Version Number: 01-2015

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)

Privacy Threshold Analysis
For
Search and Rescue Satellite-Aided Tracking (SARSAT)
NOAA5023

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Search and Rescue Satellite-Aided Tracking (SARSAT)

Unique Project Identifier: 006-48-01-15-01-3208-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
NOAA is the lead agency in the United States (U.S.) for the Search and Rescue Satellite-Aided Tracking (SARSAT) program and represents the United States to the international COSPAS-SARSAT program. SARSAT relays distress signals, via satellite, from emergency beacons carried by aviators, mariners and land based users to search and rescue authorities.
NOAA maintains a national registry of U.S.-coded 406 MHz emergency beacon registration information that is referred to as the "Registration Database," or RGDB. This registry allows 406 MHz emergency beacon users to comply with registration requirements in Title 47, Parts 80, 87 and 95, of the U.S. Code of Federal Regulations (47CFR). The RGDB also allows beacon users to comply with the requirements of the International Civil Aviation Organization (ICAO), which focuses on aviation safety and security, in compatibility with the quality of the environment, and the International Maritime Organization (IMO), a specialized agency of the United Nations, which is responsible for measures to improve the safety and security of international shipping and to prevent marine pollution from ships. It also plays a role in legal liability and compensation issues and the facilitation of international maritime traffic.

U.S. beacon owners are required by 47 CFR to register all U.S.-coded 406 MHz beacons with NOAA before installation and/or use. Each individual 406 MHz emergency beacon contains a unique hexadecimal identification code/Unique Identifying Number (UIN). When the beacon is activated within the U.S. areas of responsibility, the beacon UIN is transmitted digitally and relayed via satellite to the U.S. Mission Control Center (USMCC). The USMCC decodes the beacon UIN, links it to the RGDB, and then appends the registration information on the distress alert message relayed to the appropriate Rescue Coordination Center (RCC) or appropriate Mission Control Center (MCC).

The information contained in the RGDB provides the RCC and MCC with the identity of the individual(s) they are searching for; contact information so that the RCC can determine whether

or not the beacon has been activated as the result of an actual emergency; and information about the vessel or aircraft. The registration information allows the RCC and MCC to resolve a distress case by telephone instead of wasting valuable resources responding to false alerts. Failure to register, re-register (as required every two years), or notify NOAA of any changes to the status of one's 406 MHz beacon could result in penalties and/or fines being issued under federal law.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system.

____ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X_ This is an existing information system in which changes do not create new privacy risks.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
_X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Search and Rescue Satellite-Aided Tracking (SARSAT) NOAA5023 and as a consequence, a PIA was completed, and approved 9/02/2014.

____ I certify the criteria implied by the questions above **do not apply** to the Search and Rescue Satellite-Aided Tracking (SARSAT) NOAA5023 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Brian Little

Signature of ISSO or SO: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=LITTLE.BRIAN.WILLIAM.1365841230 Date: 2015.08.21 09:26:26 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Nancy DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=DEFRANCESCO.NANCY.A.1377370917 Date: 2015.08.24 15:32:32 -04'00' Date: 08/24/2015

Name of Authorizing Official (AO):

Mark Paese

Signature of AO: Mark S. Paese Date: 8/27/15

Name of Bureau Chief Privacy Officer (BCPO):

Robert Swisher

Signature of BCPO: SWISHER.DONALD.ROBERT.1376511460 Digitally signed by SWISHER.DONALD.ROBERT.1376511460 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.ROBERT.1376511460 Date: 2015.09.02 13:02:16 -04'00' Date: _____