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

Privacy Impact Assessment
for the
NOAA5023
Search and Rescue Satellite-Aided Tracking (SARSAT)

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2023.07.05 12:08:36 -04'00'

5/10/2023

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NESDIS/SARSAT

Unique Project Identifier: NOAA5023

Introduction: System Description

Provide a brief description of the information system.

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:

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

NOAA5023 (SARSAT) is a major application.

(b) System location

NOAA5023 is physically located in Suitland, MD with an alternate processing site in Fairmont, WV. 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.

(c) 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. Coast Guard Rescue Coordination Centers (RCCs)
- Foreign MCCs (complete list provided in PIA Section 6.3)
- Foreign Search and Rescue Points of Contact (SPOC) (complete list provided in Section PIA 6.3)
- 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) Mission Management Center (FT-MMC) – 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.
- NOAA0100 - Cyber Security Center
- NOAA0550 - NOAA Enterprise Network

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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) 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.

Video surveillance and entry reader information is only available to the security team, consisting of federal employees and contractors.

(f) 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

(g) Any information sharing conducted by the system

Information is shared with other federal agencies, foreign governments, and foreign entities in order to ensure rescue coordination and 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. Information is shared within the bureau only in case of a privacy incident. Video surveillance and/or building entry reader records may be shared in the event of a physical security incident requiring investigation.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The legal authorities are 5 U.S.C. 301, Departmental Regulations and 47 CFR parts 80, 87, and 95. The cited regulations reflect Communications Act of 1934, as amended—(Communications Act); Communications Satellite Act of 1962, as amended—(Communications Satellite Act); International Telecommunication Union Radio Regulations, in force for the United States—(Radio Regulations); Agreement Between the United States of America and Canada for the Promotion of Safety on the Great Lakes by Means of Radio, as amended, and the Technical Regulations annexed thereto—(Great Lakes Radio Agreement); International Convention for Safety of Life at Sea, 1974, as amended, and the Annex thereto—(Safety Convention); Vessel Bridge-to-Bridge Radiotelephone Act—(Bridge-to-Bridge Act).

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

NOAA5023 is a FIPS 199 high impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					
Video surveillance and building access card reader information is now being collected at a remote, unmanned, facility. Information regarding the sharing limited data with Salesforce was removed from the PIA as that project never moved forward and there is no sharing of data with Salesforce.					

____ 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.

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c Employer ID		h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	X
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Although unsolicited, some users choose to provide medical information so it can be relayed to rescue personnel.					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording	X	i. Height	X	n. Retina/Iris Scans	
e. Photographs		j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Although unsolicited, some users choose to provide distinguishing information that may aid rescue forces such as height and weight.					

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

Other Information (specify)
Names and telephone numbers of emergency contacts.

2.2 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	X	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): Foreign Mission Control Centers may send PII from their respective registration databases in the event of a distress event occurring the U.S. area of responsibility to assist with search and rescue efforts.					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Data is provided directly by the beacon owners. Confirmation of the data provided is sent to the beacon owners upon registration and/or update whereupon the beacon owners are provided an opportunity to make corrections or additional changes. Additionally, beacon owners are reminded every two years to verify and/or update their registration information in the RGDB. Any data entered by NOAA staff undergoes a three-person quality assurance process to ensure accurate data entry. All data is encrypted at rest and access is restricted to authorized data entry staff. All staff access to registration data is logged along with a detailed history of any changes made to the data.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB 0648-0295
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	X*	Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): *Smartcards are used for the access control system at the one facility mentioned (Holloman AFB). While the smartcards do not contain PII themselves, they are mapped to names of personnel who are authorized to access this building. Video surveillance has also been added.			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Search and Rescue			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the 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 mailing address of the beacon owner.

The information will be shared with Rescue Coordination Centers in the U.S. that are operated by the U.S. Air Force and 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 website or by sending hard copy notification to NOAA SARSAT.

Most of the PII/BII identified in Section 2.1 of this document is in reference to a member of the public. Federal employees and contractors provide limited PII for the purpose of creating user accounts.

The video surveillance and building entry reader activities referenced in Section 3 apply to the NOAA SARSAT ground station at Holloman AFB, NM, which is an unmanned facility that is only accessed by authorized NOAA SARSAT federal employees and contractors.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Common threats to the privacy of beacon registration data include data leakage due to the compromised chain of custody within the environments designated to store/process privacy information and insider threat. All federal employees and contractors with access to privacy

data undergo annual training on handling PII. All access to the privacy data is monitored and logged. FIPS 140-2 validated encryption is in place to protect the privacy data in transit and at rest. Video surveillance recordings are retained for 180 days and then deleted or overwritten.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

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

* For privacy incidents and in th eoccurrence of a security incident.

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA SARSAT shares with the following entities via File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) over Virtual Private Network (VPN) tunnels and via fax to assist in carrying out their mission of rescue coordination and false alert abatement: France Mission Control Center Spain Mission Control Center Australia Mission Control Center

	Russia Mission Control Center Japan Mission Control Center Brazil Mission Control Center Canada Mission Control Center Peru Mission Control Center Chile Mission Control Center Argentina Mission Control Center South Africa Mission Control Center Indonesia Mission Control Center Singapore Mission Control Center Thailand Mission Control Center China Mission Control Center Hong Kong Mission Control Center Korea Mission Control Center Taiwan Mission Control Center Vietnam Mission Control Center Air Force Rescue Coordination Center Alaska Air Command Rescue Coordination Center Coast Guard District 1 – Boston Rescue Coordination Center Coast Guard District 5 – Portsmouth Rescue Coordination Center Coast Guard District 7 – Miami Rescue Coordination Center Coast Guard District 8 – New Orleans Rescue Coordination Center Coast Guard District 9 – Cleveland Rescue Coordination Center Coast Guard District 10 – Seattle Rescue Coordination Center Coast Guard District 11 – PACAREA Coast Guard District 14 – Honolulu Rescue Coordination Center Coast Guard District 17 – Juneau Rescue Coordination Center Coast Guard Sector Guam Rescue Coordination Center Coast Guard Sector San Juan Coast Guard LANTAREA – Portsmouth Rescue Coordination Center Search and Rescue Point of Contact Belize Search and Rescue Point of Contact Bermuda Search and Rescue Point of Contact Honduras Search and Rescue Point of Contact Columbia Search and Rescue Point of Contact Costa Rica Search and Rescue Point of Contact Dominican Republic Search and Rescue Point of Contact Ecuador Search and Rescue Point of Contact El Salvador Search and Rescue Point of Contact Guatemala Search and Rescue Point of Contact Guyana Search and Rescue Point of Contact Mexico Search and Rescue Point of Contact Nicaragua Search and Rescue Point of Contact Panama Search and Rescue Point of Contact Venezuela NOAA0100 and NOAA0550 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 and MCC 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.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X*	Government Employees	X
Contractors	X		
Other (specify):			
* Beacon owners have access through the RGDB to their own PII only.			

Section 7: Notice and Consent

7.1 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 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.sarsat.noaa.gov/privacy_policy/	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the beacon registration forms (samples on file) & signage of surveillance is posted at the USAF base entry. Signage is in the process of being posted at the other locations.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Beacon owners can decline to provide the information, but then they would not be in compliance with 47 CFR Parts 80, 87, and 95. Individuals can opt not to enter the facilities with video surveillance.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Owners might indicate on their registration forms that they do not consent to particular uses of the information; however, they would not be able to receive Search and Rescue services. Individuals consent to surveillance by continuing to access these locations.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 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 website or by sending hard copy notification to NOAA SARSAT.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: There is no opportunity for individuals to review/update the video images recorded for safety & security purposes.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Logging is in place to record each attempted access attempt to PII/BII.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 6/14/2022 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. NOAA5023 is a FIPS 199 High impact system.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Detailed audit logging is captured and stored on all devices used to access or store PII/BII. Encryption and hashing are used to protect the confidentiality and integrity of PII/BII in storage and in transmission.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database COMMERCE/DEPT-25, Access Control and Identity Management System. COMMERCE/DEPT-13, Investigative and Security Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Disposition Handbook, item 1404-02, SARSAT Beacon Registration Records NOAA Records Disposition Handbook, item 901-03, Facility Security Management Operations Records
	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:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X *
Degaussing	X	Deleting	X
Other (specify): * Hard drives are overwritten/sanitized immediately upon return to IT for re-use.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	**Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the PII contained in this system. However, that is desirable in emergency situations.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: While not solicited, some users provide medical information so it can be relayed to emergency rescue personnel.
X	Context of Use	Provide explanation: Ability to search and rescue based on PII
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Physical and logical access controls are in place to restrict access to PII
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The information collected from beacon owners has been deemed the minimum necessary information to adequately provide search and rescue services. The discussions on necessary data have included the agencies with whom data is shared including the U.S. Coast Guard and U.S. Air Force.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.