

**U.S. Department of Commerce  
NOAA**



**Privacy Impact Assessment  
For  
Search and Rescue Satellite-Aided Tracking (SARSAT)  
NOAA5023**

Reviewed by: BRABSON.SARAH.1365710488, Bureau Privacy Officer or Designee  
Digitally signed by BRABSON.SARAH.1365710488  
DN: cn=US, o=U.S. Government, ou=DoD, ou=PKI,  
ou=OFFER, cn=BRABSON.SARAH.1365710488  
Date: 2014.02.11 14:36:19 -05'00'  
488

Approved by: [Signature], DOC Chief Privacy Officer

Date approved: 2/2/2014

**U.S. Department of Commerce Privacy Impact Assessment  
NOAA / Search and Rescue Satellite-Aided Tracking (SARSAT)**

**NOAA5023**

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

**Introduction: System Description**

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 Identification 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. Information may be provided to or received from international registration authorities to ensure registration information resides in the correct database based on the country code of the beacon or the mailing address of the beacon owner. 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.

As of April 17, 2008 the SARSAT System of Records Notice was published in the Federal Register, Vol. 73, No. 75 / Thursday, April 17, 2008.

This is a high impact system. The last ATO was signed on 6/14/2013 and the next one is due 6/14/2014.

**Section 1: Information in the System**

1.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. Check all that apply.

<b>Identifying Numbers (IN)</b>					
a. Social Security	<input type="checkbox"/>	e. Alien Registration	<input type="checkbox"/>	i. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Transaction	<input type="checkbox"/>
c. Employee ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Vehicle Identifier	<input checked="" type="checkbox"/>
d. File/Case ID	<input type="checkbox"/>	h. Credit Card	<input type="checkbox"/>	l. Employer ID Number	<input type="checkbox"/>
m. Other identifying numbers (specify):					

<b>General Personal Data (GPD)</b>					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>
s. Other					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)					

1.2 Indicate sources of the PII/BII in the system. Check all that apply.

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify):					

Non-government Sources					
Public Organizations	X	Public Media, Internet		Private Sector	X
Commercial Data Brokers					
Other (specify):					

**Section 2: Purpose of the System**

2.1 Indicate why the PII/BII in the system is being collected, maintained, or disseminated. Check all that apply.

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
Other (specify): Search and Rescue	X		

**Section 3: Use of the System**

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in Section 1.1 of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify).

The information that is collected is used by Rescue Coordination Centers and Mission Control Centers to assist in carrying out their mission of rescue coordination and false alert abatement. A secondary use of the information is to contact beacon owners every two years to remind them to update their registration information in the RGDB.

The intended use of the information is to provide emergency beacon owner contact information to Rescue Coordination Centers to validate the need for rescue team deployment, coordinate rescue efforts and provide early identification of false alerts.

Information may be provided to or received from international registration authorities to ensure registration information resides in the correct database based on the country code of the beacon or the mailing address of the beacon owner.

The information will be shared with Mission Control Centers and Rescue Coordination Centers in the U.S. that are operated by the U.S. Air Force and the U.S. Coast Guard. If the emergency beacon is activated overseas, the information would be shared with Rescue Coordination Centers and Mission Control Centers of other countries.

Beacon owners do not have the opportunity to decline to provide the information or consent to particular uses of the information. Beacon owners are required to provide this information under 47 CFR Parts 80, 87 and 95.

All information is provided by the beacon owner. Owners are able to update, change and

remove data at any time via the password-protected Web site or by sending hard copy notification to NOAA-SARSAT.

The PII/BII identified in Section 1.1 of this document is in reference to a member of the public.

Authority to collect this information from the public through August 31, 2014, was approved by the Office of Management and Budget (OMB Control Number 0648-0295).

**Section 4: Information Sharing**

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

Recipient	How Information will be Shared			
	Case-by-Case	Bulk Transfer	Direct Access	Other (specify)
Within the bureau				
DOC bureaus				
Federal agencies	X			
State, local, tribal gov't agencies				
Public				
Private sector				
Foreign governments	X			
Foreign entities	X			
Other (specify):				

The PII/BII in the system will not be shared.

**Section 5: Notice and Consent**

5.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. Check all that apply.

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 6.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Beacon owners do not have the opportunity to decline to provide the information or consent to particular uses of the information. Beacon owners are required to provide this information under 47CFR Parts 80, 87 and 95.

--	--	--

5.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Beacon owners do not have the opportunity to decline to provide the information or consent to particular uses of the information, because this information is used for life saving Search and Rescue activities.

5.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: All information is provided by the beacon owner. Owners are able to update, change and remove data at any time via the password protected Web site or by sending hard copy notification to NOAA-SARSAT.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

**Section 6: Administrative and Technological Controls**

6.1 Indicate the administrative and technological controls for the system. Check all that apply. Also see Appendix A, a checklist for more specific controls. This appendix will be removed after the PIA is approved.

	All users signed a confidentiality agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff received training on privacy and confidentiality policies and practices.
X	Access to PII/BII is restricted to authorized personnel only.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: 6/14/2013
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST 800-122 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). See Appendix A.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Other (specify):

**Section 7: Privacy Act**

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	<p>Yes, this system is covered by an existing system of records notice.          Provide the system name and number: As of April 17, 2008 the SARSAT System of Records Notice was published in the Federal Register, Vol. 73, No. 75 / Thursday, April 17, 2008 – in process of being updated, <i>with inclusion of medical information and physical characteristics as data elements which are not on the form, but will be entered into the database when received. Until the updated SORN is published, such information received will not be entered into the database.</i></p>
	Yes, a system of records notice has been submitted to the Department for approval on <u>(date)</u> .
	No, a system of records is not being created.

**Section 8: Retention of Information**

8.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. Check all that apply.

X	<p>There is an approved record control schedule.          Provide the name of the record control schedule: The records are scheduled in the NOAA Records Disposition Handbook, item 1404-02, which provides for a 50-year retention of the electronic registration records. The schedule was approved by the <u>National Archives and Records Administration (NARA)</u> under Job Number N1-370-03-10.</p>
	<p>No, there is not an approved record control schedule.          Provide the stage in which the project is in developing and submitting a records control schedule:</p>
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation: