Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Ingesting Ship Arrival Notification System (SANS) Data into the DHS Data Framework		
Component:	U.S. Coast Guard (USCG)	**Office or Program:**	
Xacta FISMA Name (if applicable):	Ship Arrival Notification System (SANS)	**Xacta FISMA Number (if applicable):**	**USC-00790-MAJ-00790**
Type of Project or Program:	IT System	**Project or program status:**	Operational
Date first developed:	Click here to enter a date.	**Pilot launch date:**	**N/A**
Date of last PTA update	**October 6, 2015**	**Pilot end date:**	**N/A**
ATO Status (if applicable)	**Complete**	**ATO expiration date (if applicable):**	

PROJECT OR PROGRAM MANAGER

Name:	Paul Reynolds		
Office:	Data Framework	**Title:**	
Phone:	202-617-5068	**Email:**	Paul.reynolds@hq.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Derek Richardson		
Phone:		**Email:**	Derek.richardson@associates.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Renewal PTA

The United States Coast Guard (USCG) stores Notice of Arrival and Departure (NOAD) information electronically in the Ship Arrival Notification System (SANS). The U.S. Coast Guard collects NOAD information in order to provide for the safety and security of U.S. ports and waterways and the overall security of the United States. This information allows the USCG to facilitate effectively and efficiently the entry and departure of vessels into and from the United States and assist the USCG with assigning priorities while conducting maritime safety and security missions in accordance with international and domestic regulations. PII concerning vessel owner, crew members and/or non-crew individuals is collected to give an accurate picture of who has overall responsibility for a given vessel and who is onboard that vessel. The information is collected for the purpose of ensuring the safety and security of U.S. ports and waterways and the overall security of the United States. It is used to conduct necessary screening and national security checks.

The Data Framework is the Department's information sharing platform for the movement of data from the unclassified environment to the classified environment. It was established to protect and share information across DHS entities, promoting agile and data-driven decision capabilities to meet multiple mission needs. The Framework's current core capabilities include single-site search available on classified networks, dynamic access controls to safeguard information from multiple sources while enhancing sharing, near real-time movement of data for operational decision-making, centralized access to data across DHS components and a single distribution point for DHS data to the Intelligence Community.

The DHS Data Framework is governed through the Data Framework Working Group, which is the focal point for Data Framework development including prioritizing and coordinating the ingestion of data sets, providing a venue for transparency, oversight, and governance.

This renewal is submitted because the updated PTA has expired.

The DHS Data Framework consists of three interrelated capabilities. First, the Framework provides Data Repositories on the unclassified local area network (A-LAN) and the Classified Local Area Network (C-LAN) in which information of operational value to the Department is replicated and tagged with metadata indicating the provenance and characteristics of the data at an element-by-element level. The Office of the Chief Information Officer (OCIO) within the Management Directorate maintains the data repository on the A-LAN, known as Neptune, which contains only data from other Departmental source systems. I&A maintains the data repository on the C-LAN, known as Cerberus, which contains both departmental data and information received from external partners. Second, the Data Framework includes tools for analysis of data. The tools allow users to view and manipulate data in furtherance of the users' authorized functions. Third, the dynamic access control layer enables the controlled sharing and safeguarding of the data and the capabilities themselves. The dynamic access controls within the DHS Data Framework facilitate the execution of essential homeland security functions while preserving individuals' privacy rights and civil rights and civil liberties.

The Department plans to ingest SANS data into the Data Framework. Neptune will stage USCG's unclassified SANS data and then will transfer the ingested SANS data to Cerberus. The Department intends to use the data for analytical purposes in an operational environment. A controlled set of users, as

described in Appendix C to the Data Framework PIA, will perform classified and unclassified searches against the data repositories cloud using approved search tools in support of their border security and counterterrorism missions. The addition of other types of Data Framework users will require Data Framework Working Group approval and will be captured in the Data Framework PIA Appendix C.

As the Data Framework matures, the Department will establish a scalable operational infrastructure which positions the Data Framework to integrate more data sources and deliver capability sufficient to support real-time operations, while increasing safeguarding control and compliance. This infrastructure enables use of the data within the boundary of the Data Framework systems through approved searches and data delivery services via Data Framework's user and policy/rule management.

The Department has previously published separate PIAs and updates for the DHS Data Framework, as well as Neptune and Cerberus, to reflect their transition from a pilot phase to a Limited Production Capability Phase and Initial Operational Capability Phase.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these
3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): ☒ Contractors working on behalf of DHS ☒ Employees of other federal agencies
4. What specific information about individuals is collected, generated or retained?	

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

There is no change in the collection of SANS data. USCG continues to collect the following type of information:

USCG collects information from vessels' owners, operators, masters, agents or person in charge of the vessel(s). Information is submitted at 96-hours prior to a vessel's arrival to the United States.

Notice of arrival information collected falls into the following broad categories: Vessel and Voyage Details (including arrival/departure), Crew Information, Non-Crew Information, and Cargo Information,

Specifically, the following information is collected:

Vessel and Voyage Information

- Name of vessel
- Name of registered owner
    - Country of registry
- Call sign
- International Maritime Organization (IMO) international number or, if vessel does not have an assigned IMO international number, substitute with official number
- Name of the operator
- Name of charterer
- Name of classification society
- Maritime Mobile Service Identity (MMSI)
- Vessel(s) gross tonnage

Voyage Information

- Arrival information
    - o Names of last five foreign ports or places visited
    - o Dates of arrival and departure for last five foreign ports or places visited
    - o For each port or place of the United States to be visited, a list of the names of the receiving facility, the port or place, the city, and the state
    - o For each port or port or place of the United States to be visited, the estimated date and time of arrival
    - o For each port or port or place in the United States to be visited, the estimated date and time of departure
    - o The location (port or place and country) or position (latitude and longitude or waterway and mile marker) of the vessel at the time of reporting

- The name and telephone number of a 24-hour point of contact o Duration of the voyage
- Last five ports of call
- Dates of arrival and departure in last port or place visited
- Estimated date and time of arrival to the entrance of port, if applicable

- Departure information
  - The name of departing port or place of the United States, the estimated date and time of departure
  - Next port or place of call (including foreign), the estimated date and time of arrival
  - The name and telephone number of a 24-hour point of contact

Information for each crewmember onboard:

- Full name
- Date of birth
- Nationality
- Identification information (type7, number, issuing country, issue date, expiration date)
- Position or duties on the vessel
- Where the crewmember embarked (list port or place and country)
- Where the crewmember will disembark

Information for each person onboard in addition to crew

- Full name
- Date of birth
- Nationality
- Identification information (type, number, issuing country, issue date, expiration date)
- U.S. address information
- Where the person embarked (list port or place and country)
  - Where the person will disembark

Cargo Information

- A general description of cargo, other than CDC (certain dangerous cargo), onboard the vessel (e.g., grain, container, oil, etc.)

• Name of each certain dangerous cargo carried, including United Nations (UN) number, if applicable • Amount of each certain dangerous cargo carried Operational condition of equipment required by 164.35 of this chapter of the International Safety Management (ISM) Code Notice: • The date of issuance for the company's Document of Compliance certificate • The date of issuance of the vessel's Safety Management Certificate • The name of the Flag Administration, or recognized organization(s) representing the vessel flag administration, that issued those certificates International Ship and Port Facility Security Code (ISPS) Notice: • The date of issuance for the vessels international Ship Security Certificate (ISSC), if any • Whether the ISSC, if any, is an initial interim ISSC, subsequent and consecutive interim ISSC, or final ISSC • Declaration that the approved ship security plan, if any, is being implemented • If a subsequent and consecutive interim ISSC, the reasons therefore • The name and 24-hour contact information for the Company's Security Officer • The name of the Flag Administration, or recognized security organization(s) representing the vessel flag administration, that issued the ISSC. USGC will share SANS data with Neptune as part of the Data Framework. Neptune, in turn, will share SANS data with Cerberus. Additional metadata information may be associated with the SANS data by field value validation, entity resolution, correlation and other analytics after ingest of the SANS records. This metadata will be for internal indexing, data quality, records and retention management purposes internal to Data Framework and does not modify the delivered SANS data. The authority to utilize this associated data outside Data Framework will require explicit approval by the Data Framework Working Group, to include the DHS Privacy Office, DHS Civil Rights and Civil Liberties and DHS Office of General Counsel and will be documented in appropriate privacy compliance documentation. When, during the use of the Data Framework, information of operational value is found, users are required to validate the information in the source system before using the information in any mission systems or products. The use of that data will be in the applicable systems of records and will be maintained according to the retention, use, and handling provisions of the respective SORNs for those applicable systems of records.	
4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: USGC retrieves records from the SANS by vessel and then extracts by name, passport number, or other unique identifier. NOAD information maintained in the SANS is not directly retrievable by name or other unique identifier.

4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: USCG will share SANS data with Neptune as part of the Data Framework. Neptune, in turn, will share SANS data with Cerberus.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list:
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	N/A

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: All users will receive training to validate all information of operational value that they may discover with the source system.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: ☐ Yes. Currently, Data Framework makes no disclosures. In the future, Data Framework's dynamic access control will support the capability to account for disclosures. The following information is recorded: the date, user name, and query which captures where the information was shared the access request (with user attributes) and access decision (disclosure) which captures the purpose for which the disclosure was made, and the unique identifier, which captures the source system from which the information came.
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: The Neptune system have been designated... Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☒ High ☐ Undefined Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Click here to enter text.
Date submitted to Component Privacy Office:	Click here to enter a date.
Date submitted to DHS Privacy Office:	Click here to enter a date.
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
Click here to enter text.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Max Binstock**
PCTS Workflow Number:	**1156808**
Date approved by DHS Privacy Office:	February 1, 2018
PTA Expiration Date	February 1, 2019

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

	☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/USCG/PIA-005 United States Coast Guard Maritime Awareness Global Network (MAGNET); DHS/USCG/PIA-006(b) Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS) , and DHS/ALL/PIA-046(b) DHS Data Framework Appendix A.
SORN:	SORN update is required. If covered by existing SORN, please list: DHS/USCG-029 Notice of Arrival and Departure System of Records, July 17, 2017, 82 FR 32715 and DHS/USCG-061 Maritime Awareness Global Network (MAGNET), May 15, 2008, 73 FR 28143

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

DHS Privacy Office finds that this is a privacy sensitive system because the SANS system collects PII from members of the public, DHS employees, contractors working on behalf of DHS, and employees of other federal agencies in order to information to screen individuals and cargo associated with vessels entering or departing U.S. waterways for maritime safety, maritime security, maritime law enforcement, marine environmental protection, and other related purposes.

The SANS data was approved to enter the Data Framework on December 17, 2015. PIA and SORN coverage are provided by:

DHS/USCG/PIA-005; DHS/USCG/PIA-006(b); DHS/ALL/PIA-046(b); DHS/USCG-029; and DHS/USCG-061

DHS PRIV compliance approves this PTA and requires the following compliance updates:

1. SORN Update: DHS/USCG-061 to reflect classified storage location.