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:
The National Oceanic and Atmospheric Administration (NOAA) Search and Rescue Satellite-Aided Tracking (SARSAT) System is a Major Application operating under the auspices of the Department of Commerce (DOC).

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 Prediction (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, MD are used to remotely control the primary or secondary USMCC 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 Sistyema Poiska Avariynich Sudov" (COSPAS) is Russian for "Space System for the 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.

The USMCC has five types of SARSAT users:

- Other COSPAS-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.

SARSAT Data:
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).

Questionnaire:

1. 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.

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

2
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.

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). Continue to answer questions and complete certification.

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 I, 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.

   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

   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.)

X DOC employees
X 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 PIA 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 Search and Rescue Satellite-Aided Tracking (SARSAT) NOAA5023 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above do not apply to 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.1365841
Digitally signed by
LITTLE.BRIAN.WILLIAM.1365841230
Date: 2018.09.06 12:05:52 -04'00'

Date: ____________

Name of Information Technology Security Officer (ITSO): Frank Menzer

Signature of ITSO:  MENZER.FRANK.E.102
Digitally signed by
MENZER.FRANK.E.1026670450
Date: 2018.09.11 11:08:52 -04'00'

Date: 9/11/2018

Name of Authorizing Official (AO): Mark Paese

Signature of AO: [Signature]
Date: 9/11/18

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO:  GRAFF.MARK.HYRUM.1514447
Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER,
cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.09.19 09:54:06