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

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

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NESDIS/SARSAT

Unique Project Identifier: NOAA5023

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: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The SARSAT System includes the United States Mission Control Center (USMCC) and satellite antenna and data processing systems called Local User Terminals (LUTs). The International Cospas-Sarsat Programme mission is to provide accurate, timely, and reliable distress alert and location data to help search and rescue (SAR) authorities assist persons in distress.

SARSAT is a geographically distributed system that consists of the USMCC, five LUT locations, and components at the NOAA Center for Weather and Climate Predication (NCWCP). The primary USMCC is physically located in Suitland, Maryland, along with one of the LUT locations. The alternate processing site for the USMCC is located in Wallops, Virginia. Components at the NCWCP in College Park, Maryland are used to remotely control the primary or secondary USMCCs in the event that physical access to either building is not available. The additional four LUT locations are geographically dispersed to collect satellite data throughout the United States and its territories.

The USMCC and its associated LUTs are part of a complex international program and network called COSPAS-SARSAT. "Cosmicheskaya Sisteyma Poiska Avariynich Sudov" (COSPAS) is Russian for "Space System for Search of Vessels in Distress." SAR instruments are flown on NOAA polar-orbiting and geostationary satellites; the Russian Nadezhda series of polar-orbiting satellites; the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) Meteorological Operational Satellite (METOP) series of polar-orbiting satellites and the Meteosat Second Generation (MSG) series of geostationary satellites; and the Indian National (INSAT) series of geostationary satellites. These instruments are capable of detecting signals transmitted from four types of emergency beacons referred to as Emergency Locator Transmitters (ELTs), Emergency Position-Indicating Radio Beacons (EPIRBs), Personal Locator Beacons (PLBs), and Ship Security Alerting System (SSAS) beacons. After receipt of ELT, EPIRB, PLB, or SSAS signals by the satellite, the satellite relays those signals to the LUTs.

Address the following elements:

Whether it is a general support system, major application, or other type of system

NOAA5023 (SARSAT) is a major application.

a) *System location*

NOAA5023 is physically located in Suitland, MD with an alternate processing site in Wallops, VA. In addition to the two processing sites, NOAA5023 maintains a remote control/monitoring facility in College Park, MD as well as ground stations (Local User Terminals [LUTs]) in Suitland, MD; Miami, FL; Wahiawa, HI; Vandenberg AFB, CA; Fairbanks, AK; Holloman AFB, NM; and Andersen AFB, Guam.

b) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

NOAA SARSAT interconnects with the following external information systems:

- U.S. RCCs (U.S. Coast Guard and U.S. Air Force)
- Foreign MCCs (complete list provided in the PIA Section 6.3)
- Foreign Search and Rescue Points of Contact (SPOC)
- Federal Aviation Administration (FAA) – SARSAT uses FAA's National Airspace Data Interchange Network (NADIN) as a message transport provider to communicate with U.S. and foreign MCCs and RCCs.
- USAF Personnel Recovery Command and Control (PRC2) – USAF maintains the DoD's beacon registration database and provides NOAA SARSAT with a real-time listing of the DoD's registered beacons. No privacy data is sent to or received from the USAF via this interconnection.
- NASA Search and Rescue Laboratory (SARLab) – NASA SARLab maintains a test ground station and sends test/development data to NOAA SARSAT's development environment. No operational or privacy data is sent to or received from NASA via this interconnection.
- U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (UASMDC/ARSTRAT) Friendly Force Tracking Testbed (FFTT) – NOAA SARSAT sends

beacon activation alerts for DoD registered beacons via this interconnection. No privacy data is sent to or received from the U.S. Army via this interconnection.

c) The purpose that the system is designed to serve

The SARSAT system uses NOAA satellites in low-earth and geostationary orbits as well as GPS satellites in medium earth orbit to detect and locate aviators, mariners, and land-based users in distress. The satellites relay distress signals from emergency beacons to a network of ground stations and ultimately to the U.S. Mission Control Center (USMCC) in Suitland, Maryland. The USMCC processes the distress signal and alerts the appropriate search and rescue authorities to who is in distress and, more importantly, where they are located.

d) The way the system operates to achieve the 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 (physically stored on servers within the SARSAT boundary, in Suitland, Maryland). 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 (47 CFR). 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 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). Internal software connects to the database each time there is a new distress case to check if the associated beacon is registered. If the beacon is registered, the internal software attaches the registration data from the database to the alert that is sent to the appropriate rescue agency/agencies. 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).

Then 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.

e) A general description of the type of information collected, maintained, used, or disseminated by the system

SARSAT stores, processes, and transmits alert data, which is the generic term for COSPAS-SARSAT alert and position data derived from 406 MHz distress beacon signal processing. Alert data derived from beacon signals contain the beacon identification and may contain beacon position information and other coded information. SARSAT also stores and transmits beacon registration data, which is used to correlate processed beacon identifications with the beacon's owner information and emergency contacts. The registration information is transmitted along with the alert data to search and rescue authorities when a beacon is activated. The beacon registration data contains non-sensitive PII (names, addresses, and phone numbers).

f) Identify individuals who have access to information on the system

Access to the NOAA SARSAT data is restricted to authorized federal employees and contractors. All data is encrypted at rest, located in access-controlled facilities, and logical controls are in place to provide role-based access control based on the level of need to access the information. NOAA SARSAT users use multifactor authentication to access data. NOAA SARSAT users with access to stored information include the RGDB customer service staff, system and database administrators, and software developers.

The USMCC has five types of SARSAT users:

- Other COPSAS-SARSAT Mission Control Centers
- National Rescue Coordination Centers
- SAR Points of Contact (SPOCs), which are RCCs in foreign countries
- Internal System Developers, System Analysts, System Administrators, Data Entry personnel, and Security Professionals
- Beacon Owners, considered as users of the SARSAT Beacon Registration Database (RGDB) system. The beacon owners authenticate onto the SARSAT-controlled RGDB website

and supply information that is collected and distributed as part of the SARSAT SAR process.

g) How information in the system is retrieved by the user

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 (physically stored on servers within the SARSAT boundary, in Suitland, Maryland). 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 (47 CFR). Beacon owners may provide information to the RGDB via the web application 24/7 or by sending the registration form via mail or fax. Beacon owners may access and/or update their registration information 24x7 via the RGDB web application.

h) How information is transmitted to and from the system

NOAA SARSAT transmits information to other MCCs, RCCs, and SPOCs using one or more of the following methods (prescribed by the international Cospas-Sarsat program):

- File Transfer Protocol (FTP) protected by encrypted Virtual Private Network (VPN) tunnels
- SSH File Transfer Protocol (SFTP)
- Messages sent via the FAA's National Airspace Data Interchange Network (NADIN)
- Human readable fax messages as a backup communication method

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ 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):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X__ No. This is not a new information system.

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. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

_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.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

_X__ DOC employees
_X__ Contractors working on behalf of DOC
____ Other Federal Government personnel
_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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the **NOAA5023** and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_______ The criteria implied by the questions above **do not apply** to the **[IT SYSTEM NAME]** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Thomas Renkevens, NOAA5023 SO Office: NESDIS Phone: 301-683-3257 Email: thomas.renkevens@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: RENKEVENS.THOMAS.MICHAEL.1365830637 Digitally signed by RENKEVENS.THOMAS.MICHAEL.1365830637 Date: 2022.02.24 13:08:34 -05'00' Date signed: __________	**Information Technology Security Officer** Name: Rick Miner Office: NESDIS Phone: 301-427-8822 Email: rick.miner@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: MINER.RICHARD.SCOTT.1398604519 2022.03.17 16:21:00 -04'00' Date signed: __________
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2022.04.11 08:21:13 -04'00' Date signed:	**Authorizing Official** Name: Mark S. Paese, NOAA5023 AO Office: NESDIS Phone: 301-713-2010 Email: mark.paese@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PAESE.MARK.STEFAN.1365833202 Digitally signed by PAESE.MARK.STEFAN.1365833202 Date: 2022.03.31 08:25:42 -04'00' Date signed: __________
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.04.13 11:19:00 -04'00' Date signed:	