International Civil Aviation Organization

Fifteenth Meeting of the APANPIRG ATM/AIS/SAR Sub-Group (ATM/AIS/SAR/SG/15)

Bangkok, Thailand, 25 – 29 July 2005

Agenda Item 3: Review and progress the tasks assigned to the ATM/AIS/SAR/SG by APANPIRG

THE USE OF THE PUBLIC INTERNET FOR AERONAUTICAL APPLICATIONS

(Presented by the Secretariat)

SUMMARY

This paper presents details of ICAO State Letter AN 7/11.15-05/7 seeking State views in respect of ICAO guidance for the use of the public internet for aeronautical applications and introduces the draft guidance document "*Guidelines for the Use of the Public Internet for Aeronautical Applications*" (Doc 9855).

1. INTRODUCTION

1.1 ICAO has developed guidance material to facilitate and harmonize the use of the public Internet for aeronautical applications. The development of the guidance material was undertaken in response to Recommendation 4/6 of the Meteorology (MET) Divisional Meeting (2002) which called upon the Organization to develop guidance and criteria for the accreditation and qualification of providers involved in the exchange and dissemination of aeronautical meteorological information via the Internet. In approving the aforementioned recommendation, the Air Navigation Commission agreed that the subject should be considered in a wider context taking into account all types and categories of aeronautical information.

2. DISCUSSION

2.1 Subsequently, the Aviation Use of the Public Internet Study Group (AUPISG) was established to assist the Secretariat in the development of the appropriate guidance material. As a result, the document developed addresses exchange/dissemination of meteorological and aeronautical information service (AIS) products as well as filing/processing of flight plans via the public Internet with due consideration to associated reliability, integrity, accessibility and security concerns.

2.2 A copy of the draft "*Guidelines for the Use of the Public Internet for Aeronautical Applications*" (Doc 9855) has been included as **Attachment B** to this paper, in addition to the ICAO State Letter (**Attachment A**) notifying the availability of the draft guidelines and requesting comments from States, to reach Montreal by 30 July 2005.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) review the draft "*Guidelines for the Use of the Public Internet for Aeronautical Applications*" (Doc 9855) in the context of State Letter AN 7/11.15-05/7; and

b) discuss regional issues in respect of the use of public internet for aeronautical applications.

International Civil Aviation Organization | Organisation de l'aviation civile internationale | Organización de Aviación Civil Internacional | Международная организация гражданской авиации | منظمة الطيران المدني الدولي | 国际民用航空组织

Tel.: +1 (514) 954-6712

Ref.: AN 7/11.15-05/7

21 January 2005

Subject: The use of the public Internet for aeronautical applications

Action required: To note and provide comments to reach Montreal by 30 July 2005

Sir/Madam,

1. I have the honour to inform you that the Organization has developed guidance material to facilitate and harmonize the use of the public Internet for aeronautical applications and seeks your views on the possible need for further ICAO provisions in this regard.

2. The development of the guidance material was undertaken in response to Recommendation 4/6 of the Meteorology (MET) Divisional Meeting (2002) which called upon the Organization to develop guidance and criteria for the accreditation/qualification of providers involved in the exchange and dissemination of aeronautical meteorological information via the Internet. In approving the aforementioned recommendation, the Air Navigation Commission, at the twelfth meeting of its 161st Session on 28 November 2002, agreed that the subject should be considered in a wider context taking into account all types and categories of aeronautical information.

3. Subsequently, the Aviation Use of the Public Internet Study Group (AUPISG) was established to assist the Secretariat in the development of the appropriate guidance material. As a result, the document developed addresses exchange/dissemination of meteorological and aeronautical information service (AIS) products as well as filing/processing of flight plans via the public Internet with due consideration to associated reliability, integrity, accessibility and security concerns. A degree of emphasis is placed in the document on the accreditation of Internet Aviation Service Providers (IASPs) which entails a thorough review of safeguards against information security threats.

4. The development of the guidance material has been undertaken as a first step by the Organization to address the needs of the Contracting States for matters relating to the operational uses of the public Internet. Presently, only a few States are using Internet-based services. However, as the Internet is

999 University Street
Montréal, Quebec
Canada H3C 5H7

Tel.: +1 (514) 954-8219
Fax: +1 (514) 954-6077

E-mail: icaohq@icao.int
Sitatex: YULCAYA

rapidly becoming more accessible and its performance is constantly improving, more States will be considering its use for the provision of certain aeronautical information and services. Application of the guidance material is expected to prevent, or minimize, the possibility of non-compatibility or diverging procedures being adopted by States. It is also expected that, on the basis of practical experience gained in the process, the need for further ICAO provisions relating to the public Internet can be established.

5. The "Guidelines for the Use of the Public Internet for Aeronautical Applications" were considered by the Air Navigation Commission, at the fifth meeting of its 167th Session on 2 November 2004, and are being processed for publication in the form of an ICAO manual. Pending its publication, the draft manual has been posted on the ICAO-NET (under "Other ICAO Publications" which is part of "Electronic Publications") for the immediate use of States. In considering the guidelines, the Commission requested the Secretariat to present the results of a consultation with States and international organizations on the possible need for further ICAO provisions for review by the Commission by the end of 2005.

6. May I, therefore, request that any comments you may wish to make on the possible need for and nature of additional ICAO provisions relating to the use of the public Internet in support of aeronautical applications be dispatched to reach me not later than 30 July 2005.

Accept, Sir/Madam, the assurances of my highest consideration.

for Taïeb Chérif
Secretary General

FOREWORD

This document was developed with the assistance of the Aviation Use of the Public Internet Study Group (AUPISG) to assist States in dealing with the increasing use of the public Internet (hereafter referred to as “the Internet”) for certain aeronautical applications.

This document contains guidelines on the use of the Internet as a means of communication for non-time-critical aeronautical ground-ground applications. The term non-time-critical implies that the information being transferred over the Internet has no immediate effect on an active flight. A degree of emphasis is also placed on material that could help States accredit providers of aviation information via the Internet.

Following the guidelines of this document will hopefully prevent or minimize the possibility of non-compatible/ diverging procedures being adopted by States and international organizations that choose to use the Internet for certain operational applications.

The guidelines are intended to provide high-level best practice rather than detailed technical specifications and are based upon proven operational procedures and commodity off-the-shelf (COTS) products. Where examples are included, it should be recognized that these might rapidly become outdated because of the rate of change of Internet technology. It is recommended that the most appropriate solution be deployed at the time of any implementation. Moreover, the guidelines do not cover those services which are normally provided via dedicated communications infrastructures, such as leased lines or Intranets that may use Internet-based technologies.

The document contains some historical background, general considerations relating to all Internet-based aeronautical services and considerations relating to specific types of services.

Finally, it should be noted that this document does not contain a statement of ICAO’s position on where and when the Internet should or should not be used for aeronautical applications. ICAO may develop such a position at a later stage if deemed necessary.

———————

TABLE OF CONTENTS

EXPLANATION OF TERMS

Note.— The explanations given below are to facilitate the understanding of the terms in the context of their use in this document.

Browser. Software that will load and display a web page. A browser interprets the HTML or XML code (see below) from the web-page files, executes embedded scripts and programmes, provides encryption/ decryption for security where needed, displays graphics (except text-only browsers), plays music and videos and provides links to related pages.

Demilitarized zone (DMZ). A network sitting between two networks. It is neither part of the internal network nor directly part of the Internet. The infrastructure deployed within a DMZ is afforded some protection from external attack but is still considered vulnerable.

Denial of service (DoS) attacks. Attempts to overwhelm an Internet site or server. The outcome of the attack is that genuine users are competing for the same resources as the attacker. This will either result in genuine users being blocked or the entire infrastructure grinding to a halt. Distributed DoS (DDoS) attacks are coordinated from many different locations and can be considerably more difficult to manage. A DoS is often used as a diversion by an attacker to cover up efforts to gain entry to a system.

Digital certificate. An electronic means of establishing user credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains the user's name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to Recommendation X.509 of the Telecommunication Standardization Section of the International Telecommunication Union. Digital certificates can be kept in registries so that authenticated users can look up the public keys of other users.

Electronic mail (email). One of the standard Internet protocols that enables people with different computers and operating systems to communicate with each other. Email allows one-to-one or one-to-many mailings. Mail is received and held by a mail server within an organization or by an Internet service provider until the addressee logs on and collects the mail.

Extensible Markup Language (XML). A step in the evolution of web data formats (beyond HTML).

Extranet. A network that supplements a closed Intranet by providing access to customers, suppliers, subcontractors and others outside the organization that require selective information from the organization. It is not accessible to the Internet at large.

Firewall. A device that protects the resources of a private network from users from other networks. Basically, a firewall, working closely with a router, filters all network packets to determine whether to forward them toward their destination. A firewall is often installed away from the rest of the network so that no incoming request can get directly at private network resources.

Hypermedia. Like hypertext, but includes other interlinking multi-media such as graphics, audio and video.

Hypertext. A form of text that includes visible links to other pages of text or media, accessible by clicking on or selecting the links.

Hypertext Markup Language (HTML). The coding system used to create World Wide Web (WWW) pages. A page written in HTML is a text file that includes tags in angle brackets that control the fonts and type sizes, insertion of graphics, layout of tables and frames, paragraphing, calls to short runnable programes, and hypertext links to other pages.

Hypertext Transport Protocol (Secure) (https). The standard encrypted communication mechanism on the World Wide Web. This is the HTTP operating over SSL.

Internet. A system of computer networks that interconnect worldwide and use the Transmission Control Protocol/Internet Protocol (TCP/IP) for transmission and recovery of information.

Internet aviation service provider (IASP). An accredited company that provides aeronautical information using the Internet as the means of communication.

Internet protocol (IP). A protocol used to route data packets from source to destination in an Internet (interconnected networks) environment.

Internet service provider (ISP). A company that provides Internet access and a communications infrastructure.

Intranet. A private network within a single organization that uses the TCP/IP for transmission and recovery of information. The sites within an Intranet are generally closed to the Internet and are accessible by organization members only.

Operating system (OS) integrated. A feature or function that is embedded in the computer operating system (e.g. Internet Explorer in Windows).

Port. A pre-defined internal address that serves as a pathway from the application to the transport (TCP) layer or vice versa.

Public key infrastructure (PKI). A system of digital certificates, certificate authorities and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving, and there is no single PKI nor even a single agreed-upon standard for setting up a PKI.

Redundant array of independent disks (originally redundant array of inexpensive disks) (RAID). A way of storing the same data in different places (thus, reduntantly) so that input/output operations can overlap in a balanced way, improving performance. Redundancy increases the mean time between failure (MTBF) and therefore also increases fault-tolerance. A RAID appears to the operating system to be a single logical hard disk.

Risk assessment. An evaluation of the threats to a system, the likelihood that those threats will be exploited and the impact of such exploitation.

Router. A device that determines the next network point to which a data packet should be forwarded en route toward its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks it is connected to. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet.

RSA. An Internet encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. The system is owned by the company, RSA Security, which licenses the algorithm technologies.

Secure Sockets Layer (SSL). An encrypted communications method over the Internet. SSL ensures that the information is sent, unchanged, only to the intended recipient. Online shopping or banking sites frequently use SSL technology to safeguard credit card and other sensitive information.

SecurID. RSA SecurID® is a "strong authentication" mechanism requiring both a token and a personal identification number (PIN).

Server. A computer or device on a network that delivers or manages networked resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programmes at once. A server in this case could refer to the programme that is managing the resources rather than the entire computer.

Strong authentication. A two-factor authentication method based on something the user knows (e.g. password/PIN) and something the user possesses (e.g. an authentication token). The two-level credentials provide significantly more reliable authentication of users. See RSA SecurID.

Transmission Control Protocol (TCP). A communication protocol (used in the Internet) that provides reliable host-to-host communication service in a packet-switched network or an interconnection of such networks.

Uniform Resource Locator (URL). A designator of the location of a resource in the Internet. It can be entered into the location window of the browser to allow connection to the desired location (e.g. a website).

Virtual private network (VPN). A network that employs a secure, authenticated "tunnel" across a public network (e.g. the Internet). End points of the VPN tunnel are authenticated, normally using strong authentication. Content is segregated from the public network using encryption.

Website. One or more connected web pages under a common ownership, management or theme.

World Wide Web (WWW). An Internet protocol that makes use of HTML, hypertext and hypermedia to create pages with links to other pages. WWW pages can include graphics, audio and video as well as text.

———————————

Chapter 1

BACKGROUND

1.1 The word “Internet” is a contraction of the phrase “interconnected network”. However, what is commonly referred to and is the subject of this document, i.e. the “public Internet” (or simply the “Internet”), is a loosely organized international collaboration of autonomous interconnected networks that use the Transmission Control Protocol/Internet Protocol (TCP/IP) for inter-networking. The closely related term “World Wide Web (WWW)” refers to the global network of servers (software residing in computers that are connected to the Internet) that allows text, graphics, audio and video files, and links (active connections to other web locations or resources) to be mixed and processed together.

1.2 The origin of the Internet lies in the research efforts in the United States to establish a secure computer-computer network in the mid-1960s. Those efforts resulted in the Advanced Research Projects Agency (a branch of the Department of Defence) Network (ARPANET), which began its operation linking computers in a few universities in the United States in 1969. Although the first email was exchanged over the ARPANET in 1972, many consider 1 January 1983 as the “official” beginning of the Internet because on that date the network was switched over to the TCP/IP protocol suite, which had been developed in the mid-1970s and accepted by the United States Government in 1978. Other networks were gradually connected to the ARPANET, and the Internet started growing. The ARPANET itself ceased to exist in 1989, but the Internet continued its explosive growth due to increasing interest and the availability of powerful personal computers, communication links such as optical fibre, and local area networks/wide area networks. The control of Internet traffic was handed over to the commercial sector in 1995.

1.3 Users normally lease Internet services from commercial Internet service providers (ISPs). The ever-increasing demand for the Internet, evident from the enormous growth in the number of users (from 200 million in 1998 to nearly 500 million in early 2002) provides the strongest incentive for service providers to continuously improve their system capacity/performance and offer better competitive service. It can therefore be concluded that, in general, where Internet service is commercially available (and competition is permitted), the likelihood of finding a suitable grade of service increases with time.

1.4 Traditionally, the civil aviation community has insisted on having its own dedicated communication systems on the grounds of reliability, integrity, security and their impact on aviation safety. This has caused a degree of reluctance by many aviation personnel to formalize the use of the Internet, which is not under the control of any aviation entity. Nevertheless, due to its widespread availability, accessibility (especially by the public), affordability, speed and ease of use, some States have started using the Internet for certain applications (e.g. meteorology and aeronautical information services). Also, in some parts of the world, where dedicated aeronautical communications systems are inadequate or cannot be economically justified due to very low traffic levels, the Internet is being used as a means of ground-ground communications.

1.5 ICAO has been extensively using Internet services (mainly email and web access) for dissemination of information, documentation and administrative communications. The ease of access/use and the high level of integrity of these services have greatly enhanced the overall communications process of the Organization. The notion of using the Internet for safety-related applications, however, has been treated with caution by the Organization. This is mainly due to the fact that the Organization has made great efforts to standardize communications systems that can support stringent operational requirements for aviation safety and security in anticipation that States will implement them in accordance with regional air navigation plans.

1.6 In the area of ground-ground communications, the ATS message handling system (AMHS), which is a modern system that forms the ground-ground portion of the aeronautical telecommunication network (ATN), has been developed by ICAO to replace the aging aeronautical fixed telecommunication network (AFTN). Like AFTN (and the common ICAO data interchange network (CIDIN)), AMHS is a dedicated system supporting aeronautical safety applications. However, to date, the system has only been implemented on a very limited scale, and it will take many more years for a truly global aviation messaging system to be in place. In the meantime, the Internet has emerged as a popular medium that can serve the messaging needs of the aviation community. Moreover, unlike AFTN, CIDIN and AMHS, which are closed networks, i.e. restricted to authorized aviation users, the Internet is open to the general public and therefore allows pilots or other current or potential users of aeronautical information to access the data banks and interact with relevant aviation authorities, as necessary, from home or anywhere else where there is a suitable connection. The Internet is therefore a beneficial augmentation to the current formal conduct of aeronautical communications.

1.7 Noting the above and also responding to recommendations from regional planning and implementation groups and, more recently, from the Meteorological (MET) Divisional Meeting (2002), ICAO initiated studies on the use of the public Internet for all categories of aeronautical applications (though only in the context of ground-ground communications) with due consideration to reliability, integrity, accessibility and security concerns. The guidelines contained in this document are the initial results of those studies.

1.8 This document contains guidelines on the use of the Internet for non-time-critical aeronautical ground-ground applications. Such applications generally involve the dissemination/exchange of information between:

a) a State authority and users (within the State);

b) two or more State authorities; or

c) a third party (usually a commercial entity) and users (in the same or different State(s)).

1.9 Users of aeronautical information must be assured that what they are using is provided by a source approved by the State, is managed appropriately and communicated with integrity. This issue is made more complex when information is communicated via the Internet. This entails two accreditation processes, one for the sources of aeronautical information and a second for the Internet provision of that aeronautical information. Guidelines contained in this document are aimed primarily at the Internet provision of aeronautical information.

———————

Chapter 2

RESPONSIBILITIES OF STATES

2.1 GENERAL

2.1.1 In general, the use of the Internet as a means of providing or exchanging operational information does not relieve States from their obligations and responsibilities for the implementation of an aeronautical fixed service (AFS) and other facilities and services that have been established by regional agreement and are documented in the ICAO regional air navigation plans.

2.1.2 Furthermore, like any other facility or service, the use of the Internet for inter-State data and message exchange should be subject to bilateral, multilateral or regional agreements and be properly reflected in the regional air navigation plans.

2.1.3 States that permit use of the Internet should:

a) accredit the entities (hereafter referred to as Internet aviation service providers (IASPs)) that will provide an Internet-based provision/exchange of information; and

b) ensure that they have adequate information technology and information security expertise for overseeing the accreditation process described hereafter.

2.1.4 For the purpose of accrediting/overseeing an IASP, States should:

a) publish and maintain a list of accredited IASPs with details of the service that has been accredited along with accreditation expiry dates;

b) require an IASP to advise users of any limitations associated with the provision of its services. Also, the IASP should state what the contingency or alternate service is. For example, in the case of an Internet system failure when filing a flight plan, the user should call the air traffic services or flight service facility and submit the information by conventional means;

c) require an IASP to reduce, though the use of well-designed user interfaces, the possibility of incorrect information accidentally being submitted, and to provide appropriate training for users; and

d) re-accredit an IASP after an interval of at least three years or when the IASP makes major changes to its organization or infrastructure.

2.2 APPLICABLE ICAO PROVISIONS

2.2.1 Annex 15 — *Aeronautical Information Services*, Chapter 3, specifies the responsibilities of States with regard to the provision of aeronautical information, and the functions of an aeronautical information service. Included are provisions relating to the establishment of a quality system, the exchange

of aeronautical information, copyright and so on. The philosophy underlying Annex 15, which stems from Article 28 to the Convention on International Civil Aviation, is that each State is responsible for making available any and all information that is pertinent and required for the operation of aircraft engaged in international civil aviation within its territory, as well as areas outside its territory for which the State is responsible for air traffic services.

2.2.2 Of particular note is Annex 15, Section 3.1, which provides that the State concerned shall remain responsible for the information published whether it provides the aeronautical information service, shares the provision of that service with another State, or delegates the authority for the provision of the service to a non-government agency. Accordingly, when the Internet is used by States as a supplemental means to publish their aeronautical information, States should ensure that appropriate quality system processes and procedures are put in place to support the information provided under their responsibility and should also accredit the Internet sites that publish such information.

2.2.3 Annex 3 — *Meteorological Service for International Air Navigation*, Chapter 2, 2.2, specifies the responsibilities of States with regard to the supply, quality assurance and use of meteorological information.

2.2.4 Annex 4 — *Aeronautical Charts*, Chapter 1, 1.3, specifies the responsibilities of States with regard to the availability of aeronautical charts, and Chapter 2, 2.17, provides requirements for the quality management of charted aeronautical data.

2.3 ACCREDITATION OF AN IASP

2.3.1 Accreditation of an IASP is distinct from the accreditation of sources of aeronautical information. Accreditation of data sources, including assembly, formatting and timeliness of data is a prerequisite to the accreditation of an IASP and is not within the scope of this document.

2.3.2 To ensure that information provided via the Internet meets current best practice for confidentiality, integrity, authenticity and availability, States need to develop accreditation procedures for an IASP delivering information and services via the Internet. The ensuing paragraphs provide guidelines for that purpose.

2.3.3 It would be desirable for States to require an IASP to follow the high-level steps illustrated in Figure 2-1. Individual States may wish to supplement these steps.

2.3.4 The basic elements of the typical accreditation depicted in Figure 2-1 are described in the following paragraphs.

Service plan

2.3.5 The IASP should provide a description of the Internet services that are to be delivered. The service description should indicate the:

a) type of service(s). Typical services include, but are not limited to, aeronautical information service (AIS), MET, AFTN-type communications, and flight plan submission;

b) region of applicability (e.g. local, regional or global); and

c) target market (e.g. general aviation, business aviation, commercial aviation).

A service plan is a prerequisite for a risk management process.

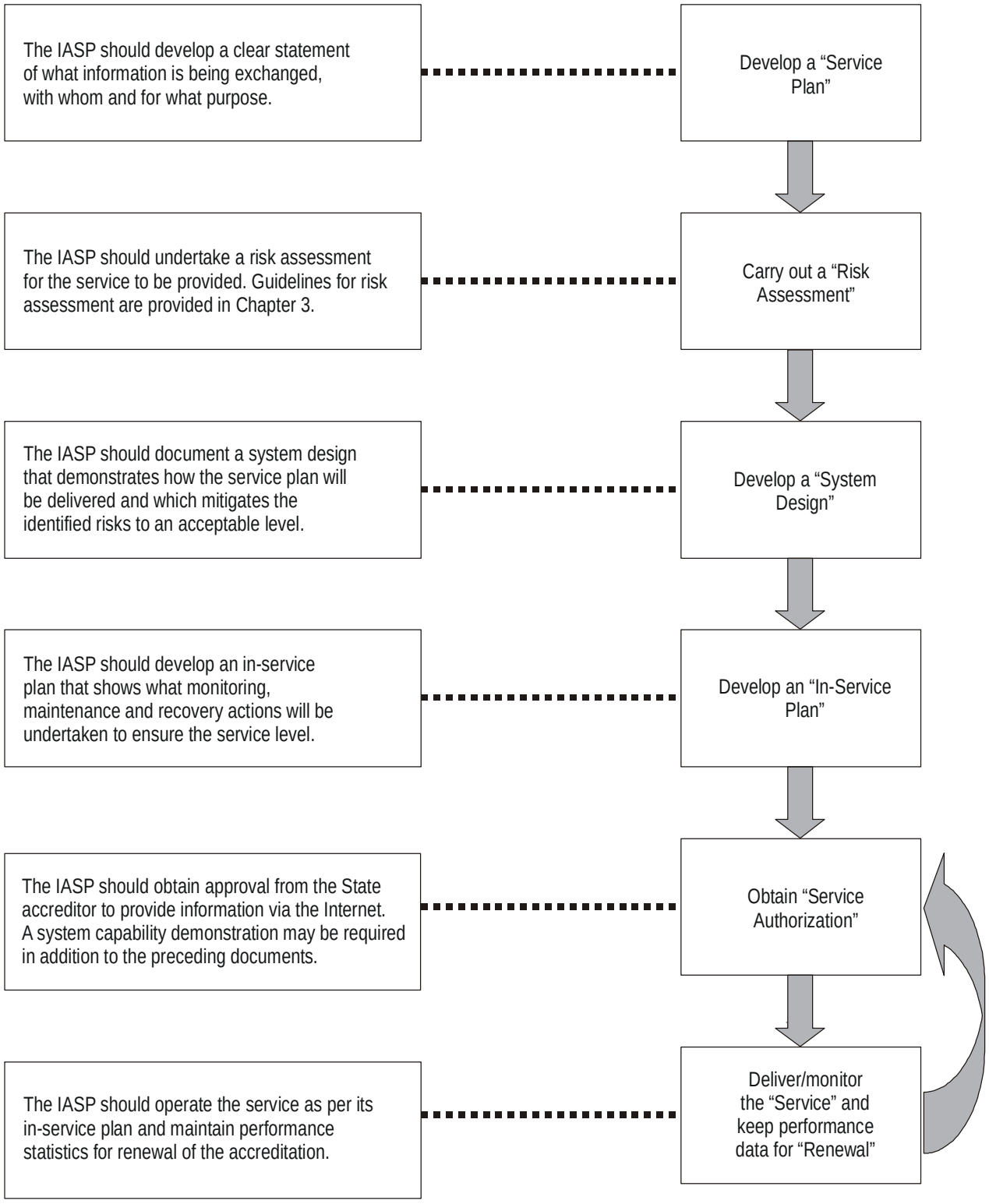

Figure 2-1. A typical process for assessment of an IASP

Risk assessment

2.3.6 Having developed a service plan, the IASP will need to consider the risks presented by offering this service on the Internet. Guidelines on risk assessment are included in Chapter 3.

System design

2.3.7 Having identified the service risks, the IASP should design its system to mitigate these risks to an acceptable level for the service it plans to provide. Guidelines on risk mitigation strategies are included in Chapter 3.

In-service planning

2.3.8 Having completed a service plan, a risk assessment and a system design, the IASP will need to consider how the service will be maintained at the required level of quality.

System maintenance

2.3.9 The IASP needs to have a maintenance plan to enable continued system operation commensurate with the type of service it is offering to aviation users. This should include regular preventative maintenance, both hardware and software. Regular updates of security software should be of primary importance. The IASP also needs to identify hardware spares to be held to enable the declared "time-to-repair" requirements to be met. Minimum training levels for maintenance staff should be identified.

Service agreement with the Internet service provider (ISP)

2.3.10 The IASP should have a service level agreement in place with its ISP(s), which specifies the requirements for service availability, including repair times, fault reporting, escalation contact points and monthly performance reports.

Data and transaction archiving

2.3.11 The IASP needs to conform to the data management requirements in the ICAO Annexes for the services it offers. This includes keeping a record of the data being offered at any point in time, and transaction records to show what data was supplied to specific users.

Note.— Where application, network and/or access logs are retained, the retention period will be identified by the State. Thirty calendar days (as per Annex 10 — Aeronautical Telecommunications*, Volume II —* Communication Procedures including those with PANS status*) for retention of AFTN messages is considered generally appropriate. However, in the event of receipt of notification of an accident, incident or overdue aircraft, or upon the request of the State, IASPs should retain data pertaining to that event indefinitely or until such time that destruction of that data is authorized by law. IASPs should make such data available in the form of a readable, certifiable, true copy upon the request of the State.*

Planned/unplanned system outage

2.3.12 The IASP needs to have a plan in place to manage service outages.

Disaster recovery

2.3.13 The IASP needs to have a disaster recovery plan, the scale of which will be dependent upon the type of service it offers.

Operational system monitoring

2.3.14 The IASP should develop a series of performance criteria and targets that will enable a State accreditation authority to determine whether the service performance targets are being met.

Granting of service authorization

2.3.15 The State accreditation authority should evaluate an IASP's system design processes and in-service planning to assess whether that IASP can deliver its service plan, and that mitigation strategies are in place to reduce the risks identified in the risk assessment to an acceptable level.

2.3.16 Prior to initial accreditation, States may request a demonstration of the service to be offered on the Internet to ensure that the system meets the performance criteria.

2.3.17 Additionally, States may consider asking the IASP to have its system thoroughly tested by an appropriate information-technology security assessment company. The test should consist of "penetration testing", scanning ports and services, and the necessary testing to ensure that the operating system and programmes (including anti-virus ones) have the latest security patches/updates installed.

2.3.18 States should accredit an IASP to deliver its service plan for a fixed period of time (e.g. one or two years). When an IASP applies for accreditation renewal, it should supply supporting historical performance data.

2.3.19 Accreditation should not be transferable, and an IASP should make this clear when linking to other website providers. An IASP should clearly indicate which State has accredited it to provide aeronautical information via the Internet and what information it is accredited to provide (in line with the service plan it submitted to the State accreditation authority).

2.3.20 In line with current ICAO provisions, accreditation is applicable only for service provision to users operating in/from the accrediting State. States may agree on reciprocal accreditation arrangements.

Service delivery/monitoring

2.3.21 The IASP should actively monitor the performance of the Internet service. The performance criteria identified in the in-service plan should be monitored at a frequency that enables substandard performance to be corrected promptly. The IASP should keep complete records of performance monitoring. These records may be audited by the State accreditation authority during the service accreditation period and should be submitted when an IASP requests accreditation renewal.

2.3.22 An IASP should include links on its website to enable aviation users to provide feedback to the IASP.

2.3.23 An IASP should include an agreed link to its State accreditation authority to enable aviation users to check its accreditation status and send feedback or comments directly to the State accreditation authority.

2.4 CHARGING

2.4.1 States incur considerable costs in the provision of aeronautical and/or meteorological information. In a vast majority of States, these costs are recovered through the levying of air navigation services charges on users. However, with the development of modern information technology and in the context of commercialization now prevailing, end users may choose to procure those products either from the State concerned or from a third-party commercial vendor.

2.4.2 Therefore, there may be occasions where commercial entities or States seek to procure aeronautical information and other air navigation documents from the originating State. In such cases, the originating State may wish to enter into a separate agreement with the party concerned regarding the conditions and costs, if any, that will be applied to the provision of that information for its subsequent re-publishing. It should be noted, however, that Annex 15 provides for the exchange of aeronautical information, without charge, between ICAO Contracting States.

2.4.3 In general, cost recovery charging schemes should be in accordance with the principles contained in Doc 9082 — *ICAO's Policies on Charges for Airports and Air Navigation Services*.

2.5 PERFORMANCE INDICATORS

The State should consider setting mandatory performance indicators for each service as appropriate. These performance indicators should be customer-focused and may be set in consultation with user communities. In general, it would be desirable to include the following in the list of performance indicators:

a) ***Availability.*** The service may be unavailable for access no less than a specified period in any calendar month, with no individual service outage longer than another specified period. This includes outage due to planned maintenance. Clearly the specified periods will vary depending on the type of service being provided.

b) ***Accessibility.*** The service should deliver page impressions to users no slower than a specified rate. A second metric could be introduced if users needed to download bulk data files.

Note.— While performance indicators are set at the discretion of the State, these should be kept within reasonable limits. Additionally, the State should adhere to a consistent policy among providers where similar services are expected to perform to broadly similar criteria.

2.6 INTELLECTUAL PROPERTY

2.6.1 While the issue of online copyright is still being developed in most States, it can be assumed that content already protected by a State's national law is equally protected when it is on the Internet. Although material made available on the Internet by a State is likely entitled to be protected in the same way as hard-copy material, posting material on the Internet carries a higher risk of copyright infringement. Most likely the infringement would be a party copying the whole or a substantial part of a copyright work without the State's consent.

2.6.2 Some States may choose to enforce their copyright for certain information (whether in written, electronic or visual chart form). As a result, these States could elect to use their right to refuse any party permission to copy and further publish that material. States that wish to facilitate the dissemination of their

material may choose to insist, pursuant to their ICAO obligations and national legislation, that appropriate quality control and audit processes be undertaken by any third party as a condition of the grant of a licence to copy or further publish aeronautical information.

2.6.3 The most effective way to advise users about copyright ownership when publishing on the Internet is to ensure that the IASP prominently displays a copyright notice © on its website clearly stating what a user can and cannot do with the copyright material and to pursue legal action in the event of infringement. A sample copyright notice used by a State is provided in the appendix to this chapter.

2.6.4 Another way to possibly minimize the risk of copyright infringement is to use copy protection or digital rights management software such as digital watermarking.

— — — — — — — —

Appendix to Chapter 2

SAMPLE COPYRIGHT NOTICE

Note.— The following copyright notice is used in Australia for an Internet-based display containing static AIS content. It is reproduced by kind permission of Airservices Australia.

All Airservices Australia aeronautical information service material and publications ("AIS Publications") are copyright. This specifically includes all elements of the Integrated Aeronautical Information Package ("IAIP"). Unless specified otherwise, you may use the AIS publications only by downloading, displaying or printing them in (in an unaltered form which retains this notice) for information purposes. Information purposes includes operational use but, except as permitted above and by the Copyright Act 1968, no part of the AIS publications may be reproduced, stored in a retrieval system, transmitted, redistributed, republished or commercially exploited in any way without the prior written permission of Airservices Australia. If you wish to use any part of the AIS publications in any way not permitted by this notice, contact the Airservices Australia's publications about a licence.

———————

Chapter 3

TECHNICAL CONSIDERATIONS

3.1 CATEGORIZATION OF MESSAGES

3.1.1 The Internet protocol suite ensures the integrity of transmitted messages under normal circumstances. However, being a public medium, the Internet is susceptible to certain security attacks (e.g. denial of service, or computer viruses) that may seriously slow down or even temporarily stop its useful operation.

3.1.2 Information security schemes can be employed to ensure the authenticity, integrity or confidentiality of messages. These measures, however, cannot counter network congestion (due to randomly high traffic or intentional malicious jamming). As such, the use of the Internet for aeronautical operational purposes should be limited to the exchange of non-time-critical messages, information or data. In the context of this document, non-time-critical means that what is being communicated has no immediate effect on an active flight.

3.1.3 It is still necessary to clarify exactly what category of aeronautical messages meet the above-mentioned criterion for being non-time-critical. In accordance with the message categories and their priority indicators (for transmission over the AFTN) in Annex 10, Volume II, the following message categories should be considered non-time-critical and, hence, suitable for transmission over the Internet:

a) certain MET messages (refer to Chapter 4 of this manual);

b) flight regularity messages;

c) certain AIS messages (refer to Chapter 5 of this manual);

d) flight plans and related messages (refer to Chapter 5 of this manual);

e) administrative messages; and

f) service messages (where applicable).

3.1.5 Notwithstanding the above, certain message types considered time-critical for aircraft in flight may be regarded as non-time-critical when used in a pre-flight context. Further description of MET and AIS messages that are considered non-time-critical can be found in Chapters 4 and 5, respectively.

3.1.6 Where time-critical data is made available for information only, users should be advised that such data should be obtained via appropriate means if intended for use in a time-critical context (e.g. for advising an aircraft in flight).

3.2 CONTENT

3.2.1 An IASP must take into account the material shown in the ensuing paragraphs when developing its services.

3.2.2 The types of information available via the service must be made clear to users of the service. For example, users need to know specifically what information is available via the service to ensure that they have all the content necessary for their operations.

3.2.3 Accredited services providing meteorological information should, at a minimum, make available the entire suite of Annex 3 (*Meteorological Service for International Air Navigation*) products provided by the State which are categorized as non-time-critical for in-flight safety or pre-flight preparedness.

3.2.4 Sources of information used by an accredited service must be clearly identified to the user.

3.2.5 The validity of the information provided must be made clear to users of the service.

3.2.6 Historical, non-operational or non-accredited information must be clearly labelled as such if it is available from the same service as operational information, e.g. expired information, archived information.

Note.— Non-accredited information may include value-added information or services that are in development or pre-release versions.

3.2.7 Procedures explaining how best to use accredited services should be made available to the user.

3.3 RISK ASSESSMENT AND MANAGEMENT

3.3.1 As part of the accreditation process defined previously, it is necessary for an IASP to have an ongoing risk assessment and management process in place for the service it proposes to provide.

3.3.2 Assessment and mitigation of risk require analyses of the system environment from physical, logical, systematic and procedural aspects.

3.3.3 In order to manage the risks involved in the provision of Internet-based aeronautical services, it is necessary to understand just what the risks are. This is performed in the risk assessment process. Once the risks have been established, appropriate action can be taken to ensure that the risks are managed to an acceptable level (i.e. a level acceptable to the IASP and the accrediting State).

3.3.4 The guidelines in this section are intended to supplement a standard risk management process and to address information-technology-specific issues.

3.3.5 ISO/IEC 17799:2000 *Information Technology — Code of Practice for Information Security Management* provides further information of relevance to this section.

3.3.6 Coverage of this topic for a non-technical audience can be found at *Secrets and Lies, Digital Security in a Networked World*. Bruce Schneier (John Wiley & Sons, Inc., 2004; ISBN: 0-471-45380-3).

3.4 RISK ASSESSMENT PROCESS

3.4.1 In order to carry out a risk assessment, the following steps should be followed:

a) identify the assets under threat and their value, the result of which is sometimes referred to as a statement of sensitivity;

b) identify the sensitivity of those assets;

c) identify the threats to those assets;

d) identify the threat sources;

e) determine or estimate the probability that those threats will actually materialize and affect the assets;

f) identify the impact should the assets be affected;

g) from the impact and the probability, derive the risk to the asset;

h) decide on the mitigating actions required if the risk is unacceptable (e.g. security measures, both technical and procedural); and

i) reassess the risk in light of the mitigation. Was the mitigation successful /sufficient?

3.4.2 The risk assessment process should be repeated in the light of any mitigating strategies employed, until the risk is considered acceptable. Additionally, the risk assessment and management process should be continued during the operational lifetime of the service. It is also important to note that the mitigating action required will be proportional to the value of the assets being protected. Each threat should be described under the headings: “threat”, “threat source”, “probability (of materializing)”, “impact” and, finally, “risk”.

Identification of assets under threat

3.4.3 Before appropriate security measures can be considered, it is essential to understand exactly what is being protected. In all systems this will include:

a) the system itself including the physical equipment and applications;

b) the data on the system; and

c) the organization’s reputation/brand image.

3.4.4 It is essential to consider network connections and the associated data flow into and out of the system. Each onward-connected system is also at risk, and further risk assessments for these systems are also necessary.

Identification of sensitivity

3.4.5 The following factors constitute the sensitivity of a typical system to various attacks:

a) ***Confidentiality.*** The sensitivity of information or assets to unauthorized disclosure, recorded as a classification or designation, each of which implies a degree of injury should unauthorized disclosure occur;

b) ***Integrity.*** The sensitivity of information or assets to being altered or destroyed;

c) ***Availability.*** The sensitivity of a service providing information, or access, to assets not being available to support operational functions; and

d) ***Authenticity.*** The sensitivity of the service to a non-legitimate user being able to access information or assets.

Identification of threats to assets

3.4.6 There are threats associated with each sensitivity as described below:

a) ***Interception: the threat to "confidentiality".*** This is the threat of someone gaining unauthorized access to information. Can a person access information that is sensitive and which that person is not permitted to see (e.g. for commercial or legal reasons)? The threat to information in transit needs to be considered as well.

b) ***Modification: the threat to "integrity".*** This is the threat of someone tampering with the system or the data. For example, can someone inject spurious data to make a forecast inaccurate? Can the system itself be compromised such that it continues to work but its output is wrong? Can data be modified while resident on the IASP platform? Can data integrity be compromised while in transit from an accredited source to the IASP; from the IASP to the user; from the user to the IASP (e.g. AFTN, flight plan submission, and weather observation input)? Would any such tampering be detectable?

c) ***Interruption: the threat to "availability".*** Does the service provide adequate performance for operational usage? Will service be degraded under peak demand? Can use of the assets be blocked? Can legitimate users be prevented from submitting information by flooding of the service with bogus entries (e.g. denial of service (DoS) attack)? The most common example of this is where web servers are simply overloaded with connections so that legitimate users can no longer access the service.

d) ***Masquerade: the threat to "authenticity".*** This is the threat of someone claiming to be someone else. For example, in an Internet service can it be assured that "customers" logging on are actually who they say they are because they may be persons trying to get a service for free. Can it be verified that the person trying to get administrator access is actually a legitimate administrator? Can users verify that they are interacting with the "real" service, not a façade presented by an attacker? Over the Internet it can be particularly difficult to confirm that the other end of a connection is who or what it claims to be.

3.4.7 The aforementioned threats can typically manifest in many ways, some of which are highlighted below:

a) ***Data/information.*** Unavailability, interruption (loss), interception, alteration, fabrication or destruction;

b) ***People/personnel.*** Omission, error, negligence, imprudence, laziness, sabotage or lack of knowledge;

c) ***Network (Intranet, Internet, etc.).*** Unauthorized access, maintenance, failure or security attacks (e.g. interception, pranks, forged identity, integrity violation or denial of service);

d) ***Hardware.*** Maintenance, failure (including power failure) or theft; and

e) ***Software and system.*** Interruption, modifications/patches or failure.

Identification of threat sources

3.4.8 The probability of an attack and its impact can depend on the source of the attack. It is appropriate to further divide the threats according to their sources. The simplest division of potential threat sources is:

a) staff (regular);

b) staff (administrators);

c) consultants/contractors;

d) competitors;

e) hackers (unskilled but numerous);

f) hackers (elite, highly skilled);

g) politically motivated and organized entities; and

h) natural events.

Identification of the probability that a threat will materialize

3.4.9 This part of the risk assessment becomes subjective. The two factors to consider here are:

a) ***The ease of executing an attack.*** This depends on the security measures in place, the type of system installed and the location of the system. It also depends on the skill level of the threat source and the opportunity that source has, as well as the resources available. This may change with time. Some attacks may be viewed as highly theoretical and very difficult, but if a tool is developed to automate them, they become orders of magnitude easier to execute.

b) ***Motivation of the threat source.*** Just because a person can launch an attack does not mean that person will do so. Thus it is important to understand the motivations of the threat sources.

3.4.10 For example, in a typical modern organization, most regular staff do not have direct access to their web server (i.e. the only access is via a browser). So even with motivation, it should be relatively difficult for most staff to launch an attack (especially if monitoring is in place). The situation of the “system administrator” is very different. Even inadvertently, a system administrator can cause major disruption, and there is practically no defence against such potential attacks. Thus a large degree of trust is placed on the system administrator.

3.4.11 Similarly, unskilled hackers are always trying to attack web servers, the motivation largely being bragging rights to say how many systems they have compromised. If the system software is maintained and up to date, the risks can be quite low. However, highly skilled hackers are likely to succeed in attacking almost any server. The issue then is why would they attack a particular organization specifically?

3.4.12 Natural events (e.g. fire, earthquakes, floods or tornadoes), while rare, will affect the provision of service and will therefore need to be considered in the risk management process as well.

Identification of the impact of a threat

3.4.13 This is still a subjective analysis. The aim is to answer (as much as possible) questions like:

a) How much would it cost to recover damaged data?

b) What is the value of that data?

c) What is the cost to the organization's reputation?

d) What contractual penalties are there?

e) What is the operational impact on the user of lost or missing information?

3.4.14 The impact or severity level will be based on system-specific factors including, but not limited to, the nature of the threat, the system functionality, its interfaces to operational systems, the criticality of the data provided, business continuity and the user of the information.

Evaluation of the risk

3.4.15 Provided the impact and probability are scored in the standard risk management form (very low | low | medium | high | extremely high) then the risk can be calculated in exactly the same way (i.e. as a product of impact and probability, where impact is the effect on the system/organization, and probability is the likelihood that the threat will be manifested — itself derived from the threat type and threat source, considering both skill level and motivation).

Risk mitigation strategies

3.4.16 It is essential to employ mitigation strategies while taking into account the value of the service or the severity of service failure. For example, a small IASP providing pre-flight information for the general aviation community may require significantly less stringent risk mitigation than an IASP that provides flight plan submission and pre-flight briefing services for commercial aircraft operating agencies. Notwithstanding the relationship between the extent of the mitigation strategy and the value of the service, reasonable measures should always be taken to preserve the integrity of the aeronautical data.

3.4.17 It should be noted that patch management of software applications is the most important factor in the risk mitigation strategy. No matter how well the system is designed and implemented, if the software is out of date (i.e. the latest patches have not been applied), the service will be vulnerable to attack.

3.4.18 The mitigation strategies are grouped according to the sensitivity they protect. Major sensitivities and possible relevant risk mitigations are listed below:

a) confidentiality

1) enable processes to ensure that the data held by the service provider is held in confidence;

2) ensure that the system design, network architecture and life-cycle management processes manage, to an acceptable level, the likelihood of access breaches;

3) manage, to an acceptable level, the likelihood that sensitive data can be "stolen" while in transit between the service provider and the user by implementing data encryption where appropriate;

4) manage, to an acceptable level, based on the severity level, the likelihood that an unauthenticated or falsely authenticated user can access the site;

5) implement a user name and password and/or other user authentication mechanisms, where appropriate, based on the severity level;

6) implement a user registration and validation process appropriate to the severity level;

7) implement a user responsibility policy with terms and conditions appropriate to the severity level;

8) ensure appropriate management of passwords; and

9) ensure secure equipment disposal;

b) integrity

Note.— Annex 15, Chapter 3, 3.2.8, provides the requirement for the integrity of aeronautical data as part of the quality system.

1) ensure that the original data is from an assured source;

2) ensure that the modification or reformatting of original data does not compromise their integrity;

3) manage, to an acceptable level, the likelihood that data can be modified while in transit between the assured source and the service provider by:

i) managing, to an acceptable level, the likelihood that data held by the service provider can be tampered with;

ii) managing, to an acceptable level, the likelihood that data can be modified while in transit between the service provider and the user;

iii) ensuring that in the event of corruption of the data held by the service provider, “clean” data can be restored;

iv) managing, to an acceptable level, the likelihood that the data store can be attacked via the website; and

v) ensuring that date- and time-stamped logs are held for recording transactions with the user for non-repudiation purposes. (It should be possible to reconstruct actual products accessed to verify what the user received if the products themselves are not archived);

c) availability

1) implement a service level agreement with the ISP (along with any associated maintenance support) that ensures availability appropriate to the importance of the site;

2) ensure that the system design provides for redundancy appropriate to the importance of the site;

3) ensure that the system design, network architecture and life-cycle management processes manage, to an acceptable level, the likelihood that the platform can be disabled by malicious intent (e.g. hacking, viruses, worms, denial of service, distributed denial of service or natural events like flooding);

4) ensure that the system design, network architecture, life-cycle management and training processes manage, to an acceptable level, the likelihood that the platform can be disabled by benign activities; and

5) implement a customer feedback process to ensure that performance issues can be identified and addressed to the service provider;

d) authenticity

1) ensure that the user can easily verify that the provider has been accredited (for the State that the user wishes to commence travel in);

2) ensure that the user can verify that the service provider is what it professes to be; and

3) ensure that, where necessary, the provider can verify who the user is.

3.4.17 Additionally, where necessary, an IASP should be able to ascertain delivery of the appropriate information to the user. This is referred to as non-repudiation.

3.4.18 Once an initial risk assessment has been completed, the risk management process should then enter an iterative phase where mitigation actions are considered and a new evaluation of risk established, until the IASP (and the accrediting State) ascertain that the remaining risks are acceptable. Furthermore, new risks will come to light during the operation of the service. The risk management process should address this and reassess existing and new risks in the light of current information and best practice.

3.4.19 The appendix to this chapter lists selected threat and risk management strategies and maps these to suggested current best practices for their realization in an information technology environment.

3.4.20 Furthermore, the Open Web Application Security Project (OWASP) (http://www.owasp.org), *The Ten Most Critical Web Application Security Vulnerabilities*, 2004 Update, defines a number of strategies for combatting vulnerabilities in web applications.

— — — — — — — —

Appendix to Chapter 3

CURRENT BEST PRACTICE FOR RISK MITIGATION STRATEGIES IN AN INFORMATION TECHNOLOGY (IT) ENVIRONMENT

Note.— Since advances in Internet technology are frequent, the specific technology solutions that may appear in the "current best practice" column are meant to be examples of what was current at the time of publication.

Risk mitigation strategy	Sensitivity category	Current best practice	To be used when impact severity is	
			Low	High
Implement user authentication appropriate to the threat level	Authenticity	• Anonymous user access • User name and password login requirement • User name, password login with separate PIN for specific functions • Digital certificate (e.g. SSL) • Secure transfer protocol (https) • RSA SecurID • VPN, OS-integrated • Client side software (token authentication)	✓ ✓	 ✓ ✓ ✓ ✓ ✓ ✓
Implement a user registration and validation process appropriate to the threat level	Authenticity	• Online registration without validation • Paper-form registration without validation • Online registration with validation • Paper-form registration with validation • Online registration with access details sent via alternate channel (i.e. email, post) to help ensure that the registered user can really be identified	✓ ✓	 ✓ ✓ ✓
Implement terms and conditions with users appropriate to the threat level	Authenticity	• Maintain confidentiality of password; do not share. • Always log off the site completely. • Advise the service provider of changes to pertinent information.	✓ ✓ ✓	
Implement data encryption appropriate to the confidentiality level	Integrity	• HTTPS, SSL • PKI (and others)	✓	✓
Manage, to an acceptable level, the likelihood that data can be modified while in transit between the assured source and the service provider	Integrity	• Use the Internet with appropriate encryption and authentication (HTTPS, SSL). • Use a secure private or virtual private network (VPN) connection to obtain data from the assured source. Do not use the public Internet without an appropriately secured VPN connection.	✓	✓

Risk mitigation strategy	Sensitivity category	Current best practice	To be used when impact severity is	
			Low	High
Manage, to an acceptable level, the likelihood that data held by the service provider can be tampered with Manage, to an acceptable level, the likelihood that data can be modified while in transit between the service provider and the user Manage, to an acceptable level, the likelihood that the data store can be attacked via the website	Integrity	• Use software firewalls and hardened infrastructure; do not allow direct access to the data store. • Deploy physical firewalls, proxy servers, host intrusion protection systems (HIPS) and network intrusion detection systems (NIDS) as appropriate. • Deploy a double layer of firewalls, each supplied by different manufacturers, to reduce the likelihood of a vulnerability compromising the service provider. • Verify the provider — digital certificates. • Prevent “man-in-the-middle” and ensure that data is passed directly to users (SSL will achieve this). • Place a firewall infrastructure between the web server and application server (if any) and the data store in addition to external boundaries to create DMZs (de-militarized zones). • Use multiple DMZs to segregate functional components (i.e. web server, application server, database server).	✓	 ✓ ✓ ✓ ✓ ✓
Ensure that in the event of corruption of the data held by the service provider, “clean” data can be restored Ensure that date- and time-stamped logs are held, recording transactions with the user for non-repudiation purposes (should be able to reconstruct actual products accessed to verify what the user received if the products themselves are not archived)	Integrity	• Store logs in interoperable formats such as ASCII. • Digitally sign log files. • Ensure that system and data back-ups are controlled from within a secure domain. • Ensure that back-ups are stored within a secure domain. • Implement off-site storage for archive disaster recovery purposes.	✓	 ✓ ✓ ✓ ✓
Implement a customer feedback process to ensure that customer concerns can be identified and addressed	All	• Customer service desk with telephone support and problem-report tracking system. • Customer email feedback and problem-report tracking system.	 ✓	✓

Risk mitigation strategy	Sensitivity category	Current best practice	To be used when impact severity is	
			Low	High
Ensure that the user can easily verify that the provider has been accredited (for the State that the user wishes to commence travel in) Ensure that the user can verify that the service provider is what it professes to be Ensure that, where necessary, the provider can verify who the user is	Confidentiality	• Verify the user using user name and password. • Verify the user using client-side digital certificates. • Verify the provider using digital certificates. • Prominently display an official logo on the site indicating accreditation (and for which State). • Hyperlink the accreditation logo to the State accreditation site. The State accreditation site should include details of what service the provider is accredited for, plus the date of accreditation and the date of expiry.	✓ ✓ ✓ ✓	 ✓
Implement an ISP and maintenance support service level agreements that ensure availability appropriate to the importance of the site	Availability	• Define a service level agreement with ISP(s) covering outage, availability and bandwidth. • Define a hardware maintenance contract for the physical infrastructure which should include service level agreements. • Ensure that the ISP(s) chosen can deliver sufficient bandwidth, including extra volume for any predicted growth.	✓ ✓ ✓	
Ensure that the system design provides capacity and redundancy appropriate to the importance of the site	Availability	• Minimize the number of single points of failure or minimize the impact of any failure. • Maintain a hot standby/cold standby/spare stock (as appropriate) for key equipment (servers, routers, etc.) so that failures can be resolved expediently. • Estimate capacity requirements for the system (i.e. through application of best practice design and/or system load testing). • Size physical infrastructure according to estimated capacity. • Deploy server clusters/server farms and load-balancers. • Deploy hot-swap drives/RAID to minimize the impact of disk failure. • Deploy dual (replicated) data stores. • Employ a dual network infrastructure (including connection to the Internet via ISP) — not necessarily separate companies if a single company can provide a resilient infrastructure. • Employ dual supplier contracts (if not necessarily manufacturer) for hardware and network infrastructure — in case of financial collapse or industrial action. • Deploy servers with uninterruptible power supplies (UPS) to cover short periods of power failure. • Deploy UPS with diesel generator back-up to cover longer periods of power failure. • Maintain a complete separate infrastructure for disaster recovery and business continuity.	✓ ✓ ✓ ✓ ✓ ✓	 ✓ ✓ ✓ ✓ ✓ ✓

Risk mitigation strategy	Sensitivity category	Current best practice	To be used when impact severity is	
			Low	High
Ensure that the system design, network architecture and life-cycle management processes manage, to an acceptable level, the likelihood that the platform can be disabled by malicious intent (hacking, viruses, worms, denial of service, distributed denial of service, flooding, etc.) Ensure that the system design, network architecture, life-cycle management and training processes manage, to an acceptable level, the likelihood that the platform can be disabled by benign activities	Availability	• Implement a system hardening strategy that ensures that the system is hardened to an appropriate level by removing or disabling all components not required for its function. This may include access restrictions (ports and protocols), limiting user population, password policies, access controls, user and group rights and intrusion detection.	✓	
		• Implement a software patching strategy that updates and maintains system software to an appropriate level.		✓
		• Deploy anti-DOS hardware — packet filters/“secure” routers.	✓	
		• Ensure anti-virus software is deployed and that the software is up to date.		✓
		• Deploy anti-virus software from multiple vendors to reduce the likelihood that a vulnerability will compromise the service provider.	✓	
		• Identify expected user access/usage patterns and traffic volume.	✓	
		• Estimate bandwidth sufficient to cope with usage patterns and traffic volumes.	✓	
		• Define appropriate test procedures to ensure that when an upgrade to the service is deployed, it is functional and does not negatively impact the provision of service.	✓	
		• Define appropriate deployment procedures to ensure that when an upgrade to the service is deployed, it is functional and does not negatively impact the provision of service.		✓
		• Ensure that each user account cannot have parallel sessions originating from multiple IP addresses.		✓
		• Deploy an (automated) fail-safe application that is available should the main site be off-line.		✓
		• Employ appropriate staff training and procedures for development, deployment and maintenance of the service.		✓
		• Monitor, twenty-four hours a day, seven days a week, infrastructure and applications with well-documented resolution and/or escalation procedures for expected issues.		✓

Chapter 4

MATTERS RELATING TO METEOROLOGICAL INFORMATION

4.1 INTRODUCTION

In accordance with Annex 3 — *Meteorological Service for International Air Navigation*, Contracting States agree to provide a range of services that include, as a minimum, observations and forecasts to support operational decisions by area control centres, fight information centres, aircraft operating agencies, flight crews or the pilot-in-command. The purpose of this chapter is to identify the meteorological information that can be provided via the Internet and in which context.

4.2 TIME-CRITICAL METEOROLOGICAL MESSAGES

4.2.1 The meteorological information listed in 4.2.2, when provided via the Internet, should not be relied upon for time-critical operational decisions, either in flight or immediately prior to departure. This information will be referred to as time-critical meteorological information, and when used in this context, it should be distributed via the aeronautical fixed service (AFS) because its characteristics will ensure that such messages are received in a timely manner.

4.2.2 According to Annex 10 — *Aeronautical Telecommunications*, Volume II, information or products that contain aeronautical meteorological information are classified under one of two categories, “flight safety messages” or “meteorological messages”. Flight safety messages related to aeronautical meteorology, which can be regarded as time-critical in the above context, include:

a) SIGMET information;

b) special air-reports (AIREP);

c) AIRMET messages;

d) volcanic ash advisories;

e) tropical cyclone advisories; and

f) amended aerodrome forecasts (TAF).

4.3 NON-TIME-CRITICAL METEOROLOGICAL MESSAGES

4.3.1 The following meteorological information is considered non-time-critical and can be provided via the Internet:

a) meteorological information concerning forecasts, e.g. TAF, area and route forecasts, and concerning observations such as aerodrome routine meteorological report (METAR) and aerodrome special meteorological report (SPECI);

b) meteorological information provided by the world area forecast centres (WAFCs), e.g. significant weather charts, and wind, temperature and relative humidity charts;

c) volcanic ash advisories in graphical format (VAG) provided by the volcanic ash advisory centres;

d) GAMET area forecasts; and

e) route forecasts (ROFOR).

Note.— The above can include binary universal form for the representation of meteorological data (BUFR) and processed meteorological data in the format of grid point values expressed in binary form (GRIB) encoded information.

4.3.2 Services for operators and flight crew members for pre-flight planning under centralized operational control are considered non-time-critical. Meteorological information for pre-flight planning by operators can include the following:

a) current and forecast upper winds, upper-air temperatures, to tropopause heights, geopotential heights and maximum wind information and amendments thereto;

b) existing and expected significant en-route weather phenomena and jetstream information and amendments thereto:

c) forecast for take-off;

d) METAR and, where available, SPECI for the aerodrome of departure, take-off and en-route alternate aerodromes, the aerodrome of intended landing and destination alternate aerodromes, as determined by regional air navigation agreement;

e) TAF and amendments thereto for the aerodrome of departure and intended landing, and for take-off, en-route and destination alternate aerodromes, as determined by regional air navigation agreement; and

f) SIGMET information and appropriate special air-reports relevant to the whole of the routes concerned, as determined by regional air navigation agreement.

———————

Chapter 5

MATTERS RELATING TO AERONAUTICAL INFORMATION SERVICES (AIS)

5.1 INTRODUCTION

5.1.1 The purpose of this chapter is to identify the aeronautical information that can be provided via the Internet and in which context.

5.1.2 The Standards and Recommended Practices (SARPs) in Annex 15 — *Aeronautical Information Services*, Annex 4 — *Aeronautical Charts*, and the guidance material contained in the *Aeronautical Information Services Manual* (Doc 8126) have been established to satisfy uniformity and consistency in the provision of aeronautical information.

5.1.3 Although aeronautical information services provided via the Internet may be tailored to support the operational needs of users (flight operations personnel including flight crews, flight planning and flight simulators as well as the air traffic services unit responsible for flight information service and the services responsible for pre-flight information), they should conform to the above-mentioned standards.

5.1.4 A quality management system should be in place to provide users with the necessary assurance and confidence that distributed aeronautical information satisfy specified requirements for quality and traceability (Annex 15, Chapter 3, 3.2.5, refers).

5.2 TIME-CRITICAL AERONAUTICAL INFORMATION

5.2.1 The following aeronautical information is considered time-critical and, when provided via the Internet, should not be relied upon for time-critical operational decisions, either in flight or immediately prior to departure:

a) dynamic information of a temporary nature, such as current national and foreign NOTAM (including SNOWTAM, ASHTAM and checklists); and

b) other information of urgent character made available to flight crews in the form of plain-language pre-flight information bulletins (PIB).

5.2.2 Annex 15, Chapter 5, 5.3.2.1, specifies that the AFS shall, whenever practicable, be employed for NOTAM distribution.

5.2.3 The provision of value-added pre-flight information bulletins or products with customized format and graphics, when appropriate, need to provide at least the services that would be available in a paper-based environment.

5.3 NON-TIME-CRITICAL AERONAUTICAL INFORMATION

The following static and basic AIS information is considered non-time-critical and can be provided via the Internet:

a) ***Static information.*** Common documented permanent or long-term information, such as:

1) Aeronautical Information Publications (AIP) (which include aerodrome information, detailed descriptions of flight information regions (FIR), navaids, maps, charts, obstacle data, air routes, etc.);

2) AIP Amendments, both aeronautical information regulation and control (AIRAC) and regular amendments;

3) AIP Supplements, both AIRAC and regular supplements;

4) Aeronautical Information Circulars (AIC);

5) monthly printed plain-language list of valid NOTAM, which also includes indications of the latest AIP amendments, AIC issued and a checklist of AIP Supplements; and

6) NOTAM containing a checklist of valid NOTAM, issued monthly, which also refers to the latest AIP Amendments, AIP Supplements and at least the internationally distributed AIC.

b) ***Basic information.*** Data required for enabling the processing of other information, which can consist of permanent, long-term or static data not provided to users (i.e. reference lists, custom/regular routes, distribution files, selection criteria, association criteria).

5.4 PROVISION OF STATIC AND BASIC INFORMATION

5.4.1 Static and basic information can either be permanent or of long-term duration. The effective date of the information needs to be identified. Each publication should be dated. If pages have different effective dates, each page should be individually dated. Where data elements are published independently, they require an identifiable effective date.

5.4.2 Common effective dates, at intervals of 28 days under the regulated system (AIRAC), are to be used for the information listed in Annex 15, Appendix 4, Part 1, and are also recommended for the that listed in Part 2 (Annex 15, Chapter 6, provides details). To ease the transition from an effective date to the next publication date (AIRAC cycle date), previous, current and next-cycle aeronautical information should be provided for a specified period. When making such a service available, it becomes increasingly important to clearly identify the effective date for all aeronautical information.

5.4.3 The Internet may be used to provide information under the AIRAC system. However, appropriate arrangements for the provision of information in paper copy form should remain available (Annex 15, Section 6.2, refers). The AIRAC system is intended to provide pre-planned information to specific recipients: AIS third-party providers, aviation agencies, chart and database producers, etc. Confidentiality is recommended (Chapter 3 of this manual refers). Organizations considering the provision of this information need to ensure that users are well aware of the AIRAC system and are fully advised about the implementation dates associated with the information.

5.5 PROVISION OF CHARTS

5.5.1 The provisions of Annexes 4 and 15 are applicable to the content and visual presentation of the ICAO Annex 4 chart types and other AIP charts including those made available by State aeronautical information services over the Internet. Charts should be presented at scales that are compatible with Annex 4 requirements. If chart scaling is permitted, users should be informed of the scale range that will preserve chart quality. It is envisaged that, in the near term, most charts to be provided over the Internet will be identical in visual presentation to current hard-copy charts. However, some cartographic and geographic information systems (GIS) are capable of providing charts in formats with greater functionality including the ability for chart users to control what information is displayed. It is important that when electronic charts are presented in such formats, all relevant information be initially displayed to the user and that safety-critical information cannot be deselected.

5.5.2 The optimum graphic formats for the posting of maps and charts on the Internet may be different from those used in document production and must be chosen with the following general considerations in mind:

a) the availability of graphic output options from cartographic production software or scanners;

b) the availability of posted charts to clients (compatibility with operating systems, web browsers, colour rendering and client printers);

c) chart functionality and image quality;

d) chart data size (and therefore the transfer time); and

e) whether the format is an open standard or a commercial one with associated costs.

Chapter 6

MATTERS RELATING TO FLIGHT PLANS

6.1 INTRODUCTION

6.1.1 The purpose of this chapter is to provide guidance on the filing and management of flight plans (to and from the aeronautical fixed service (AFS)) via the Internet.

6.1.2 The Internet may be used as a means of providing applications for filing and collecting flight plans directly from users. Furthermore, the Internet allows feedback on the acceptance of flight plans and enables subsequent consultation and modification/cancellation of the filed flight plans. Internet flight plan applications are often offered in combination with AIS and MET applications providing the full set of required aeronautical information.

6.2 FLIGHT PLAN FILING

6.2.1 The standard flight plan format and validation criteria described in the *Procedures for Air Navigation Services — Air Traffic Management* (PANS-ATM, Doc 4444) should be adhered to.

6.2.2 The use of the Internet for flight plan filing could reduce the manual workload of air traffic services reporting offices by offering the user applications for collecting syntactically correct flight plans and safely passing them on for further processing in the operational flight plan environment.

6.2.3 It should be noted that a system can be vulnerable to a denial of service (DoS) attack via such an Internet interface. With unlimited and uncontrolled submission of flight plans, it would be possible to deny other legitimate users access to the service. Further, in a fully automated system, it could also be possible to affect the actual operational systems. The implementation of automatic or manual control procedures is required to reduce the risk of DoS attacks.

6.2.4 The filing of flight plans through the Internet can easily be extended to flights that do not have to file a flight plan. For example, this could facilitate monitoring of visual flight rule flights for search and rescue purposes.

6.3 FLIGHT PLAN MANAGEMENT

6.3.1 The Internet can provide the user direct access to information such as acknowledgment of, changes to or rejection of filed flight plans, in an automated and controlled manner, in real time, subject to the availability of the communication means and the required interfaces.

6.3.2 The user should be offered feedback on the acceptance of the flight plan, enabling subsequent consultation and modification/cancellation of a filed flight plan. The main risk to operational systems is non-compliance of the Internet applications with the appropriate interfaces to the AFS.

———————

Chapter 7

OTHER APPLICATIONS

7.1 AFTN-TYPE MESSAGING APPLICATION

7.1.1 It is acknowledged that use is being made of the Internet as an alternate means of exchanging AFTN-type messages between States in exceptional cases (e.g. where dedicated circuits are either unavailable/unreliable or uneconomical due to a low traffic level).

7.1.2 In any implementation of Internet-based AFTN-type communications, the procedures contained in Annex 10, Volume II, relating to the format, processing and retention of messages should be adhered to.

7.1.3 Due regard should be given to the risk assessment and management processes outlined in Chapter 3 of this manual.

— END —