Privacy Impact Assessment
for the

Vessel Requirements for Notices of Arrival and Departure and Automatic Identification System Notice of Proposed Rulemaking

November 19, 2008

Contact Point
Mr. Michael Payne
Coast Guard Intelligence (CG-26)
Department of Homeland Security
202-372-2780

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Coast Guard (USCG) is publishing a proposed rule entitled "Vessel Requirements for Notices of Arrival and Departure and Automatic Identification System." The rule proposes to expand the applicability of notice of arrival (NOA) requirements to additional vessels, establish a separate requirement for certain vessels to submit notices of departure (NOD), set forth a mandatory method for electronic submission of NOA and NOD, and modify related reporting content, timeframes, and procedures. This proposed rule would also expand the applicability of Automatic Identification System (AIS) requirements beyond Vessel Traffic Service (VTS) areas to all U.S. navigable waters and require AIS carriage for additional commercial vessels. USCG has conducted this privacy impact assessment because portions of the rule require an expansion of an existing collection of personally identifiable information (PII) and because the system, Ship Arrival Notification System (SANS), which maintains the NOA and NOD information, will maintain the collection of PII.

Introduction

The United States Coast Guard (USCG) is proposing to expand the applicability of notice of arrival and departure (NOAD) and AIS requirements to additional types of commercial vessels. This proposed rule would expand the applicability of NOA requirements to additional vessels, establish a separate requirement for certain vessels to submit NOD, set forth a mandatory method for electronic submission of NOA and NOD, and modify related reporting content, timeframes, and procedures. This proposed rule would also expand the applicability of AIS requirements, beyond VTS areas, to all U.S. navigable waters and require AIS carriage for additional commercial vessels. These proposed changes would improve navigation safety, enhance the Coast Guard's ability to identify and track vessels, heighten USCG's overall maritime domain awareness, help USCG address threats to maritime transportation safety and security and mitigate the possible harm from such threats, and bring consistency between USCG's requirements and those of Customs and Border Protection (CBP).

The proposed rule seeks to accomplish four rule modifications which affect PII: 1) expand the applicability of NOA requirements to additional vessels, 2) establish a separate requirement for certain vessels to submit NOD, 3) set forth a mandatory method for electronic submission of NOA and NOD, and 4) modify related reporting content, timeframes, and procedures. These items are the subject of this PIA. The AIS requirements mentioned above do not involve the collection of PII and therefore this PIA will not discuss them.

1. Expand the applicability of notice of arrival (NOA) requirements to additional vessels

USCG proposes to expand the applicability of the NOAD regulations by changing the minimum size of vessels covered below the current 300 gross tons. USCG seeks to revise the exemption for vessels 300 gross tons or less not carrying certain dangerous cargo(s) (CDCs) so that all commercial vessels coming from a foreign port or place would be required to submit a NOA, regardless of tonnage.

2. Establish a separate requirement for certain vessels to submit notices of departure (NOD)

USCG is proposing to require all covered vessels to submit NOD information in addition to NOA information, currently USCG only requires NOA and CBP requires certain vessels to provide NOD

information. Departure information will better enable USCG to fulfill its mission under 33 U.S.C. 1225--to prevent damage to structures on, in, or adjacent to the navigable waters of the United States, as well as protecting those navigable waters--may differ somewhat from information CBP requires to implement the laws defining its missions. To the extent, however, that USCG and CBP require the same information of vessels, USCG and CBP does not require separate submissions of that information to satisfy our respective regulations in 19 CFR and 33 CFR.

CBP currently requires commercial vessels departing U.S. ports or places bound for foreign ports or places to submit an electronic passenger departure manifest and an electronic crewmember departure manifest, the equivalent of NOD. CBP has adopted the use of USCG's electronic Notice of Arrival and Departure (eNOAD) to eliminate duplicate reporting requirements for filing manifest information See 70 FR 17831 (Apr. 7, 2005). This USCG proposed rule would expand the CBP requirement to encompass USCG's broader scope and mission.

3. *Set forth a mandatory method for electronic submission of NOA and NOD*

USCG currently collects NOA information electronically, by mail, fax, or phone. The primary method of collection of NOA information is the online interface called eNOAD. A vessel operator is required to submit the name of the vessel, crew and passenger lists, and other information (see Question 1.1). USCG uses this information to assess and assign risk to vessels arriving or departing from a U.S. and to identify vessels that may pose a safety or security risk to the United States. USCG uses the information for a myriad of activities to include but is not limited to scheduling of required vessel inspections, establishing safety and security zones.

In the proposed rule, USCG seeks to require NOAs and NODs be submitted via electronic formats found at the National Vessel Movement Center's (NVMC) eNOA website.[1] Mandating electronic submission of NOADs allows the Coast Guard and CBP to process, validate, and screen arrival and departure notices. The CBP's Advance Passenger Information System (APIS) regulations, 19 CFR 4.7b and 4.64, mandated that arrival and departure information be submitted by the electronic system. USCG and CBP consolidated the reporting requirements and provided the public with a "single-window" for transmitting NOA and NOD information. Information received through the eNOAD system is automatically forwarded to USCG and CBP.

4. *Modify related reporting content, timeframes, and procedures*

USCG is proposing a new requirement to mandate times for submitting NODs. This requirement is similar to the time frame for departure notices mandated by CBP in its APIS requirements, 19 CFR 4.7b. For NOAs, for U.S. commercial vessels 300 gross tons or less, arriving from a foreign port, and on a voyage of less than 24 hours, USCG proposes in the NPRM a submission time of 60 minutes prior to departure from the foreign port or place. This proposed rule would also mandate that foreign commercial vessels of 300 gross tons or less that had been required by § 160.210(c) to contact COTPs in the Seventh Coast Guard District would instead submit their NOAs and NODs to the NVMC.

The rule also proposes to require passport country of issuance and passport date of expiration information from everyone onboard who presents a passport--crewmembers and persons in addition to crew. This additional passport information will aid in the detection of person's of interest to the United

[1] http://www.nvmc.uscg.gov

States government by individuals, both foreign and domestic, attempting to enter or depart the United States.

Information Technology Systems

All NOA, including the CBP sea-APIS (Advanced Information System) [2], information is collected through eNOA maintained by USCG. USCG retains the information by vessel in the Ship Arrival Notification System (SANS) which is operated by the National Vessel Movement Center (NVMC) at the USCG's Operations Systems Center (OSC) in Kearneysville, WV. SANS provides a central location for all collected information from vessels scheduled to enter the United States.

Currently Notice of Arrival (NOA) information is received at the NVMC via e-mail, facsimile, telephone, and electronically.[3] SANS makes NOA information available to USCG personnel at the various Captain of the Port zones, at the Intelligence Coordination Center (ICC), at the National Maritime Intelligence Center (NMIC). For port safety issues, NOAD is reviewed to determine whether inspections are required on a particular vessel, or if there is a need to establish safety zones, escorts, boardings and other safety operations. Information is loaded into the Marine Information for Safety and Law Enforcement system MISLE. MISLE is used to store data on marine accidental and deliberate pollution, inspections results and other shipping and port accidents in US territorial waters. It accounts for vessels and other facilities, like port terminals and shipyards as well. SANS matches the vessel with its record in MISLE and attaches the MISLE unique vessel number so arrival information may be pulled into the MISLE arrivals page for ease of access. This allows the Coast Guard user to use one system in lieu of two.

For national security and screening purposes, CBP receives the information directly from eNOA for both its own mission related to APIS and for USCG intelligence analyst to access for USCG mission related intelligence screening.[4] The USCG intelligence analyst correlates the information through other maritime related databases and any information related to possible alerts or lookouts placed into both USCG's Maritime Awareness Global Network (MAGNet) system (73 FR 28143, May 15, 2008) and Customs and Border Protection (CBP) Treasury Enforcement Communication System (TECS) (66 FR 52984, October 18, 2001).

SANS is the repository for NOAD information and has four modules, none of which allow the information to retrieved by a personal identifier:

- SANS –the database is the central repository of SANS data/information and maintained by vessel
- iSANS – internal to USCG, used by NVMC personnel to input and/or validate NOA information received and USCG personnel to view information

---

[2] Original privacy impact assessment published on March 21, 2005 and subsequent updates at www.dhs.gov/privacy; follow links to "Privacy Impact Assessments." Original system of records notice published on August 23, 2007 at 72 FR 48349 with subsequent updates at www.dhs.gov/privacy and follow links to "system of records notices."

[3] Assuming the proposed rule is finalized in its current form, electronic submission will be the only submission method in the future.

[4] See APIS rule at 70 FR 17280 (April 7, 2005). Rule amended at 72 FR 48320 (August 23, 2007).

- SANS-DHS – web based portal for DHS and other Federal users that require a Maritime Domain Awareness (MDA) role and need access of NOA information. This allows the other MDA users the ability to view what they need for their mission without inundating the Coast Guard Captain of the Port with numerous inquiries.
- e-NOA/D – external web based portal for regulated vessels to provide electronic submission of Notice of Arrival/Departure information

USCG extracts NOAD information from SANS to assess risk to vessels arriving or departing from a U.S. port and to identify vessels, as well as, individuals associated with those vessels that may pose a safety or security risk to 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 with conducting maritime safety and security missions in accordance with International and domestic regulations. The data will be retained for trend analysis by other systems and components of the U.S. Coast Guard. SANS will not provide the analysis functionality, but will provide data to other USCG offices responsible for such analysis, as well as to CBP who is also responsible for similar screening and analysis. SANS also provides data directly to CBP for use in the Advanced Passenger Information System.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

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[5]

[5] Classification societies are organizations that establish and apply technical standards in relation to the design, construction and survey of marine related facilities including ships and offshore structures. These standards are issued by the classification society as published rules. A vessel that has been designed and built to the appropriate

- Maritime Mobile Service Identity (MMSI)[6]
- Vessel(s) gross tonnage

Voyage Information

- Arrival information
  - Names of last five foreign ports or places visited
  - Dates of arrival and departure for last five foreign ports or places visited
  - 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
  - For each port or port or place of the United States to be visited, the estimated date and time of arrival
  - For each port or port or place in the United States to be visited, the estimated date and time of departure
  - 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
  - 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 (type[7], 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

---

rules of a society may apply for a Certificate of Classification from that society. The society issues this certificate upon completion of relevant classification surveys.

[6] Maritime Mobile Service Identities are formed of a series of nine digits which are transmitted over the radio path in order to uniquely identify ship stations, ship earth stations, coast stations, coast earth stations, and group calls. These identities are formed in such a way that the identity or part thereof can be used by telephone and telex subscribers connected to the general telecommunications network principally to call ships automatically.

[7] Identification types include Passport, U.S. Alien Registration Card, U.S. Merchant Mariner Document, Foreign Mariner Document, Government Issued Picture ID (Canada), or Government Issued Picture ID (US).

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.

1.2 From whom is information collected?

NOAD information is collected from vessels bound for or departing from United States ports in accordance with Title 33 CFR Part 160 – Ports and Waterways Safety – General Subpart C – Notifications of Arrival, Hazardous Conditions, and CDCs. The owner, operator, master, agent, person in charge vessel submits information for the vessel, including information collected from crews and non-crew members.

1.3 How is the information collected?

NOAD information is submitted to eNOA and entered into SANS at the NVMC via email, facsimile, telephone, and electronically and submitted into CBP APIS. For non electronic submissions, NVMC personnel manually enter the data into SANS.

1.4 Why is the information being collected?

The U.S. Coast Guard collects NOA 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.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The laws and regulations that govern the collection of Notice of Arrival information are Title 33– Navigation and Navigable Waterways Chapter 25 – Ports and Waterways Safety Program, and Title 33 CFR Part 160 – Ports and Waterways Safety – General Subpart C – Notifications of Arrival, Hazardous Conditions, and Certain Dangerous Cargoes. Chapter 25, 33 USC 1223 (a)(5) gives Secretary authority to collect information "necessary for the control of the vessel" and does not preclude security concerns as the basis of that necessity; 33 USC 1226 includes inspections, port and harbor patrols, the establishment of security and safety zones, and the development of contingency plans and procedures to prevent or respond to acts of terrorism. The screening of NOAD data is a process designed to prevent acts of terrorism.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The Rule proposes to expand the coverage of existing NOAD requirements by expanding the covered vessels as well as the amount of PII being collected to include passport information. eNOA, SANS, and CBP APIS will be required to handle additional PII related to additional vessels. In reviewing the amount and type of data, USCG has demonstrated that it needs the information in order to provide the additional safety and security required at the ports. Additionally, in the case of the addition of passport information, this information is already required by CBP under its APIS rule. It has been determined that the passport information is required to provide an effective screening process that minimizes the number of individuals who are required to receive additional screening because their name is the same or similar to someone who is otherwise wanted by the U.S. Government.

Any risks associated with the expanded collection of departure information will be evaluated as comments are received and the final rule for this rulemaking is published. The collection of departure information represents an expansion of the information collected by USCG, the collection is in accord with other DHS operations which collect exit data of individuals leaving the country.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The information listed in Section 1.1 above, NOAD information, is to screen passengers and crew members arriving from foreign travel points and departing the United States to identify those vessels that may pose a risk to the United States. The data will be retained for analysis by other systems and components of USCG and DHS. SANS will not provide the analysis functionality, but will be the data provider.

eNOA information is sent to CBP's TECS system and simultaneously to SANS. Captains of the Port will use SANS data directly for daily operations, including safety analysis and inspections of incoming vessels. USCG conducts vetting activites through CBP's TECS system, as well as its own information sources in USCG's Intelligence Coordination Center (ICC). The only information retained based initially on SANS data is those individuals about whom derogatory information is revealed. All other crew and passenger information vetted by USCG is immediately deleted. Should derogatory information be discovered by USCG either through TECS or USCG's own sources, such alerts and information would be communicated either through USCG's Maritime Awareness Global Network (MAGNet) system, or through the Coast Guard Messaging System (CGMS).[8]

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No. The primary repository for NOAD data is SANS, and SANS does not manipulate or analyze NOAD data in any way. Other USCG systems receive all or some portion of NOAD data (see Question 2.1), and those system may analyze NOAD data as it pertains to law enforcement or intelligence investigations and research, but SANS and the procedures proposed by this rule do not demand new or advanced analytical capabilities. Similarly, CBP APIS and TECS provide analysis of the information to identify matches to terrorist watchlist.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Data is submitted by the vessel owner, operator, agent, charterer, or entity acting for the owner and is retained as is. Electronic submissions must follow an XML schema. SANS personnel validate that the information submitted is complete prior to input into SANS. The regulation establishing the requirement for NOAD information (not the expanded rule that is the subject of this PIA)requires the entity submitting

[8] See www.dhs.gov/privacy for PIAs for MAGNet and the Law Enforcement Intelligence Database (LEIDB), a system used to analyze USCG message traffic.

the NOA to provide the information required for the vessel (vessel centric); information is not collected from individuals.[9]

USCG understands there may be incorrect submissions or a vessel may need to submit updated information after its initial submission. Corrections and updates can be made pursuant to 33 C.F.R. 160.208 et seq. The vessel operator must submit a new NOAD to update any information.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

SANS receives notice of arrival information from vessels intending to arrive in U.S. ports from the vessels' owner, operator, master, agent, or person in charge of the vessel. USCG reviews the information to validate that the vessel operator provided all required information. The accuracy of the information is dependent on the submitter. Submitters are able to provide updates if information is incomplete or they recognize that some information was inaccurate when originally submitted. SANS is the submission repository of NOA information and only validates for completeness of information. SANS interface for users does not currently allow data retrieval by PII, but the interface does have the capability for this function. Retrieving data by PII is a foreseeable option in the future but is not currently available to SANS users.

SANS information is used by the Coast Guard ICC and by Captain of the Port Zone personnel to review vessels entering ports to establish safety and/or security zones and schedule compliance inspections or boardings.

There is a risk that information may be inaccurately submitted. If the error is benign the submitter may resubmit the NOAD information. The previous NOAD information will automatically be updated and replaced. If the error is found to be willful or suspicious in some way, Captains of the Port have the authority to deny entry to a vessel, cargo operations can be restricted or suspended, and civil or criminal penalties may apply. The Captains of the Port may also choose to take no action at all.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

The NARA approved retention schedule states the following:

Master file, which includes data includes details about vessels, reporting party, arrival/departure, date/time group, voyage information, crew, passenger and cargo manifest, previous ports visited, ship security and safety certifications and version control will be deleted when ten years old or no longer needed for reference, whichever is later. This information is maintained in SANS.

Outputs, which include ad-hoc reports generated for local and immediate use to provide a variety of interested parties, for example, Captain of the Port and marine safety offices, sea marshals, Customs and

[9] 33 CFR § 160.208 et seq.

Border Patrol (CBP), Immigration and Customs Enforcement (ICE) - with the necessary information to set up security zones, scheduling boarding and inspections activities, actions for non-compliance with regulations, and other activities in support of CG's mission to provide for safety and security of U.S. ports, will be deleted after five years if it is not a permanent record according to the National Archives and Records Administration

The only NOAD information retained based initially on SANS data is information related to those individuals about whom derogatory information is revealed during the screening process. All other crew and passenger information vetted by USCG is immediately deleted. Should derogatory information be discovered by USCG either through TECS or USCG's own sources, such alerts and information would be communicated either through USCG's Maritime Awareness Global Network (MAGNet) system, or through the Coast Guard Messaging System (CGMS).10 The SANS data is transmitted to the ICC and stored in the CoastWatch Pre-Arrival Processing Program (CP3). SANS data within CP3 is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes. NARA's Request for Records Disposition Authority, dated 5/31/05, Job Number N1-026-05-11.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

SANS is the repository of notice of arrival information which has been retained since its inception. The information has been used for statistical purposes to analyze vessel arrival trends and workload at the National Vessel Movement Center.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Information is regularly shared with CBP. Information may also be shared with Immigration and Customs Enforcement (ICE) and Intelligence and Analysis.

Within DHS, NOA/NOD information sharing is limited to components with an enforcement, security, or analysis mission. This decision was based on the belief that only those mission sets benefit from the use of this data. Individual component employees are provided access rather than the entire component in an effort to limit access to those with a true need to use this information to further component missions.

---

[10] See www.dhs.gov/privacy for PIAs for MAGNet and the Law Enforcement Intelligence Database (LEIDB), a system used to analyze USCG message traffic.

4.2 For each organization, what information is shared and for what purpose?

For each of the DHS components listed in Question 4.1, any NOAD information listed in Question 1.1 will be made available once the agency demonstrates a need to know the information. For each agency the information will be shared for law enforcement and terrorism screening and investigation purposes, however, the purpose of the sharing will generally be defined by the component agencies mission. For example, any sharing with ICE would be for the purpose of immigration or customs law enforcement operations. Similarly, any sharing with CBP will be for the security of the border and in support of CBP mission operations.

4.3 How is the information transmitted or disclosed?

NOAD information submitted electronically is automatically transmitted to U.S. Customs and Border protection via Message Queue to facilitate compliance with CBP's SeaAPIS regulation (5 U.S.C. 301; 19 U.S.C. 66,1431, 1433, 1434, 1624; 2071 note; 46 U.S.C. App. 3, 91 and Section 4.7b also issued under 8 U.S.C. 1221). In addition, CBP and ICE field agents are able to have access to SANS data via a web interface

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

As with any system that contains PII, there is the risk that information may be obtained by someone without an official "need to know" or that information obtained from the system could intentionally or inadvertently be further disseminated outside of the Federal government without consent. Within the Department of Homeland Security, sharing of SANS data is limited to components with law enforcement, security, and/or intelligence function and an official "need to know" the information. Individual component employees are provided access rather than the entire agency in an effort to limit access to those with a true need to use this information to further agency missions. These employees are briefed on how to access and use data within the system. Additionally, Coast Guard employees who utilize SANS and PII must complete annual Privacy Awareness training and are encouraged to attend FOIA/Privacy Act training on a semi-annual basis. These limitations should mitigate the risk of potential misuse of this data.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Currently SANS data is shared with the CDC, DOJ, Federal Bureau of Investigation (FBI), U. S. Navy, U.S. Northern Command (NORTHCOM) and U.S. Southern Command (SOUTHCOM), and other

Federal agencies involved in law enforcement and intelligence. The Coast Guard also anticipates shares certain SANS data with the Saint Lawrence Seaway Development Corporation, a government-owned corporation overseen by the Department of Transportation. NOA/NOD information sharing is normally limited to agencies with a law enforcement, intelligence or maritime safety/security analysis mission. This decision was based on the belief that only those mission sets benefit from the use of this data. However, there exists the potential that SANS data could be shared with other external Federal, state, local, foreign, or private sector partners so long as legal authority to do so exists and proper safeguards are in place. For example, SANS data could be shared with the National Transportation Safety Board as part of an ongoing investigation by that board. Information is always collected and shared for the purpose with which it was collected, that is, to maintain notice of arrival and notice of departure information for the DHS and the USCG who is responsible for maritime safety, maritime security, maritime law enforcement, marine environmental protection, and other related purposes. Specific purposes for sharing with external agencies are described in Question 5.2 below.

Individual agency employees with technical expertise and a "need to know" are provided access rather than the entire agency in an effort to limit access to those with a true need to use this information to further agency missions. In some cases, a Memorandum of Agreement or similar document with a specific point of contact within the agency will be executed to provide the partner with limited information and to ensure there is a restriction in place to prevent unauthorized dissemination. These limitations should mitigate the risk of potential misuse of this data.

5.2 What information is shared and for what purpose?

All or only some of the data fields listed in Section 1.1 above may be provided for a variety of purposes either on a "one-time" or routine basis to Federal, state, local, foreign, or private sector entities so long as not prohibited by existing statute, regulation, or policy.

The following is a list of the primary purposes of sharing SANS data externally outside of DHS:

- Law enforcement actions in coordination with DOJ and FBI, among others
- Counterintelligence operations within DHS and in cooperation with other Federal agencies
- Port security and law enforcement actions in coordination with State and local authorities
- Regulatory or other associated public health or safety action with other Federal agencies (CDC, for example) and State and local authorities

Based on the need to know information and the nature of the request, agencies receiving NOAD information may or may not receive PII. For example, port safety operations or regulatory actions directed at vessel safety may require less PII than a law enforcement or counterintelligence action which will require the sharing of a greater amount of PII.

5.3 How is the information transmitted or disclosed?

Agencies receive NOAD data through direct user access to SANS. Information is disclosed via a web interface requiring a user logon name and password, and access is read-only.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes. when the Coast Guard provides access to SANS to any partner, a Memorandum of Agreement/Understanding or similar document identifying specific points of contact within each organization will be executed that reflects the scope of the information that will be shared and to ensure there is a restriction in place to prevent unauthorized dissemination by the receiving party. Further, individual users are required to sign "user agreements." The user agreement is intended to provide a guarantee that users will only log onto and use SANS data for agency purposes in accordance with applicable agency guidelines and rules.

5.5 How is the shared information secured by the recipient?

The user agrees to handle the data as For Official Use Only (FOUO), shared with only individuals having a need to know. This information is not to be provided to any third parties without the express authorization of the U. S. Coast Guard.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Users are given telephone training on the use and restrictions of the information contained in the system. Agencies outside DHS have their own scheduled training relating to Privacy Act and FOIA concerns to supplement the training provided when new users initially access the system.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

As with any system that contains PII, there is the risk that information may be obtained by someone without an official "need to know" or that information obtained from the system could intentionally or inadvertently be further disseminated outside of the Federal government without consent from the individual. This risk is mitigated by the fact that potential receiving entities (described in Section 5.2 above) sign an MOA/MOU, and individuals employed by these entities sign a user agreement. In some cases, a receiving entity may be required to sign a DHS form Non-Disclosure Agreement that could subject the receiving party to civil and criminal penalty if the data is used in an unauthorized manner. At a minimum, any user of SANS and any information shared from SANS must be shared with an agency who has the authority to view such information and has a need to know the information.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Information in SANS is retrieved by ship name, ship ID number, state, port, or Captain of the Port Zone. Information is not retrieved by a personal identifier. Other vetting, screening, or analytical systems using SANS data may and will retrieve by personal identifier as required by their operational mandates.

In order to provide greater transparency to the traveling public, DHS is publishing a SORN for NOAD information which details the scope, sharing, and information access procedures for NOAD data at USCG. In addition to the new SORN, USCG has previously provided notice of the use of NOAD information in Marine Information for Safety and Law Enforcement (MISLE, DOT/CG 679, April 22, 2002, 67 FR 19612) and the Maritime Awareness Global Network (MAGNet, DHS/USCG-061, May 15, 2008, 73 FR 28143).

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Providing the NOA information is a regulatory requirement imposed by the U.S. Coast Guard pursuant to lawful authority to regulate entry into the United States. Individuals do have the right to decline to provide this information, although failure to provide complete information may result in a denial or delay of entry.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Once information is provided, individuals are not able to consent to particular uses of the information. Information required by 33 CFR Part 160 (the Coast Guard's Ports and Waterways Safety regulations), Table 160.206 is submitted by vessels (owner, operator, master, agent, or person in charge) for arriving in and departing to foreign from US ports.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

There is a risk that individuals will not know about the particular collection of the NOAD information. While existing System of Records Notice provide notice and existing published Federal

Regulations (33 CFR Part 160), DHS decided to provide additional notice specific to the NOAD information. This increases the transparency of the program.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals may submit requests for Information to the U.S. Coast Guard based on the Privacy Act and Freedom of Information Act. The Coast Guard's Privacy Act and Freedom of Information Act office is located a Commandant (CG-611), U.S. Coast Guard, 2100 2nd Street S.W., Washington, DC 20593. The individual will need to identify the vessel and voyage (destination U.S. port) they were embarked on so that vessel's record may be retrieved and reviewed.

7.2 What are the procedures for correcting erroneous information?

The vessel owner, operator, agent, charterer, or entity acting for the owner who is responsible for collecting the notice of arrival information for submission to the Coast Guard can submit updates to the Coast Guard to correct previously reported information. The submitting individual could be notified of erroneous information in a variety of ways (i.e. verbally by an individual crewmember, etc.), however, USCG does not check PII to insure what is submitted is correct; if an individual finds that they have provided erroneous information to a submitter, the submitter would likely submit an update to their previous (original or subsequent update(s)) submission. Additionally, an individual may seek access to his/her information by contacting the individuals noted above in 7.1 to determine whether USCG has retained a copy of his/her NOAD.

7.3 How are individuals notified of the procedures for correcting their information?

Information is not collected from individuals, rather it is submitted by the entity responsible for the vessels' compliance with Coast Guard and CBP rules/regulations. Information about crew is collected by the entity controlling the vessel to insure those on board are licensed/qualified to be employed on the vessel. Information about persons other than crew is collected by the entity controlling the vessel to insure those on board are entitled to enter a destination port/country.

7.4 If no redress is provided, are alternatives available?

Information to be corrected or previously filed notices to be completed are submitted as an update to a previously provided NOAD by the entity responsible for the vessels' compliance with Coast Guard and CBP rules/regulations. An individual that believes information provided to the vessel was incorrectly transmitted by the vessel may file a Freedom of Information Act request identifying the vessel and voyage (destination U.S. port) they were embarked on so that vessel's record may be retrieved and reviewed. Once

the data is retrieved, there are methods to correct the information, although any beneficial Government use of the data may have lapsed by that point. Whether or not it would be prudent to correct the information would depend on the circumstances at the time of the request.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and if access, correction and redress rights are not provided please explain why not.

An individual may appeal to the Coast Guard's Privacy Act and Freedom of Information Act office for access to SANS data that identifies them. Once the data is retrieved, there are methods to correct the information, although any beneficial Government use of the data may have lapsed by that point. Whether or not it would be necessary to correct the information would depend on the circumstances at the time of the request.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

National Vessel Movement Center (NVMC) Watchstanders and IT specialists have general access to the system (Read Write Update Delete.) USCG intelligence analysts and field enforcement personnel have limited access (Read Only). Analysts and Enforcement officials from other Federal agencies, listed above, have limited access (Read Only.)

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

A number of contractors have access to SANS, including from the Coast Guard, DHS and other Federal agencies under a variety of contract vehicles. Contractors providing IT services to the system including creation of the software, maintenance of the system, and data entry when public submissions require human intervention for data integrity are located at the Coast Guard Operations System Center in Kearneysville, WV, a government owned, contractor operated facility.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Write access (i.e. the ability to manipulate or move information) is only granted to National Vessel Movement Center personnel. Read access (i.e. the ability to read the data) is granted to all users.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Coast Guard users of SANS are required to register as a user completing a User Access Request Form which is reviewed prior to access being granted. Once authorized, the user can then access the system using a username and password. External users of SANS data are required to complete a User Access Authorization/ Revocation form, in accordance with Ship Arrival Notification System (SANS) User Account Management Procedures for External Agencies. Their access need is verified and authorized by an 'Agency' point of contact, if one is established, or by a Coast Guard representative having cognizance of the individuals' need if one has not been established at their own agency.

SANS incorporates variety of security measures to insure data integrity. Public facing system components employ Secure Sockets Layer (SSL) and are behind a firewall. System components on the Coast Guard Data Network are protected by two firewalls. Systems employ user authentication consisting of user name and complex password, which is not stored as clear text in the database (MD5 hash strings). Forgotten passwords have to be changed. Access is restricted by Internet Protocol security (IPsec) to an IP address or a range of IP addresses. SANS users external to the Coast Guard's National Vessel Movement Center only have read access.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Controls are in place to restrict users to read only access to the data. Users outside of the USCG are reviewed by representatives from their respective agencies for access need prior to establishing read access and accesses are tallied.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Timestamps are noted when records are input and updated; transaction logs may be reviewed to see actions taken. Users of the system are prompted with security and privacy declarations when accessing the system and use user names and passwords to gain access. Audit logs can be audited to find out who inputted and updated the data. The system itself cannot judge whether records were inputted properly or not.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Users of SANS are provided guidance when individual accounts are established. Users must complete the USCG's Privacy Awareness training in addition to the unit's Freedom of Information Act and Privacy Act training which is provided on an annual basis.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

SANS completed Certification and Accreditation in August 2006.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The various entities using SANS data use it in conjunction with their law enforcement, maritime safety and security responsibilities in the performance of their duties.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

USCG built the system from the ground up.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Controls are currently in place to restrict access to data. Users outside of the USCG are screened by representatives from their respective agencies. Physical access to the system hardware is restricted. Data submitted electronically is validated by humans prior to being inserted.

9.3 What design choices were made to enhance privacy?

Information collected is not made available to the public. SSL and IPSec are used to limit access to the system.

Responsible Officials

Mr. David Roberts, Privacy Officer, Commandant , CG-611, United States Coast Guard Headquarters, 2100 2nd Street, SW, Washington, D.C. 20593-0001

Mr. Michael Payne, System Manager for SANS, Commandant, CG-26, United States Coast Guard Headquarters, 2100 2nd Street, SW, Washington, D.C. 20593-0001

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security