Privacy Impact Assessment Update
for the
Vessel Requirements for the Notice of Arrival and Departure (NOAD) and Automatic Identification System (AIS) Rulemaking

DHS/USCG/PIA-006(b)

April 28, 2015

Contact Point

Mr. Nicholas Andersen
Coast Guard Intelligence (CG-26)
Department of Homeland Security
202-372-2780

Reviewing Official

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
202-343-1717

vessel to recognize other vessels around it (on a visual display) that also have AIS. This aids in situational awareness and collision avoidance. The MMSI is assigned by a vessel's Flag Administration. For U.S. commercial vessels, the Federal Communications Commission (FCC) assigns MMSI numbers.

The two other fields – (4) last port of departure, and (5) arrival and departure date for last port of departure – are currently required[8] but the Coast Guard is expanding to capture the last port of departure (whether foreign or domestic), the arrival and departure date, and the last 5 foreign ports or places visited and the dates of arrival and departure for those five visits. In addition, the final rule removes the submission of a consolidated NOA and the three ports-to-be-visited fields associated with those submissions.

Using Maritime Transportation Security Act of 2002 (MTSA) authority,[9] this final rule also expands AIS requirements[10] beyond Vessel Traffic Service (VTS) areas to all U.S. navigable waters, removes an exception for passenger and fishing vessels from the applicability threshold for commercial vessels 65 feet or more in length, and expands applicability to certain dredges and vessels moving certain dangerous cargo (CDC) or flammable or combustible liquid cargo in bulk. Unlike NOA, these AIS requirements do not involve the collection of PII. These requirements for additional commercial vessels to install and use AIS are consistent with statutory requirements and in limited cases rely on the Secretary's discretionary authority. The Coast Guard has identified dredges as the only vessels that will be required to install AIS based solely on the Secretary's discretionary authority to decide which vessels need AIS for safe navigation purposes.[11] The final rule will enhance our overall maritime domain awareness (MDA) by allowing the Coast Guard to retrieve more AIS and NOA data to meet the safety and security objectives of the MTSA and the PWSA.

Reason for the PIA Update

All NOA information is collected through eNOAD. 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.

Telecommunication Union (ITU), adopted by the International Maritime Organization (IMO), that—
(1) Provides vessel information, including the vessel's identity, type, position, course, speed, navigational status, and other safety-related information automatically to appropriately equipped shore stations, other ships, and aircraft;
(2) Receives automatically such information from similarly fitted ships, monitors, and tracks ships; and
(3) Exchanges data with shore-based facilities.

[8] *See* 33 CFR 160.206, Table 160.206(2)(i) and (ii).
[9] MTSA (46 U.S.C. § 70114) specifies which vessels must carry AIS.
[10] Current AIS requirements are found in 33 CFR 164.46.
[11] 46 U.S.C. § 70114(a)(1)(D).

Uses of the System and the Information

The uses of PII have not changed with this update, and no new privacy risks have been identified. New fields added pursuant to the new regulation do not contain PII.

Retention

The retention schedules have not changed.[14]

Internal Sharing and Disclosure

The internal sharing and disclosure have not changed with this update, and no new privacy risks have been identified.

External Sharing and Disclosure

The external sharing and disclosure have not changed with this update, and no new privacy risks have been identified.

Notice

To provide extensive notice of the expanded collection and revised rulemaking, Coast Guard provided a four month comment period for the proposed rule. Coast Guard received 91 written submissions, and 27 persons made oral statements at Coast Guard public meetings. There were approximately 475 comments in response to the NPRM.

Information in SANS is retrieved by Vessel Name, Vessel ID Number, State, Port, or Captain of the Port Zone (geographical location), and therefore is not covered under the Privacy Act because information is not retrieved by a personal identifier. As outlined in the original PIA, because SANS data is used by other IT systems in order to vet, screen, or analyze information on individuals, Coast Guard nonetheless published a SORN for Notice of Arrival and Departure information that details the scope, sharing, and information access procedures for NOAD data at USCG.[15] In addition to the NOAD SORN, USCG has previously provided notice of the use of NOAD information in the Marine Information for Safety and Law Enforcement and the Maritime Awareness Global Network SORNs.[16]

Individual Access, Redress, and Correction

Access, redress, and correction have not changed with this update, and no new privacy risks have been identified.

---

[14] NARA's Request for Records Disposition Authority, dated 5.31.05, job Number N1-026-05-11.
[15] DHS/USCG-029 Notice of Arrival and Departure SORN 79 FR 64812 (October 31, 2014).
[16] *See* DHS/USCG-013 Marine Information for Safety and Law Enforcement SORN 74 FR 30305 (June 25, 2009) and DHS/USCG-061 Maritime Awareness Global Network SORN 73 FR 28143 (May 15, 2008).

Privacy Impact Assessment Update
for the

Vessel Requirements for Notices of Arrival and Departure and Automatic Identification System to add the Notice of Arrival on the Outer Continental Shelf

June 3, 2009

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

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Privacy Impact Analysis

In each of the below sections, consider how the system has changed and what impact it has on the below fair information principles. In some cases, there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

The proposed rule, once final, would require vessel owners and operators of floating facilities, mobile offshore drilling units (MODU's), and vessels to submit an advance notice of arrival electronically to the NVMC prior to engaging in OCS activities. This requirement would require a change in the previously approved OMB Collection 1625-0100 because it expands the NOA requirement to include units engaging in OCS activities. The respondents are vessel owners and operators who arrive on the OCS from foreign ports and engage in OCS activities. The proposed rule would increase the number of respondents in this OMB-approved collection by no more than 144 respondents. OCS units such as MODU's and floating production facilities may stay on the OCS for long periods, such as a year or more, so the Coast Guard does not expect these units to have more than one NOA submittal per year.

The NPRM proposes a collection of the following information for each individual onboard a vessel that intends to engage in OCS activities:

i. Full name;

ii. Date of birth;

iii. Nationality;

iv. Passport number or marine documentation number (type of identification and number);

v. Position or duties of the mariner; and

vi. Name of the port, or place, and country where the individual embarked.

Uses of the System and the Information

The uses of the personally identifiable information have not changed with this update, and no new privacy risks have been identified.

Retention

The retention schedules have not changed. NARA's Request for Records Disposition Authority, dated 5.31.05, job Number N1-026-05-11.

Internal Sharing and Disclosure

The internal sharing and disclosure have not changed with this update, and no new privacy risks have been identified.

External Sharing and Disclosure

The external sharing and disclosure have not changed with this update, and no new privacy risks have been identified.

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

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

- 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

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.

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.

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.

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.

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

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.

8.8 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.