U. S. Department of Commerce
National Oceanic and Atmospheric Administration

SARSAT
NOAA 5023

PRIVACY IMPACT ASSESSMENT

February 22, 2012

Prepared by: Mr. Stephen Roark, SARSAT Program Analyst

Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

SARSAT

Unique Project Identifier: 006-000320800 00-48-01-15-02-00

Project 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 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).

The information contained in the RGDB provides the RCC 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 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.

*Cosmicheskaya Systyema Poiska Aariynyich Sudov
Which loosely translates into: "The Space System for the Search of Vessels in Distress"

This PIA has been developed to comply with the requirement in Section 208 of the E-Government Act of 2002 (44 U.S.C. 3501 note) and the Department of Commerce IT Privacy Policy.

1. What information is to be collected (e.g., nature and source)?

Personally identifiable information (PII) collected by the RGDB:

Beacon Unique Identifier Number (UIN); beacon category, model, and manufacturer; owner name, mailing address, e-mail address; home, work, cellular, fax, and other telephone numbers; and the name and telephone number of primary/alternate 24-hour emergency contact.

Non-personal information that is also collected includes (arranged by type of beacon application/registration):

Emergency Position-Indicating Radio Beacons (EPIRB) and Ship Security Alerting System (SSAS) beacon registrations - vessel information including usage, type, name, color, survival and radio equipment, vessel telephone numbers with call sign, Inmarsat global message system number, cellular and Mobile Maritime Service Identification (MMSI) number, federal/state registration number, length, capacity and homeport.

Emergency Locator Transmitter (ELT) registrations - aircraft information including registration (tail) number, type, manufacturer, model, color, seating capacity, radio equipment, survival equipment and principal airport.

Personal Locator Beacon (PLB) registrations - use data including general usage, specific usage and type.

This information is entered into the RGDB by the beacon owner via a password protected Web site or by sending a hard copy directly to NOAA-SARSAT.

2. Why is the information being collected (e.g., to determine eligibility)?

The information that is collected is used by Rescue Coordination 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.

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).

3. What is the intended use of the information (e.g., to verify existing data)?

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.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

The information will be shared with 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 of other countries. Other reasons may be found in the SARSAT Privacy Act System of Records Notice, last published in the Federal Register on March 30, 2011.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how may individuals grant consent?

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.

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.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls

National Institute of Standards and Technology Special Publication 800-53 (NIST-800-SP 53), Recommended Security Controls for Federal Information Systems and Organizations, rev. 3, August 2009, identifies security controls for high, low, and moderate impact systems. The SARSAT Registration Database is categorized as High impact, and its security controls are evaluated every three years to ensure compliance with operational, management, and technical controls established by the Department of Commerce. The current Authorization to Operate (ATO) under the Federal Information Security Management Act of 2002 (FISMA) was issued on June 14, 2011. Continuous monitoring tests are conducted to ensure controls remain in place and reviews, updates, and adjustments are completed where appropriate, e.g., system processes and procedures, system policies, risk assessment, and contingency testing.

Operational Controls

The SARSAT Beacon Registration Database computer systems are located at NOAA's USMCC facility in Suitland, Maryland. The facility has a uniformed guard service and the USMCC has key card controls limiting access to all production servers. Access to the facility and the database is strictly limited to personnel who require access to carry out their official duties.

Technical Controls:

Access controls are implemented on the production equipment through the use of system usernames and passwords as well as database usernames and passwords. Access logs are maintained and reviewed for any improprieties. The entire database is covered by an intrusion detection system that monitors and detects any attempt to access or hack any part of the database. Communications with Web users are via Secure Sockets Layer (SSL) protocol to ensure safe transmission of information. In addition to the SSL, information that is sent to the database is transferred through two firewalls prior to storage and use in the USMCC. The computerized database is backed up daily and the information is housed using Redundant Array of Independent Disks (RAID) architecture to minimize loss of data. In addition to redundant disk storage, every month the data is backed up to tape and stored in a safe at an offsite location.

Access to the database is limited to those individuals who require it to carry out their official duties. Those who have access are granted it in accordance with the approved routine uses published in the Privacy Act system of records notice (SORN) for these records. Personnel with access to the system are instructed on the confidential nature of this information and the requirement to protect it from disclosure.

Data Extract Log and Verify

All data extracts require E-authentication and IP addresses, usernames and passwords are logged. All data extract logs are required to be retained for a 50 year period. The logging process is automated. There is no current monitoring of the logs

This system underwent a rigorous Information Technology (IT) security review. Based on the successful outcome of that certification and accreditation process, the system (NOAA 5023) was authorized to start operations.

A Security Certification and Accreditation (C&A) in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) was completed for this system on June 14, 2011. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

Yes. The original SARSAT System of Records Notice was published in the Federal Register on April 17, 2008, effective June 6, 2008. An update was published on March 30, 2011.

8. Are these records covered by an approved records control schedule?

Yes, 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 National Archives and Records Administration (NARA) under Job Number N1-370-03-10.

Program Contact:

Stephen Roark
SARSAT Program Analyst
Ph: (301) 817-3896
stephen.roark@noaa.gov