INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

ASIA/PACIFIC REGIONAL GUIDANCE MATERIAL FOR THE USE OF THE PUBLIC INTERNET FOR THE AFTN

VERSION 1.0

AUGUST 2003

CONTENTS

EXECUTIVE SUMMARY

This document presents the various issues that need to be addressed before implementing a system that uses the Public Internet to support low speed AFTN. These areas include conducting a safety case analysis that identifies risks and mitigation plans, ensuring that security measures are implemented in order to protect the integrity of the AFTN from external unauthorized sources. The use of appropriate logging and audit reporting required ensuring conformity and integrity of the service.

The document also covers the need for appropriate contract agreements to be put in place with end users to ensure that they do not abuse or allow the system to be misused.

Examples of a safety case and a contract agreement documents are also included in appendices to the document to illustrate the sort of subject matter that should be considered.

1 Introduction

The purpose of this document is to provide guidance for the use of the public Internet technology to support low speed AFTN, where required.

2 Purpose

There are a number of States where dedicated low speed AFTN facilities are either not available or unaffordable. Such stations have been receiving and sending AFTN by fax or phone.

The costs associated with using the above method are high because the connection calls are charged at ISD rates. The process also is labor intensive and may result in a higher than necessary workload for staff. Such stations are ideally suited for which this Internet type of service delivery is more convenient and economical until the operational requirement dictates a need for a dedicated AFTN/ATN links.

3 Assessment Process

There are several assessments that should be followed to ensure that the system is implemented in a safe and secure manner. These are outlined in the following sections.

3.1 Risk Assessment

Before considering the development and implementation of a system that utilizes the internet for delivery of AFTN, a * Safety Hazard Analysis must be conducted. The Safety Hazard Analysis should identify hazards and the risks associated with the hazards. Once the risks are identified they must be mitigated against. The following table illustrates the minimum hazards that will need addressing. Additional hazards may be realized depending on the situation.

Safety Requirement	**Hazards**	**Safety Requirement Explanation**	**Met/Yet to be met**
1. Customer contract specifications	1. Risk of Customer of failure to receive data. 2. Risk to Customer due to corrupted or missing data. 3. Risk to Customer due to bogus data. 4. Risk to Customer due to delayed data 5. Risk to Customer due to flooding of data. 6. Risk to Customer due to messages sent to incorrect address 7. Risk to Customer due to Virus in system (internal or external generated). 9 Inbound messages. System failure or degraded operations	Customers will be made aware, through the contract, of the limitations of this service due to outside ISP issues. This will include user contingency arrangements during outages or if corrupted data is received on a regular basis.	Met

Safety Requirement	**Hazards**	**Safety Requirement Explanation**	**Met/Yet to be met**
	from the Provider		
2. Anti-hacking strategy	8. INBOUND- Hacking into System.	1.URL for send screen - limited distribution- as per contract restrictions. 2. Must have registered user name & password. 3. A user name and password can not have duplicate sessions running at a time. 4. Access is through main web server with an ASP page front end. Prevents direct TCP-IP connection from end-user to server. 5. AFTN Protocol (async) between switch and Server. 6. All IP addresses are logged.	Met
3. Server parameters to limit number of incoming messages per minute	8. Inbound Hacking into System	The AFTN/Internet Server parameter will limit the number of incoming messages from the customer to the server to a factor of 'X' messages at time. This factor will be checked over a period of mili- seconds to ensure the X factor is not reached	Met
4. Encryption of data from customer	8. Inbound Hacking into System	The system uses SSL (Secure Socket Layer) to encrypt any data sent from the user to the server. This ensures that the data sent from the user cannot be read. SSL is used by the banking industry to secure transactions	Met

Safety Requirement	**Hazards**	**Safety Requirement Explanation**	**Met/Yet to be met**
5. HTML page	10. Inbound - Incorrect users data received by The Provider	HTML pages are designed to ensure correct AFTN format for messages. Use of preformatted templates eliminates errors in the AFTN message format.	met
6. Users AFTN training	10. Inbound - Incorrect users data received by system	All contracted users of the gateway will have been trained in AFTN message handling procedures or will be provided with appropriate training prior to using the system. A user Operating procedures manual will also be provided for quick reference of the user.	Met

* See Appendix A for an outline of a Hazard Analysis.

3.2 Security

To maintain the integrity of the AFTN the following security measures must be employed as a minimum to protect against abuse of the system by unauthorized user.

- The system server must maintain a database of authorized web users.
- Usernames and passwords must consist of no less than six alphanumeric characters and no greater than eight alphanumeric characters.
- Usernames and passwords must be treated confidentially in the same way as pin numbers are for bank cards. The security codes shall not be disclosed to any unauthorized user.
- There shall be only one user session allowed at one time for individual user accounts. Any attempt to logon to the system by more than one session for a user will result in that attempt being disallowed by the web server.
- The URL for the website must be hidden from public view. It is not to be published and no hyperlinks from home pages or other web sites are to be used allowed.
- The site must use a secure connection (Secure Sockets Layer or SSL protocol 128 bit encryption) utilising an SSL server.

- The user must type in the URL starting with 'https' otherwise the user will receive a message warning that 'https' must be used.
- Session authentication must be implemented on either the client (using cookies etc) or client and web server (session tracking).
- The web server must provide a 'lockout' facility that locks a web user out from the system when excessive amounts of AFTN messages have been received by a web user. This protects against flooding of the system by a potential hacker.
- The web server should be protected from direct exposure from the internet. The main ATC web server should direct any AFTN web requests to a middle proxy server which then on forwards requests to the AFTN web server. This protects the AFTN web server from direct TCP-IP connections from the Internet.
- Internet firewall protection shall be utilised.
- All transactions must be logged. IP addresses, user names and transaction information are to be logged for each transaction and time stamped by the web server.

3.3 Logging and Auditing

A system that supports AFTN over the internet must maintain a log of all the different types of transactions that occur between the server system and web user, mail server and AFTN switch. The following points indicate the various areas that system logging should cover.

- The system shall maintain an AFTN message transaction log file.
- The system must archive all received and transmitted AFTN messages for 30 days.
- The AFTN message transaction log file must contain the original message information that is received or transmitted by the system.
- Each transaction stored in the database must be time stamped with the server time.
- Each Web transaction stored must be stamped with the identification of the user (obtained from their original logon) and user IP address.
- Additional a system log shall be kept to store system related messages.

3.4 Formulation of Contract Agreements

Because there are security issues involved with setting up an internet based system that connects to the AFTN, *contractual agreements need to be formally established between the party supplying the AFTN Internet Gateway access and any external party's utilising the facility. These contract agreements are to be put in place with end users to ensure that they do not abuse or allow the system to be misused. When formulating a contract agreement besides the normal contractual information the contract must address the following areas that are specific to setting up a system that allows access to AFTN via the internet.
The customer must:

- ensure that the services are only accessed from the designated sites;
- ensure that the procedures for AFTN circuit that conform to the requirements specified in International Standards and Recommended Practices, Annex 10 to the Convention on International Civil Aviation, are used at all times;

- not cause or authorize any Internet site to be linked with the AFTN Internet Gateway Internet sites without prior consent of the AFTN Internet Gateway provider;
- treat all Security Information as confidential and should not, without prior written consent of the provider, disclose the Security Information to any person (including persons within Its own organisation) or not use the security information for any purpose other than the purpose for which it is provided by the provide;
- ensure that only users at a Designated Site have access to, and knowledge of, the Security Information specific to that Site;

- lodge, through the Help Desk, a request for a new Security Information when the membership of a user group changes in any way;

* See Appendix B for an example of a Contract agreement.

4 System Recommendations

4.1 Acronyms

AFTN	Aeronautical Fixed Telecommunications Network
AFTN Gateway	The gateway sever that provides the Internet email/web conversion between the AFTN switching device and the internet/intranet
ASP	Active Server Pages
ATS	Air Traffic Services
COOKIE	A small text file kept on the client computer that is used to track user's activity
CGI	Common Gateway Interface
CSN	Channel Sequence Number (AFTN Message CSN)
DTG	Date Time Group
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISP	Public Internet Service Provider
ISD	International Subscriber Dialing
PC	Personal Computer
PERL	Program Language
SSL	Secure Sockets Layer protocol
TCP-IP	Transmission Control Protocol-Internet Protocol

4.2 System software

The system should consist of the following software components:

- Operating system
- Web server
- Web server program to handle and process web form submissions (Eg: CGI, ASP, PERL etc)
- Program/s to handle AFTN switch to Email conversion and web form to AFTN format conversion including message error handling and logging.

4.3 Equipment Hardware Specifications

4.3.1 Hardware

The AFTN Gateway system hardware for the Operational System shall be Commercial off the Shelf (COTS).

The hardware should be proven hardware, which is demonstrably suitable for use in a critical system with the reliability requirements of the AFTN Gateway system.

It shall consist of at least the following minimum components:

(a) Pentiumn III CPU

(b) 264 Mb of RAM

(c) LAN Card.

(d) Two standard Serial Ports

(e) CD Drive.

(f) 20 G Hard Drive

The system shall consist of two servers, an on-line server and an off-line server.

The on-line server keeps an up to-date message database and is connected to both the AFTN and intranet/internet.

The off-line server is not connected to the AFTN or intranet/internet. It contains the same configuration information as the on-line server but the message database will not be current or may be empty.

Upon complete failure of the on-line server the AFTN and network connection may then be transferred to the backup server which will become on-line.

4.3.2 System Interfaces

- AFTN interface
- Optional station clock (UTC time reference)
- Network connection (TCP/IP) Internet/Intranet connectivity.

AFTN Interface

(a) interfaces to the AFTN through an asynchronous connection (RS232 port)

(b) ensures the availability of the connection both to and from the AFTN host;

(c) controls the flow of data to and from the AFTN host;

(d) receive messages from, and transmit messages to, the AFTN host;

(e) checks received AFTN message Channel Sequence Numbers (CSNs) for consistency;

(f) utilises SVC QTA MIS for missed messages;

(g) has the abilty to retrive transmitted missed message/s from the message database;

(h) provides transmission of CH messages every 20 minutes;

(i) should be able receive and process CH and test messages from the AFTN host;

Optional Station Clock Interface

(a) time synchronisation, be connected to the UTC time reference, interface to the Station Clock.

(b) In the absence of a station clock, the system clock shall have an accuracy of 10 seconds for a period of 1 week.

(c) The clock will be within 1 second of the station clock when the station clock is available.

Network Interface

(a) Controls the conection to the mailserver/internet

4.4 Reception of AFTN Web messages

The Web User interface consists of a series of web pages.

(a) A Web page for username and password verification and login.

(b) The AFTNGateway web site must have a number of web forms that allow the input of various types of standard ICAO AFTN messages FreeText ,FPL, ARR, CHG, DEP, CNL, DLA,EST, Notam, etc.

(c) The web site may also support AFTN message templates that can be saved and recalled at a later time.

(d) The origin address must be automatically generated based on user login.

(e) Upon reception of an AFTN web message the AFTNGateway server will insert the date time group (DTG) into the AFTN message.

(f) Form field validation must be supported on both the client side and server side.

(g) An AFTN Web form submission confirmation page, verifying receipt of web message at the web server.

(h) A number of Web pages the warn the user of logon errors, database errors etc.

(i) The AFTNGateway web server will generate a four (4) digit web sequence number that is associated with the AFTN message submitted that can be used to identify and track the message submited by individual AFTNGateway web users.

(j) The AFTNGateway web server will automatically generate a email as receipt message for the web user submission which will be sent to the web user as a record for the transaction.

(k) The web server must support Internet Explorer and Netscape browsers.

4.5 Transmission of AFTN Email messages

(a) The AFTNGateway server must provide a database with a table of AFTN to Email address translations.

(b) Email messages generated from AFTN messages will be allocated an individual Email Sequence Number for each user consisting of four (4) digits.

(c) There must be a provision for e-mail 'CH' messages to be sent to the user every 20 minutes.

(d) A change of day message must be sent at 0000 to all e-mail users notifying users of change of day and reset of e-mail sequence number back to one (0001).

(e) An AFTN SVC message shall be sent to the AFTN COM centre/station in the event that the AFTNGateway server cannot connect to the mail server.

(f) An AFTN SVC message shall be sent to the AFTN COM centre/station in the event that the AFTNGateway server cannot find an e-mail address for the AFTN address.

(g) The e-mail sequence number shall be reset at start of day.

(h) The e-mail sequence number shall be reset when the server is re-started.

(i) The sender field of the generated AFTN e-mail message shall be the e-mail address of the AFTN COM centre/station.

(j) The subject field of the generated AFTN e-mail message shall consist firstly of the four digit e-mail sequence number followed by up to forty character of the first line of text of the AFTN message.

Example: (Email Sequence Number)

0035 METAR NWWW 140000Z 27008KT 220V300 9999

up to 40 characters

(k) It is the responibility of the end user to check the email account for missed messages.

4.6 Security

(a) The AFTNGateway server must maintain a database of authorised web users.

(b) Usernames and passwords must consist of no less than six alphanumeric characters and no greater than eight alphanumeric characters.

(c) Usernames and passwords must be treated confidentially in the same way as pin numbers are for bank cards. The security codes shall not be disclosed to any unathorised user.

(d) There shall be only one user session allowed at one time for individual user accounts. Any attempt to logon to the system by more than one session for a user will result in that attempt being disallowed by the web server.

(e) The URL must be hidden for the AFTNGateway website. It is not to be published and no hyperlinks from home pages or other web sites are to be used allowed.

(f) The site must use a secure connection (Secure Sockets Layer or SSL protocol 128 bit encryption) utilising an SSL server.

(g) The user must type in the URL starting with ‘https’ otherwise the user will receive a message warning that ‘https’ must be used.

(h) Session authentication must be implemented on either the client (using cookies etc) or client and web server (session tracking).

(i) The AFTNGateway web server must provide a ‘lockout’ facility that locks a web user out from the system when excessive amounts of aftn messages have been received by a web user. This protects against flooding of the system by a potential hacker.

(j) The AFTNGateway web server should be protected from direct exposure from the internet. The main ATC web server should direct any AFTN web requests to a middle proxy server which then on forwards requests to the AFTNGateway web server. This protects the AFTNGateway web server from direct TCP-IP connections from the Internet.

(k) Internet firewall protection shall be utilised.

(l) All transactions must be logged. IP addresses, user names and transaction information are to be logged for each transaction and time stamped by the web server.

4.7 Archiving and Reviewing Data

(a) The AFTNGateway system shall maintain an AFTN message transaction log file.

(b) The AFTNGateway system must archive all received and transmitted AFTN messages for 30 days.

(c) The AFTN message transaction log file must contain the original message information that is received or transmitted by the AFTN Gateway system.

(d) Each transaction stored in the database must be time stamped with the AFTNGateway server time.

(e) Each Web transaction stored must be stamped with the identification of the user (obtained from their original logon) and user IP address.

An example of the format of the AFTN message transaction log file is shown here:

14/11/2001 00:10:19
---INCOMING---
THE FOLLOWING AFTN MESSAGE WAS RECEIVED:
! TEE0002 140010
GG ABCDYSYX
140010 NWBBYMYX
" SANC20 NWBB 140000
METAR NWWW 140000Z 27008KT 220V300 9999 SCT023 BKN056 30/21
Q1015
NOSIG=

14/11/2001 00:10:20
---OUTGOING---
EMAIL FOR Pacific FIS(Pacific@yahoo.com.au)
WITH SEQ NO OF 0002 SUCCESSFULLY SENT FOR FOLLOWING
AFTN MESSAGE:
TEE0002 140010
GG ABCDYSYX
140010 NWBBYMYX
SANC20 NWBB 140000
METAR NWWW 140000Z 27008KT 220V300 9999 SCT023 BKN056 30/21
Q1015 NOSIG=

The system must log user login and system information.

Examples of the format of these types of messages that may appear in the transaction log file are shown here:

8/11/2001 00:35:35
EMAIL Connect Failed
--- Welcome to a new day ---

Your last Email Sequence Number was 0023.
This message has reset your sequence number to 0001.

8/11/2001 00:37:45
AFTN PROCESS TERMINATED

8/11/2001 00:37:45
EMAIL PROCESS TERMINATED

8/11/2001 00:37:45
LOGGER PROCESS TERMINATED

8/11/2001 00:59:30
AFTN SVC Message - EMAIL NOW SENT AFTER PROBLEMS
SVC Message from AFTNGATEWAY.
Email with sequence number: 0023
was Successfully sent.

4.8 System Start up and Recovery

At system start up the AFTNGateway system shall automatically notify all users via e-mail that the system has been restarted and all user e-mail sequence number shall be reset to one (0001).

The following illustrates the contents of a typical e-mail restart message.

The system has RESTARTED.
Your last e-mail Sequence Number was 0356.
This message has reset your sequence number to 0001.

4.9 End User Equipment and software

- Standard PC
- Any email program or web based mail
- Internet Explorer or Netscape browser
- Email account dedicated to reception of AFTN messages

APPENDIX A - USE OF AFTN OVER THE PUBLIC INTERNET HAZARD ANALYSIS

The following sections should be considered and included in the Hazard Analysis.

INTRODUCTION
EXECUTIVE SUMMARY
SCOPE
CONFIGURATION DESCRIPTION
- Provide a full description on how the system is to be configured.

SYSTEM OPERATION
- Provide details on how the system operation will work.

ASSUMPTIONS
- List all assumptions associated with how the system will be implemented.

SAFETY REQUIREMENTS DERIVATION
- State how the safety requirements were derived.

SAFETY REQUIREMENTS
- Outline the safety requirements identified for this system.

DESIGN PROCESS
- Outline the design process that will be applied to develop the system.
- This should include System Test Plans, Engineering Readiness Checklist, Operational Readiness checklist, Commissioning process and Service Agreements.

DESIGN AUTHORITY
- Identify who is the design authority for the system.

STATUTARY AND REGULATORY REQUIREMENTS
- Identify the regulations that will apply to various parts of the system.

DEPENDENCIES, LIMITATIONS AND SHORTCOMINGS
- List all dependencies, limitations and shortcomings that are known about the system.

INSTALLATION, INTEGRATION COMMISSIONING AND TRANSITION INTO SERVICE PROCESS
- Detail the process that will be followed for the installation, integration commissioning and transition into service criteria.

OPERATION, MAINTENANCE AND PERFORMANCE MONITORING
- Identify who will be carrying out the operation, maintenance and performance monitoring of the system.

OPERATIONAL PROCEDURES
- List the operational procedures documents that will be used to operate the system.

ENGINEERING PROCEDURES
- List the engineering procedures documents that will be used to maintain and manage the system.

CHANGE CONTROL
- Identify the change control process that will be used to manage the configuration and engineering changes to the system.

SUPPORT

- Identify the support arrangements that will be put in place to manage and maintain the support of the system.

STAFF

- Identify the staff responsible for supporting the system and their level of technical certification for the system.

CONCLUSION

- List the conclusions about whether or not the system is low risk to the safety of the National Airways System and that all risks identified have been mitigated to a reasonable level that is practical.

REVIEW

- Identify if a review of the hazard analysis will be ongoing and if so the period in which a review must take place.

APPENDIX A - Hazard Report

- Contains the detail report on the hazards that have been identified and the plan on how they will be mitigated, the safety requirements and the effect on customers and operations.
- The report may be in the form of a table as shown below.

Project *The Project Name*

Status: Active

Description	Hazard Initiation	Mitigation Plans	Effect	Safety Requirement	Comments

APPENDIX B - Safety Management and Methodology

- Contains the methodology in how the safety management process works in your organisation.

APPENDIX B – EXAMPLE OF A CONTRACT AGREEMENT

THE PROVIDER'S NAME

THE USER'S NAME

[Product Name] AGREEMENT

AGREEMENT made **BETWEEN**

The Provider

AND:

The User ('**You**')

1. **INTRODUCTION**
2. **DEFINITIONS**
3. **TERM OF CONTRACT**
4. **PROVISION OF THE SERVICES**
5. **RESPONSIBILITIES OF THE CUSTOMER**
6. **FEE**
7. **TAXES**
8. **INTELLECTUAL PROPERTY**
9. **LIABILITY**
10. **LIMITATION OF LIABILITY**
11. **SECURITY INFORMATION**
12. **IMMEDIATE TERMINATION**
13. **TERMINATION FOR CONVENIENCE**
14. **FORCE MAJEURE (such as** The Provider will not be liable for any loss, damage, expense or charge of any kind for failure to perform the Services due to any event beyond its reasonable control, such events to include, but not be limited to, unsuitable weather conditions; fire; storm, flood, earthquake or any other Act of God; labour dispute or transportation embargo; act or omission of a government or other competent authority; viruses, catastrophic hardware failures, usage spikes, attacks on The Provider servers, an inability to transit or receive information over the Internet, and changes to any laws or regulations or the making of any legally enforceable orders frustrating the effectual performance of this Contract**)**
15. **PRESERVATION OF RIGHTS**
16. **ASSIGNMENT AND NOVATION**
17. **ENTIRE CONTRACT AND VARIATION**
18. **SEVERABILITY**
19. **WAIVER**
20. **GOVERNING LAW**

SIGNED AS AN AGREEMENT

EXECUTED by **THE PROVIDER**)
by its authorized officer)
)

Signature of witness

Signature of authorized officer

Name of witness

Name of authorized officer

EXECUTED by **The User** by its Authorized officer)
)
)

Signature of witness

Signature of authorized officer

Name of witness

Name of authorized officer

SCHEDULE

CONTRACT DETAILS

Clause No.	**Issue**	**Information**
1	**Commencement Date**	
1	**Services**	
1	**Message**	
1, 6	**Fee**	
1, 5.1	**Customer's Information**	***The User's Address***

Clause No.	**Issue**	**Information**
11	**Designated Sites**	**The Designated Sites are:** ***The User's site address***
20	**Notices**	**The Provider**