documentation can include Privacy Impact Assessments (PIAs), System of Records notices (SORNs), and Privacy Act Exemption Rules (Exemption Rules).

The majority of the Department's privacy risk emanates from its direct collection, use, storage, and sharing of Personally Identifiable Information (PII),[2] and the IT systems used to support those processes. However, privacy risk can also be created in the Department's use of paper records or other technologies. The Department may also create privacy risk for individuals through its rulemakings and information collection requirements that require other entities to collect, use, store or share PII, or deploy technologies that create privacy risk for members of the public.

To ensure that the Department appropriately identifies those activities that may create privacy risk, a PTA is required for all IT systems, technologies, proposed rulemakings, and information collections at the Department. Additionally, the PTA is used to alert other information management stakeholders of potential risks, including information security, records management and information collection management programs. It is also used by the Department's Chief Information Officer (CIO) and Associate CIO for IT Policy and Governance (Associate CIO) to support efforts to ensure compliance with other information asset requirements including, but not limited to, the Federal Records Act (FRA), the Paperwork Reduction Act (PRA), the Federal Information Security Management Act (FISMA), the Federal Information Technology Acquisition Reform Act (FITARA) and applicable Office of Management and Budget (OMB) guidance.

Each Component establishes and follows its own processes for developing, reviewing, and verifying the PTA prior to its submission to the DOT CPO. At a minimum the PTA must be reviewed by the Component business owner, information system security manager, general counsel, records officers, and privacy officer. After the Component review is completed, the Component Privacy Office will forward the PTA to the DOT Privacy Office for final adjudication. Only PTAs watermarked "adjudicated" and electronically signed by the DOT

[1] For the purposes of the PTA the term "system" is used throughout document but is not limited to traditional IT systems. It can and does refer to business activity and processes, IT systems, information collection, a project, program and/or technology, and proposed rulemaking as appropriate for the context of the assessment.

[2] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

CPO are considered final. Do NOT send the PTA directly to the DOT PO; PTAs received by the DOT CPO directly from program/business owners will not be reviewed.

If you have questions or require assistance to complete the PTA please contact your Component Privacy Officer or the DOT Privacy Office at privacy@dot.gov. Explanatory guidance for completing the PTA can be found in the PTA Development Guide found on the DOT Privacy Program website, www.dot.gov/privacy.

PROGRAM MANAGEMENT

SYSTEM name: Shipyard Orderbook and Shipyard Employment

Cyber Security Assessment and Management (CSAM) ID: N/A

SYSTEM MANAGER CONTACT Information:

Name: **Beth Gearhart**

Email: beth.gearhart@dot.gov

Phone Number: 202-366-1867

Is this a NEW system?

☐ **Yes** (Proceed to Section 1)
☒ **No**
☒ **Renewal**
☐ **Modification**

Is there a PREVIOUSLY ADJUDICTED PTA for this system?

☐ **Yes:**

Date: *<<Provide the date of the most recently adjudicated PTA.>>*

☒ **No**

1 SUMMARY INFORMATION

1.1 System TYPE

☐ **Information Technology and/or Information System**

Unique Investment Identifier (UII): *<<Provide the persistent numeric code applied to the investment that allows for tracking and identification.>>*

Cyber Security Assessment and Management (CSAM) ID: *<<Provide the system name found in the Cyber Security Assessment and Management (CSAM) system. If you do not have a system ID in CSAM, provide an explanation.>>*

☐ **Paper Based:**

☐ **Rulemaking**

Rulemaking Identification Number (RIN): *<<Provide RIN assigned by OMB's electronic docketing system>>*

Rulemaking Stage:

☐ **Notice of Proposed Rulemaking (NPRM)**
☐ **Supplemental NPRM (SNPRM)**:
☐ **Final Rule**:

Federal Register (FR) Notice: *<<Provide full Rulemaking Name, Federal Register citation, and web address if available.>>*

☒ **Information Collection Request** (ICR)[3]

☐ **New Collection**

☒ **Approved Collection or Collection Renewal**

☒ **OMB Control Number: 2133-0029**

☒ **Control Number Expiration Date: May 31, 2020**

☐ **Other:** <<*Describe the type of project*>>

1.2 System OVERVIEW:

In compliance with the Merchant Marine Act of 1936, as amended MARAD conducts this information collection (survey) to obtain information from the shipbuilding and ship repair industry to be used primarily to determine if an adequate mobilization base exists for national defense and for use in a national emergency.

For additional information, see **2133-0029, Support Statement**

2 INFORMATION MANGEMENT

2.1 SUBJECTS of Collection

Identify the subject population(s) for whom the system collects, maintains, or disseminates PII. (Check all that apply)

☒ **Members of the public:**

☐ **Citizens or Legal Permanent Residents (LPR)**

☐ **Visitors**

☐ **Members of the DOT Federal workforce**

☐ **Members of the DOT Contract workforce**

☒ **System Does Not Collect PII.** If the system does not collect PII, proceed directly to question 2.3.

2.2 What INFORMATION ABOUT INDIVIDUALS will be collected, used, retained, or generated?

2.3 Does the system RELATE to or provide information about individuals?

☐ **Yes:** Click here to enter text.

☒ **No**

[3] See 44 USC 3201-3521; 5 CFR Part 1320

If the answer to 2.1 is "*System Does Not Collect PII*" **and** the answer to 2.3 is "*No*", you may proceed to question 2.10.
If the system collects PII or relate to individual in any way, proceed to question 2.4.

2.4 Does the system use or collect SOCIAL SECURITY NUMBERS (SSNs)? (This includes truncated SSNs)

☐ **Yes:**

Authority: *<< Provide explicit legal authority for collection or use of SSN in the system.>>*

Purpose: *<< Describe how the SSN is used and why it is necessary as opposed to lower-risk identifiers.>>*

☐ **No**: The system does not use or collect SSNs, including truncated SSNs. Proceed to 2.6.

2.5 Has an SSN REDUCTION plan been established for the system?

☐ **Yes:** *<< Provide the details of the reduction plan including date conducted, alternatives evaluated, determination reached and any steps taken to reduce the SSN collection and use.>>*

☐ **No:** *<< A system without an SSN reduction plan is in violation of the Privacy Act. Explain why a reduction plan has yet to be completed and provide an anticipated completion date.>>*

2.6 Does the system collect PSEUDO-SSNs?

☐ **Yes:** *<< Describe how the pseudo-SSNs are used to accomplish the authorized purpose and why they are necessary as opposed to lower-risk identifiers.>>*

☐ **No**: The system does not collect pseudo-SSNs, including truncated SSNs.

2.7 Will information about individuals be retrieved or accessed by a UNIQUE IDENTIFIER associated with or assigned to an individual?

☐ **Yes**

Is there an existing Privacy Act System of Records notice (SORN) for the records retrieved or accessed by a unique identifier?

☐ **Yes:**

SORN*: <<Provide the full SORN Name, the Federal Register citation, and the URL>>*

☐ **No:**

Explanation:

Expected Publication: Click here to enter text.

☐ **Not Applicable:** Proceed to question 2.9

2.8 Has a Privacy Act EXEMPTION RULE been published in support of any Exemptions claimed in the SORN?

☐ **Yes**

Exemption Rule: *<< Provide the full Exemption Rule Name, the Federal Register SORN citation, and the URL.>>*

☐ **No**

Explanation: *<< An explanation must be provided for failure to comply with all the requirements of the Privacy Act without an Exemption Rule.>>*

Expected Publication: *<< List the expected date of publication for an Exemption Rule that will bring the system into compliance with the Privacy Act.>>*

☐ **Not Applicable**: SORN does not claim Privacy Act exemptions.

2.9 Has a PRIVACY IMPACT ASSESSMENT (PIA) been published for this system?

☐ **Yes:** *<< Provide the full PIA Name, the publication date, and the URL. >>*

☐ **No**: Click here to enter text.

☐ **Not Applicable:** The most recently adjudicated PTA indicated no PIA was required for this system.

2.10 Does the system EXCHANGE (receive and/or send) DATA from another INTERNAL (DOT) or EXTERNAL (non-DOT) system or business activity?

☐ **Yes:** *<<Identify the systems/business activities engaged in data exchange and provide a general reason for the exchange. If PII is exchanged, identify the PII elements and the specific reason for the exchange.>>*

☒ **No**

2.11 Does the system have a National Archives and Records Administration (NARA)-approved RECORDS DISPOSITION schedule for system records?

☐ **Yes:**

Schedule Identifier: *<< Identify the relevant NARA schedule, including the schedule number, title, section, and URL.>>*

Schedule Summary: *<< Provide a synopsis of the relevant portion(s) of the schedule.>>*

☐ **In Progress:** *<< Include proposed schedule, when it will be submitted to NARA, or job code.>>*

☒ **No:** Click here to enter text.

3 SYSTEM LIFECYCLE

The systems development life cycle (SDLC) is a process for planning, creating, testing, and deploying an information system. Privacy risk can change depending on where a system is in its lifecycle.

3.1 Was this system IN PLACE in an ELECTRONIC FORMAT prior to 2002?

The E-Government Act of 2002 (EGov) establishes criteria for the types of systems that require additional privacy considerations. It applies to systems established in 2002 or later, or existing systems that were modified after 2002.

☐ **Yes**: <<Provide date was the system established as an electronic system.>>

☒ **Not Applicable**: System is not currently an electronic system. Proceed to Section 4.

3.2 Has the system been MODIFIED in any way since 2002?

☐ **Yes**: The system has been modified since 2002.

☐ **Maintenance.**

☐ **Security.**

☐ **Changes Creating Privacy Risk**: *<< Describe any modification that may introduce new privacy risk, including but not limited to: paper to electronic conversions, changing anonymous information into information in identifiable form, significant system management changes (including application of new technologies), significant system or data merging, use of new authentication technologies in support of public access, commercial data sources, new interagency uses, changes in internal flow or data collection, or alternation of data characterization.>>*

☐ **Other**: Click here to enter text.

☐ **No**: The system has not been modified in any way since 2002.

3.3 Is the system a CONTRACTOR-owned or -managed system?

☐ **Yes**: The system is owned or managed under contract.

Contract Number: *<<Contract #>>*

Contractor: *<< Contractor Name >>*

☐ **No**: The system is owned and managed by Federal employees.

3.4 Has a system Security Risk CATEGORIZATION been completed?

The DOT Privacy Risk Management policy requires that all PII be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards. The OA Privacy Officer should be engaged in the risk determination process and take data types into account.

☐ **Yes**: A risk categorization has been completed.

Based on the risk level definitions and classifications provided above, indicate the information categorization determinations for each of the following:

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Based on the risk level definitions and classifications provided above, indicate the information system categorization determinations for each of the following:

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

☐ **No:** A risk categorization has not been completed. Provide date of anticipated completion.

3.5 Has the system been issued an AUTHORITY TO OPERATE?

☐ **Yes:**

Date of Initial Authority to Operate (ATO): <<Date>>

Anticipated Date of Updated ATO: *<<Provide the date of the next anticipated ATO renewal.>>*

☐ **No:** *<<Provide the anticipated ATO date.>>*

☐ **Not Applicable**: System is not covered by the Federal Information Security Act (FISMA).

4 COMPONENT PRIVACY OFFICER ANALYSIS

The Component Privacy Officer (PO) is responsible for ensuring that the PTA is as complete and accurate as possible before submitting to the DOT Privacy Office for review and adjudication.

COMPONENT PRIVACY OFFICER CONTACT Information

Name: Shelly Nuessle

Email: shelly.nuessle@dot.gov

Phone Number: 202-366-1104

COMPONENT PRIVACY OFFICER Analysis:

Since this report simply collects numbers and job classifications, no personal information is contained in the reports. This reporting is consolidated manually for consumption and is not entered into an electronic system except by the system owner.

5 COMPONENT REVIEW

Prior to submitting the PTA for adjudication, it is critical that the oversight offices within the Component have reviewed the PTA for completeness, comprehension and accuracy.

Component Reviewer	Name	Review Date
Business Owner	Beth Gearhart	4/8/2020
General Counsel	Mitch Hudson	
Information System Security Manager (ISSM)	Shelly Nuessle	4/8/2020
Privacy Officer	Shelly Nuessle	4/8/20
Records Officer	Steve Snipes	

Table 1 - Individuals who have reviewed the PTA and attest to its completeness, comprehension and accuracy.