ANNEX E

COSPAS-SARSAT STANDARD FOR THE TRANSMISSION OF MESSAGES VIA FTP

E.1 FILE TRANSFER PROTOCOL (FTP) COMMUNICATIONS

Each ground segment facility (e.g., MCC or LUT) communicating via FTP shall comply with the applicable standards described in the Internet Engineering Task Group document RFC 959 - File Transfer Protocol, which can be found at the following web address: www.ietf.org.

E.1.1 FILE NAMING CONVENTION

A ground segment facilityshall send a message by writing a file on the FTP server of the receiving facility. Each file shall contain exactly one message.

The FTP file name format shall be "?SRCE_?DEST_?CUR#.TXT", where:

- "?SRCE" is the name of the facility that originated this message (www.cospas-sarsat.int),
- "?DEST" is the name of the facility to which this message is being sent (www.cospas-sarsat.int), and
- "?CUR#" is the Current Message Number (Message Field 1).

The FTP file name shall contain only upper case characters. For example, a file with the name "USMCC_CMCC_02345.TXT" contains Current Message Number 02345 sent by the USMCC to the CMCC.

Any facility that wants to receive data via FTP shall provide the Host Name and/or Internet Protocol (IP) Address, User Name, Password, and Message Directory Name in Table F.1, to enable other ground segment facilities to place data on the FTP server of the receiving facility. On a bilateral basis, the receiving and sending facility should agree on passwords and other security measures. It is the responsibility of the receiving facility to provide adequate security for its FTP server.

The sending facility shall write a file with a file name extension of ".TMP" on the FTP server of the receiving facility. A file is given a temporary name to prevent the receiving facility from processing a file before it is complete. Once the file transfer is complete, the sending facility shall rename the file with an extension ".TXT". Once the file has been renamed, the sending facility shall not manipulate the file. The receiving facility shall not process files with an extension of

".TMP". The receiving facility shall be responsible for disposing of files placed on its FTP server.

If the receiving MCC detects an anomalous condition in the FTP file transfer, it shall notify the transmitting MCC. If an FTP file transfer fails for any reason the transmitting MCC shall try to resend the message, and notify the receiving MCC if the failure persists.

If the receiving MEOLUT detects an anomalous condition in the FTP file transfer, it shall notify its associated MCC. If an FTP file transfer fails for any reason the transmitting MEOLUT shall maintain a 10 minutes buffer of messages. Upon re-establishment of a connection the transmitting MEOLUT shall send the buffered messages. If MEOLUT FTP file transfer failures persist, the transmitting MEOLUT shall notify its associated MCC.

Each facility communicating via FTP shall operate in binary transfer mode.

E.2 FILE TRANSFER PROTOCOL (FTP) INFORMATION LIST

A list of information used to send messages to a facility via FTP is provided in this section. This list is composed of 6 items:

1. Receiving Ground Segment Facility.
2. Host Name.
3. IP Address.
4. User Name.
5. Password.
6. Message Directory Path.

E.2.1 Receiving Ground Segment Facility

The name of the ground segment facility to receive data via FTP. For an MCC, this name matches the MCC Identification Code in the Cospas-Sarsat website, www.cospas-sarsat.int. For a MEOLUT, this name matches the MEOLUT name in the Cospas-Sarsat website, (www.cospas-sarsat.int), noting that spaces are always replaced with an underscore ("_") character.

E.2.2 Host Name

This is the FTP Host Name of the receiving ground segment facility. ***

E.2.3 Internet Protocol (IP) Address

This is the Internet Protocol Address referenced to reach the receiving ground segment facility. ***

E.2.4 User Name

The User Name required to login to the FTP server of the receiving facility. If the value is "Sending Ground Segment facility Name", then the user name is the name of the sending ground segment facility, per the Cospas-Sarsat website (www.cospas-sarsat.int). ***

E.2.5 Password

The password required to access the FTP server of the receiving facility. ***

"*** indicates that the information is provided on a need to know basis."

E.2.6 Message Directory Path

The path of the directory into which message files shall be written. <facilityname> indicates that each facility will put messages in a sub-directory per facility, where the sub-directory name is the name of the sending facility, per the Cospas-Sarsat website, (www.cospas-sarsat.int).

E.3 SECURITY

All ground segment facilities with an Internet connection must be protected by firewall technology.

E.3.1 Passwords

Ground segment facilities shall formulate passwords using security best practices. The passwords shall have the following characteristics:

- contain at least 8 characters,
- not have any characters that are "blank",
- six of the characters shall occur once in the password,
- at least one of the characters must be a number (0-9) or a special character (~,!,$,#,%,*) – see Table E.1,
- at least one of the characters must be from the alphabet (upper or lower case),
- passwords shall not include:
  - words found in any dictionary (English or other language), spelled forward or backward,
  - system User Ids,

- addresses or birthdays,
- common character sequences (e.g., 123, ghijk, 2468),
- vendor-supplied default passwords (e.g., SYSTEM, Password, Default, USER, Demo),
- words that others might guess.

Ground segment facilities shall change passwords at least semi-annually.

To protect passwords from unauthorized disclosure facilities shall exchange passwords by telephone or facsimile if allowed by security authorities at each facility. Facilities shall coordinate the exchange of new passwords during the last full work week of April and October of each year. Facilities exchanging passwords shall agree on an implementation date that is not later than the end of the week during which new passwords are exchanged.

Table E.1: FTP Password Special Characters

SYMBOL	NAME
~	TILDE
!	EXCLAMATION POINT
@	AT SYMBOL
#	OCTOTHORPE
$	DOLLAR SIGN
%	PERCENT
^	CHAPEAU / HAT
&	AMPERSAND
*	ASTERIX
)	CLOSE PARENTHESES
(	OPEN PARENTHESES
`	APOSTROPHE
-	HYPHEN
“	QUOTATION
/	SLASH

E.3.2 Access

Access permissions on all directories and files on the FTP server shall follow the principle of “least permissions” to ensure that no unauthorized access is allowed. “Least permissions” means that each user is granted the minimum access required to perform their assigned tasks.
Facilities shall check IP addresses to limit server access only to authorized users.

Facilities shall allow access to their FTP servers only through ports 20 and 21. All other ports that are not being used shall be closed.

E.3.3 Anonymous FTP

Facilities shall not use anonymous FTP.

E.3.4 Encryption of Critical Information

Facilities shall implement methodologies to encrypt FTP login names (userids) and passwords during file transmission to prevent unauthorized disclosure. These methodologies include FTP over Internet Virtual Private Network (VPN). Standards for the use of hardware VPN are contained in Annex F.

E.3.5 Monitoring for a Potential Security Breach

Facilities shall monitor the FTP servers for abnormal activity. If a breach of security is found, ground segment facilities shall notify all FTP correspondents as soon as possible to minimize exposure.

Examples of items that should be monitored on a FTP server include:

Event logs:
should be set and checked for failed login attempts,
gaps in time and date stamps,
attempts to elevate privileges;

Disk Space:
unexplained loss of disk space,
unexplained disk access;

Unexplained events:
large number of failures (system or programs crash),
unexplained process or programs running,
new users added,
virus protection has been disabled.

E.3.6 Security Patches

Facilities shall apply the latest software and security patches to their FTP servers as soon as possible.

- END OF ANNEX E -