FUNCTIONAL REQUIREMENTS FOR THE COSPAS-SARSAT INTERNATIONAL BEACON REGISTRATION DATABASE

C/S D.001
Issue 3
October 2024

FUNCTIONAL REQUIREMENTS FOR THE COSPAS-SARSAT INTERNATIONAL BEACON REGISTRATION DATABASE

History

Issue	Revision	Date	Comments
1		October 2004	Approved CSC-33
2		October 2010	Approved CSC-45
2	1	October 2014	Approved CSC-53
3		October 2024	Approved CSC-71

Definitions of acronyms can be found in the Cospas Sarsat Glossary (document C/S S.011).

Contents

LIST OF ANNEXES

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 Overview

The Cospas-Sarsat system provides search and rescue (SAR) services with distress alerts that include the unique 15-character (first-generation beacon, FGB) or 23-character (second-generation beacon, SGB) hexadecimal identification of the transmitting beacon. This identification is decoded to obtain detailed information such as the type of beacon, i.e. aircraft Emergency Locator Transmitter (ELT), vessel Emergency Position Indicating Radio Beacon (EPIRB) or Personal Locator Beacon (PLB), the country code (Maritime Identification Digits, MID) associated with the unique beacon identification, the type of auxiliary radio locating (homing) device, etc.

However, to assist SAR services additional information is required such as the aircraft or vessel identification, the type of aircraft or vessel in distress, communications equipment on the vessel or aircraft, number of persons in distress, etc. Such information can be made available to SAR services only if the 406 MHz distress beacon has been properly registered and the required information provided to the registration authority by the beacon owner/operator.

Therefore, a number of administrations have made beacon registration mandatory and maintain their own national beacon registration databases. Registration of 406 MHz beacons is also required pursuant to international regulations on SAR established by the International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO). This registration information must be made available to SAR services on a 24-hour basis in case of an emergency.

Despite the clear advantage of registration, a large percentage of beacons are not properly registered due to a lack of registration facilities provided by national administrations. Furthermore, a number of beacon registers do not have 24-hour points of contact easily accessible by SAR services. Therefore, in 2004 the Cospas-Sarsat Council decided to establish an International Beacon Registration Database (IBRD) available to users when no national registration facilities have been implemented, and to Administrations who wish to avail themselves of the facility to make their national beacon registration data available to SAR services.

The proposed IBRD is an Internet (or web-based) system that maintains and provides various levels of access by beacon owners who wish to register their beacons, Administrations who wish to make registration data available to international SAR services, and SAR services that need to access beacon registration data to efficiently process distress alerts.

The responsibilities associated with the provision of the IBRD include maintenance of the database, providing the means to view, enter, modify and query records in the database, ensuring that these records are available, providing automated monitoring of the registration process and generating various reports as required to manage the database. This document specifies the functional requirements to support these responsibilities.

1.2 Document Organisation

Section 2 of the document provides definitions for some of the terms used, when these terms carry a specific meaning in the context of the IBRD functional requirements, and the IBRD general requirements.

Section 3 defines the requirements, rules and functionality associated with IBRD access by various categories of users.

Section 4 addresses security aspects.

Section 5 defines logging requirements for the administration of the IBRD.

Section 6 addresses the user interface requirements, including password management,

Section 7 includes data validation requirements definition.

Section 8 details functionalities associated with the provision of reports on operations statistics, for use by the Database Administrator, and queries of database information, for use by SAR services and other authorised public bodies.

Section 9 addresses the Bulk upload software requirements and functionalities.

Section 10 provides the performance requirements.

Section 11 provides the functionality in respect of the IBRD maintenance.

1.3 Reference Documents / Materials

The following documents are a valuable source of information on 406 MHz emergency beacons and registration, and contain specific details on the requirements contained in this document.

- C/S T.001, Specification for Cospas-Sarsat 406 MHz Distress Beacons,
- C/S T.018, Specification for Second Generation Cospas-Sarsat 406-MHz Distress Beacons,
- C/S A.001, Cospas-Sarsat Data Distribution Plan,
- C/S G.005, Cospas-Sarsat Guidelines on 406 MHz Beacon Coding, Registration and Type Approval,
- C/S G.008, Operational Requirements for Cospas-Sarsat Second-Generation 406-MHz Beacons
- C/S P.011, Cospas-Sarsat Programme Management Policy.

1.4 Source of Requirements

The IBRD requirements are based on the following international requirements:

a) International Maritime Organization (IMO) Assembly Resolution A.887(21);

b) Annex 10 to the Convention on International Civil Aviation (ICAO),

Other related documents are listed in document C/S S.007, Handbook of Beacon Regulations.

- END OF SECTION 1 -

2. DEFINITIONS AND GENERAL REQUIREMENTS

2.1 Definitions

15 or 23 character hexadecimal character identification (15 Hex ID, 23 Hex ID or Hex ID)

The representation in hexadecimal characters of the content of:

- bits 26 to 85 in the beacon message, as defined in document C/S T.001 for first generation beacons,

  or

- bits 1 to 92 in the beacon message, as defined in document C/S T.018 for second generation beacons,

which should be permanently marked on the exterior of the beacon.

Authorized Ship and Aircraft Inspectors and Maintenance Facilities

This account type is for inspectors and maintenance personnel who wish to confirm that a beacon has been registered. This access does not allow visibility into detailed owner/operator information and is used only to confirm that a beacon is properly registered.

Beacon

406 MHz distress beacons that meet the requirements of Cospas-Sarsat System documents C/S T.001 or C/S T.018.

Beacon identification code

For first generation beacons, the content of bits 26 to 85 in the beacon message that uniquely identifies a beacon in accordance with document C/S T.001.

For second generation beacons, the content of bits 1 to 92 in the beacon message that uniquely identifies a beacon in accordance with document C/S T.018.

Confirmation

The process used to verify the accuracy of beacon registration information.

Database Administrator

The Officer designated by the Cospas-Sarsat Council to manage and administer the IBRD in accordance with policy guidance and directions given by the Council. The Database Administrator may direct the database operator on actions required to maintain the appropriate level of service to IBRD users.

Data Provider

An individual beacon owner, an organisation that owns/operates beacons, or an organisation that acts on behalf of a beacon owner, who submits registration data on-line for one or several beacons.

IBRD database

The system, which may include hardware, software, and cloud-based components, that contains the beacon registration records.

IBRD user interface

The screens and supporting software that provide for IBRD input and output via the Internet. This includes a web-browser based interface as well as an application programming interface (API).

National Data Provider (NDP)

An Administration that has informed Cospas-Sarsat of their decision to make use of the IBRD to allow 24-hour access to beacon registration data under their country code(s). NDPs retain full responsibility for the collection, control and updates of all registration data associated with their country code(s) and may allow delegation of this responsibility to individual Data Providers. Acceptance of a National Data Provider is subject to the completion of appropriate procedure and agreement, as may be required by the Cospas-Sarsat Council.

SAR service

A recognised Search and Rescue (SAR) organization that has been assigned a specific user identification and password for accessing the IBRD, as provided for in section 3. In the context of this document, SAR services also include Cospas-Sarsat MCCs, ship surveyors, and other authorised public bodies that have been assigned a user identification and password to access the IBRD.

User identification

The user name assigned by the Database Administrator to a SAR service, a National Data Provider, an Authorized Inspector, or a Data Provider (including individual beacon owners). Previous versions of the IBRD software relied on the use of a Hex ID for identification of individual Data Providers (beacon owners). The current version of the IBRD does not allow new accounts to be created using a Hex ID as a username. At account creation, the user may choose a username and

is strongly encouraged to provide an e-mail address. E-mail is the primary mechanism for password recovery by beacon owners and may be used as an alternative to the username at login. Other account types (NDP, administrators) must contact the system administrator for password reset assistance, and these accounts may not log in using their e-mail address as a username.

2.2 Beacon Types

The document C/S T.001 "Specification for Cospas-Sarsat 406 MHz Distress Beacons" contains a full description of all beacon types and coding protocols for first generation beacons.

The document C/S T.018 “Specification for Second Generation Cospas-Sarsat 406-MHz Distress Beacons” provides the same for second generation beacons.

2.2.1 The International Beacon Registration Database (IBRD) shall have the capability to accommodate all types of 406 MHz beacons, i.e.:

a) Emergency Position Indicating Radio Beacons (EPIRB) carried onboard vessels;

b) Emergency Locator Transmitters (ELT) carried onboard aircraft, including ELT(DT) designed for inflight tracking of aircraft; and

c) Personal Locator Beacons (PLB) for use by individual persons in any environment.

2.2.2 The type of a beacon registered in the IBRD shall be determined by the beacon message, which is presented as the 15 Hex ID of a first generation beacon or the 23 Hex ID of a second generation beacon plus its Type Approval Certificate (TAC).

2.2.3 The IBRD does not support registration of 406 MHz Ship Security Alert System (SSAS) beacons.

2.2.4 The IBRD does not support registration of beacons coded with any National User Protocols.

2.3 Data Retrieval

2.3.1 All information shall be retrievable for any beacon in the database.

2.3.2 Data shall be retrievable by:

d) the IBRD User Interface running on all supported platforms (see section. 6.5);

e) the IBRD software responsible for the automatic generation of Confirmation Requests (see section. 2.6); and

f) direct access to IBRD application programming interfaces (APIs).

2.4 Supported Country Codes and Beacon Types

2.4.1 The IBRD shall decode the beacon identification code (Hex ID) to determine the country code and the beacon type (see documents C/S T.001 and C/S T.018).

2.4.2 The IBRD shall accept on-line beacon registration only for those beacons encoded with one of the country codes provided in the list of supported country codes and for the beacon type (ELT, PLB and EPIRB) configured for a given country code. However, on-line registration may not be provided when the responsible Administration has informed Cospas-Sarsat that they wished to control themselves the registration of beacons with their country codes and beacon types in the IBRD (see definition of National Data Providers).

2.4.3 The list of supported country codes and beacon types shall be determined by Cospas-Sarsat in accordance with national requirements known to Cospas-Sarsat.

2.4.4 Changes to the list of supported country codes and beacon types per country code shall be possible under the control of the Database Administrator.

2.4.5 Registration of beacons with unsupported country codes and beacon types per country code shall be possible via an override sequence under the control of the Database Administrator.

2.4.6 National Data Providers may register beacons with their country code and beacon types even if the country code and beacon type is unsupported for individual beacon owners.

2.5 Database Fields

Beacon registration information shall include the 15 Hex ID or 23 Hex ID of the beacon and additional vital information such as owner name, emergency points of contact, vessel name, etc. Annex A to this document provides the complete list of the name of the fields that shall be defined in the database. Annex A includes all the fields required for compliance with International Maritime Organization (IMO) Resolution A.887(21) and Annex 10 to the Convention of the International Civil Aviation Organization (ICAO).

2.6 Acknowledgement of Registration and Requests for Confirmation

2.6.1 Upon new user registration, entry of an email address shall be strongly encouraged and input should be validated as possible. If left blank, an informational disclaimer will be displayed and must be acknowledged by the user before proceeding.

2.6.2 The IBRD shall provide an automatic acknowledgement of the initial registration and of each registration modification to the Data Provider. This acknowledgement shall be provided through the IBRD user interface via the Internet. An email will be sent to the Data Provider's email address confirming the registration information. If a beacon registration has been recorded or uploaded by a National Data Provider on behalf of the

beacon owner, the email will be sent directly to the National Data Provider's email address and not to the beacon owner's email address.

If the combination of beacon type and MID decoded from the Beacon UID is set to 'Delegate' in the IBRD settings, this means that the National Data Provider has elected to register beacons of that type on behalf of beacon owners but delegate the future management of those beacons to the beacon owner. In this case, the confirmation email is sent to the email address of the beacon owner as entered by the National Data Provider.

2.6.3 The acknowledgement shall include:

a) all data provided in the initial registration or as modified by the Data Provider; and
b) a statement reminding the Data Provider that it is his/her responsibility to submit in due time any required modification to the registered data, or to confirm the registered data within one or two years of the last entry/modification, as defined by the Database Administrator.

2.6.4 The database shall have a designated field to store the date of the original registration (see Annex A).The database shall have a designated field to store date of the last modification or confirmation of the registered data (see Annex A).

2.6.5 The database shall automatically prepare Confirmation Requests two years after the date of the last modification or confirmation of the registered data, send the Confirmation Request to the email address of the Data Provider, and track the status of the Confirmation Request.

2.6.6 The automatic generation of Confirmation Requests shall be suppressed on the basis of known national requirements associated with the country code.

2.6.7 Dates shall be shown in "yyyy-mm-dd" format and time shall be shown in "hh:mm:ss" format.

2.7 Beacon Status

2.7.1 The IBRD shall have a designated field and the capability to record the status of each beacon as reported by the Data Provider (e.g. lost, destroyed or stolen beacons, see Annex A).

2.7.2 The IBRD shall have the capability to record and display the previous status of a beacon.

2.8 Ease of Installation

2.8.1 The IBRD shall be designed such that accessing it on a supported computing platform is a simple process. Specifically, accessing the IBRD software as an end-user shall only require familiarity with a web browser.

2.9 Bulk Record Uploads

2.9.1 The IBRD shall provide a means for uploading multiple beacon registration records in a single operation.

2.9.2 The IBRD software shall:

a) support the CSV and XML formats for bulk record uploads (other formats may optionally be supported in addition to CSV and XML);

b) insert all valid records into the IBRD database; and

c) prepare an upload status message to the National Data Provider and Block Owner.

2.9.3 The upload status message shall include the registered data for each valid record inserted in the IBRD and a list of all invalid records that were rejected with an indication of the cause of rejection. A summary of total successful and failed registrations should be available at the beginning of this message.

2.9.4 An interface document describing the required format for bulk uploads and the possible causes for record rejection shall be developed.

2.10 Bulk Record Download

2.10.1 The IBRD shall provide to National Data Providers and Block Owners a means for downloading multiple beacon records in a single operation to make these records available to the offline Bulk Upload software.

2.10.2 The IBRD software shall provide the file in XML format requesting the user to save the file under the appropriate folder in the Bulk Upload software. Other supported formats are CSV, TSV, and JSON.

- END OF SECTION 2 -

3. USER ACCESS

3.1 Internet Access

The IBRD user interface shall be available via the Internet.

3.2 Classes of Users

The IBRD user interface shall only be accessible to the following users (see definition in section 2.1):

a) Beacon Owners
b) National Data Providers;
c) SAR services (to include also Cospas-Sarsat MCCs, and other authorised public bodies);
d) Inspectors and Maintenance Providers; and
e) Database Administrator.

3.3 Access to the IBRD Capabilities

3.3.1 The IBRD shall provide the following capabilities to the various classes of users:

a) view record: display existing registration records;
b) new record: create new registration records;
c) modify record: change existing registration information in a record;
d) beacon Status: modifies existing registration records by entering an appropriate "beacon status code" (see Annex A); and
e) query: display information for multiple records using search indexes (e.g., by owner name, vessel name, etc.).

3.3.2 Access to IBRD capabilities shall be provided to each class of users only as specified in Table 3.1.

Table 3.1: Types of Access for User Classes

CLASS OF USER:	TYPE OF USER ACCESS				
	View Record	New Record	Modify Record	Change Beacon Status	Query
Beacon Owner	Yes	Yes	Yes	Yes	Yes*
National Data Prov.	Yes	Yes	Yes	Yes	Yes*
SAR Services **	Yes	No	No	No	Yes
Inspectors and Maintenance Providers	No	No	No	No	Yes***
Database Admin.	Yes	Yes	Yes	Yes	Yes

Notes: * Only beacon records associated to the Beacon Owner account or to the National Data Provider country codes can be queried.

** In the context of this document, SAR services also include Cospas-Sarsat MCCs, and other resources as approved by national administrations.

*** Ship surveyors and authorised shore-based maintenance (SBM) providers are allowed to access records and view beacon data and vehicle information, but excluding beacon owner information.

3.4 Administrator Interface

The Database Administrator shall be able to log in to an interface to easily create, edit, and manage:

a) user accounts
b) points of contact for beacon registries
c) country codes and beacon types
d) beacon manufacturer list
e) beacon type approval certificate (TAC) information
e) special messages on the home page
f) reports (see section 8)

- END OF SECTION 3 -

4. SECURITY

4.1 Unauthorized Changes

The IBRD database shall be secure from unauthorized changes. Prevention of unauthorized changes is a function of the user interface, as well the general IBRD environment. This is accomplished specifically by controlling user access (section 3) and by implementing a secure Internet environment.

4.2 User Validation

4.2.1 Access to the IBRD database shall be validated for each user, depending on the user class, as follows (see section. 3.2):

a) Beacon Owner: “user identification” or “email address”AND "password";

b) National Data Provider: "user identification" AND "password";

c) SAR services / Inspectors and Maintenance Providers: "user identification” AND “password”; and

d) Database Administrator: “user identification” AND “password”.

4.2.2 User accounts shall be temporarily deactivated (i.e. locked out) for 20 minutes upon 5 successive failed logon attempts.

4.2.3 Provision of a forgotten password to Data Providers, and/or the reactivation of their account, shall be possible via a password “challenge” question/answer process. Upon successful completion of the challenge question/answer process, the account shall be reactivated and/or the assigned password shall be automatically sent to the Data Provider using the email address recorded by that Data Provider in the IBRD.

4.2.4 Provision of a forgotten password to a SAR service or a National Data Provider, or reactivation of the deactivated account of the SAR service or National Data Provider shall be made by the Database Administrator in accordance with the procedure agreed by the Cospas-Sarsat Council.

4.2.5 Additional access methods, which may include API keys, may be provided in order to secure access via API interfaces and may supplement or replace the username and password mechanisms for any user class.

4.3 Access by Data Providers

Specific limitations shall apply for Data Providers access to registered information.

4.3.1 Beacon Owners shall only be permitted to:

a) view and/or modify registration records for their own beacons; and

b) view and/or modify one beacon registration record at a time.

c) extend changes to owner/operator information across all records contained within the account that they own in a single operation.

4.4 Database Isolation

4.4.1 While a user enters, modifies, or views registration data and/or query results, the IBRD user interface shall not be physically connected to the IBRD database.

4.4.2 The link to the IBRD database shall be opened to perform an operation and closed as soon as that operation is complete. As a minimum, the following operations require opening (and subsequent closing) of the IBRD database:

a) retrieve an existing record;

b) store a new record (after all error checking is complete);

c) store a modified record (after all error checking is complete); and

d) execute a query and obtain the result.

4.5 Web-Based Access

The IBRD shall be implemented such that the database is not directly linked to users on the Internet at any time. The Web based access system may be defined in terms of three main components as illustrated in Figure 4.1:

a) the Web Application, built in JavaScript which provides the user interface and application logic;
b) the application programming interface (API) gateway, a platform that applies user actions to the IBRD database providing a critical "buffer" layer between the Internet and the database; and
c) the Beacon Registration Database.

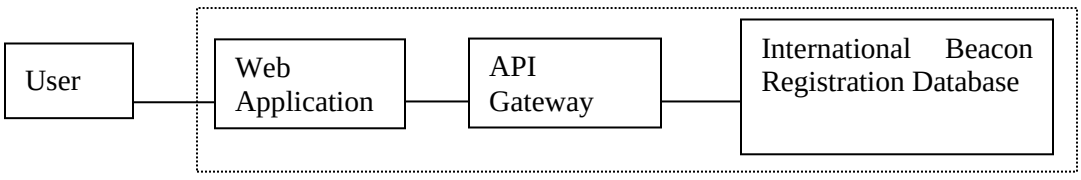

Figure 4.1: Relationship Between Main IBRD Components

4.6 Denial of Service Protection

The IBRD shall provide protection from malicious attempts to interfere with normal operation and authorized access (e.g., high volume repetitive access). The IBRD cloud infrastructure provides always-on network flow monitoring, which inspects incoming traffic to cloud services and applies a combination of traffic signatures, anomaly algorithms, and other analysis techniques to detect malicious traffic in real time.

Automated mitigation techniques are built into the IBRD cloud infrastructure, giving underlying services protection against common infrastructure attacks. Automatic mitigations are applied inline to protect these services, so there is no latency impact. Techniques such as deterministic packet filtering and priority-based traffic shaping automatically mitigate basic network layer attacks.

4.7 Virus Protection

The architecture of the IBRD relies on cloud-based web services. These services do not rely on traditional servers, and as such there is no server supporting IBRD on which to install malicious code (i.e. viruses). Email service is configured in such a way using cloud services that outgoing mail will sent with sender authentication.

4.8 Virtual Private Cloud Security Groups and Web Application Firewall

The IBRD utilizes web application firewall and security groups, integrated with the cloud infrastructure, which provide protection against common web exploits and bots that can affect availability, compromise security or consume excessive resources.

Security groups control the traffic that is allowed to access and depart the resources that they are associated with, acting as a virtual firewall.

4.9 Password Encryption

4.9.1 Password information received, transmitted, or stored by the IBRD shall be protected using standard Internet encryption technology in transit and at rest.

4.10 New Registration Validation

4.10.1 Data Providers entering a new beacon registration shall be required to provide the beacon identification code (Hex ID) as the first input. The beacon identification code shall then be:

a) validated as per section 7.1; andchecked for duplicate records as per section 7.3.

b) Failure to pass either test successfully will terminate the new registration process and a warning message indicating the cause of the failure shall be returned to the Data Provider.Secure Coding

c) The IBRD shall employ best practices in secure software design techniques. The IBRD code shall employ methodologies that mitigate the risk posed to application and data integrity including but not limited to cross-site scripting and SQL injection. Secure Email Messaging

d) all email messages shall be constructed and sent securely using sender identity management (e.g. DKIM, SPF); and

e) messages generated by the IBRD system shall be constructed such that treatment of messages as spam by email filters shall be minimized as possible.

- END OF SECTION 4 -

5. LOGGING

5.1 Changes to Database Records

All changes to the database records shall be logged such that it would be possible to fully reconstruct the complete contents of any record in the database at any point in its revision history. Logging of individual changes to the database includes the following minimum information:

a) beacon identification code (Hex ID);

b) date/time of transaction;

c) user identification;

e) IP address of source;

f) old value for each changed field; and

5.2 g) new value for each changed field.User Access

The following minimum information shall be logged for all user access, both successful and failed access attempts:

a) user identification;

b) authentication mechanism of user;

c) IP address of source;

d) date/time of start of session;

5.3 Queries

All query operations shall be logged. Query logging shall include as a minimum:

a) user identification;

b) authentication mechanism of user;

c) IP address of source;

d) number of records returned;

e) time for execution (in seconds); and

f) search string.

- END OF SECTION 5 -

6. ON-LINE USER INTERFACE

6.1 On-line Help

Guidance (or "Help") on how to use the software data shall be available via the IBRD user interface and shall:

a) appear on every screen layout as an option, in approximately the same location;

b) be context sensitive (e.g., different classes of users have different access capabilities and the on-line help should likewise only refer to the capabilities that are available to the current user); and

c) provide responses to a series of frequently asked questions (FAQs).

6.2 Assisted User Input

Wherever possible, fields shall provide drop-down menus for user input. The list of entries shall be limited to the allowable values. In some cases, users may be allowed to override the list of possible entries by selecting "Other".

6.3 Error Handling

Wherever possible, user input shall be checked for errors, and warnings shall be provided on-line to Data Providers and National Data Providers. Error checking shall:

a) be applied as much as possible before any attempt to insert data into the database is made; and

b) allow the user to have as many chances as necessary to correct each errant entry, without destroying or losing other information that has been entered elsewhere.

6.4 Cancel Option

Every user interface screen shall:

a) have an option for cancelling the current operation; and

b) have an option for returning to the opening menu or dashboard (as given after successful login).

6.5 Commonly Available Platforms

6.5.1 The IBRD user interface software shall be designed to run smoothly using only the native capabilities of commonly available commercial software and hardware platforms.

Specifically, the user interface software shall run properly when accessed via the Internet from:

a) standard Mac (Macintosh OS) based systems running Safari, Chrome, Firefox, and Edge based browsers.

b) standard PC (Microsoft Windows Vista or later) based systems running Chrome, Safari, Edge and Firefox.

c) Android mobile phones running Android 4.4+ with Play Services running Chrome

6.5.2 d) Apple mobile phones running iOS 11.3+ running Chrome or Safari for online access, and running Safari only for optional offline accessAccess to the IBRD web interface shall not require using or downloading any additional applications onto a user's computer.

6.5.3 The IBRD user interface shall not require a display with a resolution greater than 800x600 pixels.

6.5.4 The files generated by bulk download of records, and required for bulk upload of records, will require additional software to read, generate or modify. Similarly, API access will require specific software and configurations.

6.6 User Assistance

The IBRD user interface shall provide the following means for problem description and reporting to the database operator personnel:

a) via an integrated form submission tool;

b) via email to the Database Administrator email in a manner such that the address is not visible to web bots;

c) via telephone; and

b) the postal address of the Database Administrator.

6.7 File/Print Listings

The IBRD user interface software shall provide the user with a capability to direct the current registration information, as displayed on the user computer screen, to:

a) their local computer's printer; and

b) a PDF file to be stored on their computer hard drive.

Text-only renditions of registration records, in tabular form, may be provided via the bulk export tool.

6.8 Registration Practices Reminders

The IBRD user interface shall remind Data Providers (Beacon Owners and National Data Providers) about recommended registration practices, including as a minimum, that:

a) beacon registration is required by IMO and ICAO regulations for ships/aircraft under their jurisdiction, facilitates SAR operations, and is, therefore, in the beacon owner's best interest;
b) updates to registered data must be provided by the beacon owner whenever registration information changes; and
c) confirmation of registration information is recommended every 2 years from the date of the last update, or the initial entry of registration data.

6.9 Other Registration Points of Contact

6.9.1 If a Data Provider attempts to register a beacon encoded with a country code that is not supported by the IBRD, the IBRD user interface shall provide on-line, when available, an alternate point of contact (POC) for the registration of beacons with that country code.

6.9.2 The IBRD shall maintain reference tables of known international POCs for unsupported country codes. SAR services should be referred to the 24-hour contacts and the Beacon Owner should be referred to the Administrative contact.Reference tables exist in the Cospas-Sarsat website and should be used or replicated if possible. The tables shall be designed such that POC updates may be performed in an efficient manner. Specifically, although several country codes point to the same POC, updates of POC details should not require multiple redundant entries.

6.10 Disclaimer of Liability and Data Release Statements

6.10.1 The IBRD user interface shall display on the opening screen of the user interface after user login the appropriate disclaimer of liability statement(s), as required by the Cospas-Sarsat Council.

6.10.2 The IBRD user interface shall display on the opening screen of the user interface the appropriate statements, as required by the Cospas-Sarsat Council, authorising the release of the registered data to SAR services, as may be needed for processing Cospas-Sarsat distress alerts, and to the national administration that has jurisdiction for the country code embedded in the Hex ID of the beacon.

6.10.3 The IBRD user interface shall request a positive acknowledgement of the disclaimer of liability and data release statements by the Data Provider prior to proceeding with the processing of any registration data entry.

6.10.4 API users must implicitly agree to the same disclaimers and limitations of liability as users of the web interface.

6.11 Links to Related Web Sites

The IBRD user interface shall provide links to the following related Internet sites, as a minimum:

a) Cospas-Sarsat;

b) ITU MARS database;

c) ICAO;

d) IMO; and

e) Beacon Decode program.

6.12 Password Management

6.12.1 Passwords for SAR services, Inspectors and Maintenance Providers, National Data Providers and the Database Administrator shall be assigned by the Database Administrator. Beacon Owners shall have the capability to select their own password on-line. A password shall have a minimum of 8 characters, and have one each of: upper-case letter, lower-case letter, number, and symbol.

6.12.2 As a minimum, the following password related facilities shall be provided:

a) Change of Password (for Beacon Owners only): to change an old password, the IBRD user interface shall require entry of the old password, the new password and a repetition of the new password for verification, using a standard mechanism to hide the typed characters.

b) Guidance for forgotten passwords (all classes of users): guidance shall be provided to users who have forgotten their password, and to users whose account has been deactivated, with clear instructions on how to proceed (see Req. 4.2).

c) Password assignment (for SAR services and National Data Providers): a password management tool shall be provided to assist the Database Administrator in assigning new passwords, and recording and retrieving assigned passwords with the user identification.

6.13 Contact Us Form

6.13.1 The IBRD user interface shall provide a means for the Database Administrator to solicit user feedback on the operation of the IBRD.

6.13.2 The IBRD user interface shall have the capability to provide users with the required form, a simple means of filling out the proposed form, and forwarding it on-line to the Database Administrator.

6.14 Languages

6.14.1 The IBRD user interface shall allow beacon registration entries using exclusively Latin characters (Unicode.org).

6.14.2 The IBRD user interface shall support queries using the international Standard English vocabulary only.

6.14.3 The IBRD user interface shall allow Data Providers to select beacon registration instruction screens and Help features presented in either the English, French, Russian languages, and any other languages that could be implemented (e.g., Spanish).

6.15 Home Page

The home page shall allow new Beacon Owner users to create an account or returning users to log into their existing account.

The following types of users will be directed to request access using an online form, to be reviewed and approved on a case-by-case basis:

a) National Data Providers
b) Search and Rescue Services
c) Inspectors and Maintenance Personnel

6.16 Registration Form

6.16.1 After information has been entered in a form and submitted successfully, the IBRD interface shall bring the user to a “view only” version of the beacon record.

6.16.2 The IBRD user interface shall provide the user with, at minimum, the following options:

a) Log out;
b) Register another beacon (for Beacon Owners); and
c) Home

- END OF SECTION 6 -

7. DATA VALIDATION

7.1 Beacon Identification Code

7.1.1 Beacon identification codes provided for new beacon registrations shall be validated against C/S T.001 and C/S T.018 coding requirements. The beacon identification code contents shall satisfy the criteria provided in Table 7.1 below (see C/S A.001 "Cospas-Sarsat Data Distribution Plan",).

7.1.2 The IBRD shall determine if the beacon is a "test coded" beacon and shall prevent the user from registering the beacon.

Table 7.1: Validation Criteria for Beacon Identification Codes

Item to Check	**Bits**	**Fail if:**
Country Code	27 – 36	Decimal value < 200 or > 780, or corresponds to non allocated country codes
User Protocol	37 – 39	Bit 26 = 1 and Bits 37 – 39 = 101
Serial User Protocol	40 – 42	Bit 26 = 1 and Bits 40 – 42 = 101 or 111
Maritime User or Radio Call Sign	82 – 83	Bit 26 = 1 and Bits 37 – 39 = 010 or 110 and Bits 82 – 83 are non-zero
National-Short Location Protocol and National Location Protocol	37 – 40	Bit 26 = 0 and Bits 37 – 40 = 0000, 0001, 1001, 1100 or 1101
Modified Baudot Code	Varies	Unassigned Baudot Character
Binary Coded Decimal	Varies	Decimal Value for Four Bit Group > 10
All National and Standard Location Protocols	Varies	Location Data Fields content different from C/S T.001 specified default values

7.2 Checksum Feature

A checksum feature shall be provided that allows, on an optional basis, the automatic verification of the Hex ID entered by a beacon owner when registering a beacon. The checksum is provided by beacon manufacturers when required by national regulations (see document C/S S.007, Handbook of Beacon Regulations).
Use of the checksum feature is designed to ensure correct initial registration of beacons and is not designed for checking changes to beacon registrations or changes to the Hex ID that might be implemented in the field (for example to change the Country Code when a beacon changes flag-state).

The algorithm for calculating the beacon checksum and guidelines for its use can be found in document C/S G.005, Guidelines on 406 MHz Beacon Coding, Registration and Type Approval.

7.3 Duplicate Registrations

7.3.1 Registration of duplicate beacon identification codes (Hex IDs) shall not be permitted.

7.3.2 During the initial portion for the registration process of a new entry the IBRD user interface software shall:

a) advise the user to wait while the duplicate check is run;
b) compare the entry of the new beacon identification code against the existing records; and
c) terminate the registration process if a duplicate is found, and provide proper guidance to the Data Provider on how to proceed.

7.4 Record Fields Set from Beacon Decode

7.4.1 Where possible, record fields shall be automatically set to the values directly decoded from the beacon identification code. These fields are (see detailed description in Annex A):

a) country code;
b) beacon type (ELT, EPIRB or PLB);
c) coding protocol;
d) activation mode (automatic / manual); and
e) C/S type approval certificate number (when encoded).

7.4.2 If the user attempts to override the content of the fields directly decoded from the beacon identification code, the IBRD user interface shall display the appropriate warning. However, user override of the country code and coding protocol number shall not be allowed.

7.4.3 For designated fields the IBRD shall record both decoded values and user provided data.

7.5 Field Logical Content

Where possible, fields shall be verified for proper logical content and general format, and proper guidance shall be provided on how to proceed if verification fails. The fields to be verified for proper logical content and general format shall include as a minimum:

a) the Hex ID (beacon identification code) – only hexadecimal characters and exactly 15 or 23 characters in length (see also section. 7.1); and
b) Vessel/Aircraft capacity (no. of persons on board) - must be numerical.

7.6 Field Relational Content

7.6.1 The following fields to be entered by a user shall be verified for proper relational content:

a) MMSI versus country code; and

b) Radio Call Sign versus country code.

7.6.2 A visual warning and proper guidance shall be provided on how to proceed if verification fails.

7.7 Field Length/Type/Range

7.7.1 Before the final step of insertion into the IBRD database, all field entries shall be checked for validity, as a minimum with regard to:

a) length in bytes (or characters);

b) data type (e.g., numerical, text, date etc.);

c) range (the "practical range" (e.g. 10 to 1,000) may be provided on a per field basis in Annex A. When no "practical range" is given in Annex A, the range as defined by the field type in the database shall be applied); and

d) any additional specific field criteria or constraint given for each field definition in Annex A.

7.7.2 A visual warning and proper guidance shall be provided on how to proceed if verification fails.

7.8 Required Fields

Required fields shall be marked in a very obvious way according to industry standards. If not filled in, a visual warning message should appear.

7.9 Provision of Accepted Values

In the event of an error or warning message, the IBRD shall provide an example of accepted values.

- END OF SECTION 7 -

8. REPORTS AND QUERIES

8.1 Monthly/Annual Statistics

8.1.1 The IBRD shall provide tools for use by the Database Administrator to compute and report basic monthly and annual statistics, including:

a) new registrations entered into the database;

b) number of SAR Logins; and

c) beacons recorded with special status (e.g., replaced, sold, stolen, lost, out of service, destroyed).

8.1.2 Registration counts shall be broken down according to:

a) beacon manufacturer;

b) communication language; and

c) country code.

8.1.3 The Database Administrator shall have the capability to directly specify the start and end date of any report.

8.2 Searches and Queries

8.2.1 The IBRD user interface shall employ appropriate logic to retrieve and display a list (query result) of beacon records that approximately meet a given set of search criteria, allowing for search criteria with "wildcard" values (unspecified characters in the search string accepted as a match for any character in the searched field). The user shall be able to use wildcard characters anywhere in the search string (could be restricted to a limited number of search fields).

8.2.2 The IBRD user interface shall, as a minimum, process queries based upon any combination (logical AND) of the following fields:

a) Hex ID;

b) vehicle name;

c) owner name;

d) vehicle registration number;

e) radio call sign;

f) MMSI;

g) country/administration name;

h) beacon country code;

i) beacon type;

j) last edit date; and

k) last confirmation date.

l) aircraft 24-bit address;

m) type approval certificate;

n) serial number;

o) special status;

p) email address; and

q) owner username.

8.2.3 The IBRD user interface shall provide access (view and/or modify as allowed on the basis of the user class) to the actual registration information for each record directly from the resulting query list, and a means to return to the query list after viewing a specific record.

8.2.4 The count of records found in the query result shall be provided.

8.2.5 As a minimum the query list shall display the following fields:

a) aircraft 24-bit address;

b) aircraft 24-bit address decoded;

c) type approval certificate;

d) owner name;

e) vehicle registration number;

f) email address; and

g) MMSI.

8.2.6 The IBRD user interface shall provide a capability for re-sorting the resulting query list on the basis on the displayed fields in ascending or descending order.

8.2.7 The IBRD user interface shall provide the Database Administrator with a capability to identify individual records from the query list, and send the full listing of the associated record contents either to a text file or a printer.

8.2.8 The National Data Providers and Data Providers shall have access to a query tool within their own user interface with the same properties as the tool for SAR Services and

Inspectors/Maintenance Personnel; however, they shall only have access to their own beacon records.

8.3 Query Export

The IBRD user interface shall provide the following minimum export capabilities for query results:

a) export the displayed query results to a tab separated value (TSV) text file;

b) export the displayed query results to a comma separated (CSV) text file;

c) export the displayed query results to an XML file; and

d) export the displayed query results to a JSON file.

- END OF SECTION 8 -

9. BULK UPLOAD

This software shall be built with the National Data Provider and owners of multiple beacons in mind. The Bulk Upload is meant to be an "offline" Method of modifying beacon records. The information for the desired beacons is exported out of the IBRD and edited locally by the user's preferred spreadsheet or text editor. When enough beacon records have been created or updated, the National Data Provider or beacon owner shall log in to the IBRD and upload the new/modified beacon records.

9.1 Download

The IBRD interface shall provide means for downloading:

a) all beacon records from the associated country codes of a National Data Provider and;

b) all beacon records from the associated user identification.

9.2 Basic Functionalities

The Bulk Upload software shall emulate all Data Provider aspects of the IBRD software on a local computer. The National Data Provider and Owner shall at minimum be able to:

a) create and/or modify beacon records locally;

b) search for beacon records saved offline; and

c) prepare CSV, XML and JSON bulk upload file for uploading to the IBRD.

9.3 Bulk Upload File

The Bulk Upload software shall allow the National Data Provider and Owner to prepare and save the exported file with new or modified beacon records.

9.4 Data Update

When uploading a file to the IBRD:

- data is automatically created or updated.
- the IBRD shall compare the record "last updated" timestamp from the database to the incoming record. If data is more recent on the live database, the IBRD will allow the National Data Provider and Owner to view the information and confirm changes manually.
- the special status of the beacon should also be updatable from the bulk upload file.

- END OF SECTION 9 -

10. PERFORMANCE

10.1 Database Capacity

The IBRD shall have the capability to accommodate the current and forecast beacon population, for up to 30,000,000 beacon registrations with capacity to expand beyond this volume if required.

10.2 Availability

10.2.1 The IBRD shall be available for operational use 99.5% of the time on an annual basis.

10.2.2 The IBRD shall not remain continuously unavailable for time periods of more than 2 hours.

10.3 Maximum Response Time

10.3.1 The IBRD shall provide a timely response to Data Provider requests and inputs. The IBRD total processing time, including the recording of new or modified data in the IBRD database and the transmission of any response to the Internet entry point, shall not exceed 10 seconds.

10.3.2 The IBRD user interface shall display on the Data Provider's computer screen a "time passage" indicator (such as an "hourglass" or a "progress bar") when the processing time exceeds 2 seconds.

10.3.3 The IBRD shall process bulk record inputs from National Data Providers, including the transmission of the appropriate response at the entry point of the communication network, within a time period that does not exceed 10 seconds per processed record.

10.3.4 The IBRD shall provide a response to a SAR service query within 10 seconds of receipt, at the Internet entry point.

10.4 User Load

The IBRD shall meet the above requirements with up to 100 simultaneous users.

- END OF SECTION 10 -

11. IBRD MAINTENANCE

11.1 Backup

The IBRD shall provide means for backup on a routine schedule. The backup operation shall copy the entire IBRD database to an external repository that can be stored separately from the IBRD system.

11.2 Monitoring

The IBRD shall provide tools and displays that allow routine monitoring of the IBRD status and operation by the Database Administrator, with the objective of ensuring security / availability of proper system operation.

11.3 Maintenance Notifications

The IBRD shall provide means for adding special messages to the Home page in case of maintenance or other special events regarding the IBRD software.

- END OF SECTION 11 -

ANNEX A

INTERNATIONAL BEACON REGISTRATION DATABASE DATA ELEMENTS

The following data elements represent the minimum required elements to satisfy the needs of SAR services and database access. Additional data elements may be required for use by the application database software. Mandatory data elements are required for a beacon registration to be entered. Latin characters (with different accents) shall be accepted in the database.

A.1 Beacon Data

Data Name	Description	Mandatory User Input	Source *
Beacon Hexadecimal ID	Bits 26-85 of 406 MHz beacon message. Expressed as 15 or 23 hexadecimal characters. Encoded position bits set to default values.	Yes	data provider
C-S TAC Number	Cospas-Sarsat beacon type approval number		data provider or beacon decode
Beacon Type	Type of beacon, i.e, EPIRB, ELT, PLB.		beacon decode
Beacon Country	Administration where beacon is registered	Yes	beacon decode
Beacon Protocol	Protocol used for beacon coding		beacon decode
Activation Mode	Automatic or Manual activation capability of beacon		data provider
Beacon Manufacturer	Name of manufacturer of beacon		data provider
Beacon Model	Model name of beacon		data provider
Serial Number	Serial number of beacon		beacon decode
Beacon Status	Indicates if the beacon is in-use, lost, stolen, sold, adrift, etc. Data should be from drop-down menu		data provider
Previous Beacon Status	Store the previous status of the beacon when provided (see above)		data provider
Beacon Homing Device	Frequency or type of homing device. Drop-down menu should be used for data provider input.		data provider or beacon decode
Additional Data	Any other information on the beacon that may be useful, e.g., manufacturers' serial number.		data provider
Last Update Date	Date data last updated		database
Confirmation Request Date	Date request for confirmation email sent		database
Original Registration Date			database

Note: * Where the source indicates “beacon decode” or “database”, the field will be automatically provided by the IBRD, whenever possible.

A.2 Beacon Owner Information

Data Name	Description	Mandatory User Input	Source
Owner Name	Full personal name, company name, or government agency name	Yes	data provider
Owner Password	User password	Yes	data provider
Owner Address	Street, city, country, postal code		data provider
Owner email	Email address of beacon owner		data provider
Communication Language	Preferred language of verbal communication		data provider
Medical Information	List any relevant medical information such as medications or conditions		data provider
Owner phone number and type	Contact numbers for beacon owner including type such as phone, fax, mobile, etc.	Yes	data provider
Challenge Question	Challenge question user selected for supporting re-instatement of password	Yes*	data provider
Challenge Response	Challenge response user selected for challenge question for supporting re-instatement of password	Yes*	data provider
Additional Notes	Any other information on the beacon owner that may be useful.		data provider

Note * Mandatory for Beacon Owners and Block Owners only, not mandatory when registration is controlled by a National Data Provider.

A.3 Emergency Contact Information

Data Name	Description	Mandatory User Input	Source
First Emergency Contact Name	Name of primary emergency point of contact	Yes	data provider
First Emergency Contact Address	Address of primary emergency point of contact		data provider
First Emergency Contact Phone Numbers (up to 4)	Phone number and type for primary emergency point of contact	Yes	data provider
Second Emergency Contact Name	Name of second emergency point of contact		data provider
Second Emergency Contact Address	Address of second emergency point of contact		data provider
Second Emergency Contact Phone Numbers (up to 4)	Phone number and type for second emergency point of contact		data provider

A.4 Vehicle Information

For ELT beacons

Data Name	Description	Mandatory User Input	Source
Vehicle Type	Vehicle code for aircraft, vessel or personal use. Should be selectable from drop-down menu.	Yes	data provider
Vehicle Registration Number	Aircraft's registration number	Yes	Data provider
Home ICAO Code	Aircraft's home ICAO code		data provider
Aircraft Manufacturer	Aircraft manufacturer		data provider
Aircraft Model	Model of aircraft		data provider
Aircraft Colour	Colour of aircraft		data provider
Aircraft Operating Agency	Aircraft operating agency designator and operator's serial number.		data provider
Aircraft Operating Agency Phone Number	Aircraft operating agency phone number		data provider
Radio Equipment	Radio equipment present on aircraft		data provider
Deployable Survival Craft / Equipment	Type and number of survival craft		data provider

Data Name	Description	Mandatory User Input	Source
Fixed Survival Craft / Equipment	Type and number of survival craft		data provider
Max Endurance (h)	Maximum endurance in hours		data provider
Cruise Air Speed (kt)	Cruising air speed in knots		data provider
Length Overall (m)	Overall length of aircraft in metres		data provider
Wing Span (m)	Wing span of aircraft in metres		data provider
Capacity (Crew and Passengers)	Vehicle capacity in numbers of people		data provider
Aircraft 24-bit Address (decoded)	24-bit address of the aircraft, expressed as 6 hexadecimal characters		beacon decode
Aircraft 24-bit Address (user-entered)	24-bit address of the aircraft, expressed as 6 hexadecimal characters if different from that provided from beacon decode		data provider
Aircraft Nationality	MID country code for vessel flag State or aircraft nationality of registration.		data provider
Additional Vehicle / Usage Information	Any other information on the vehicle or vehicle usage that may be useful.		data provider
Picture 1	Photograph of vehicle		data provider
Picture 2	Photograph of vehicle		data provider

For EPIRB Beacons

Data Name	Description	Mandatory User Input	Source
Vehicle Type	Vehicle code for aircraft, vessel or personal use. Should be selectable from drop-down menu.	Yes	data provider
Vehicle Registration Number	Registration number of vessel	Yes	Data provider
Vessel Name	Name of vehicle or vessel	Yes*	data provider
Vessel Model	Make or model of vessel		data provider
Vessel Port	Vessel's home port		data provider
Vessel Colour	Vessel's colour		data provider
Number of Life Boats	Number of life boats		data provider
Number of Life Rafts	Number of life rafts		data provider
Radio Equipment	Description of radio equipment with a drop down for selection		data provider

Data Name	Description	Mandatory User Input	Source
Radio Callsign (decoded)	Vessel radio call sign or aircraft registration number	Yes*	beacon decode
Callsign (user)	Vessel radio call sign or aircraft registration number if different from that provided from beacon decode.	Yes*	data provider
AIS Number	Automatic Identification System number		data provider
INMARSAT	INMARSAT Number		data provider
Vessel Cellular	Cellular phone number		data provider
Vessel Satellite Phone	Satellite phone number		data provider
MMSI (decoded)	Maritime Mobile Service Identity	Yes*	beacon decode
MMSI (user)	Maritime Mobile Service Identity if different from that provided from beacon decode.	Yes*	data provider
Length Overall (m)	Overall length of vessel in metres		data provider
Capacity (Crew and Passengers)	Vehicle capacity in numbers of people		data provider
Vehicle Nationality	Nationality of vehicle		data provider
Equipped with Simplified Voyage Data Recorder	Drop down Yes or No		data provider
Additional data	Any other information on the vehicle or vehicle usage that may be useful.		data provider
Picture 1	Photograph of vessel		data provider
Picture 2	Photograph of vessel		data provider

Note: * Only one of the marked entries is mandatory.

For PLB Beacons

Data Name	Description	Mandatory User Input	Source
Vehicle Type	Vehicle type for aircraft, vessel or personal use. Should be selectable from drop-down menu.	Yes	data provider
Specific Usage	Should be selectable from drop-down menu.		Data provider
Additional Vehicle / Usage information	Any other information on the vehicle or vehicle usage that may be useful. Details of any secondary uses of PLBs may be included.		data provider

- END OF ANNEX A -

- END OF DOCUMENT -

Cospas-Sarsat Secretariat
1250 Boul. René-Lévesque West, Suite 4215, Montréal (Québec) H3B 4W8 Canada
Telephone: +1 514 500 7999 / Fax: +1 514 500 7996
Email: mail@cospas-sarsat.int
Website: www.cospas-sarsat.int