Advisory Circular

U.S. Department
of Transportation
Federal Aviation Administration

Subject: INTERNET COMMUNICATIONS OF AVIATION WEATHER AND NOTAMS

Date: 11/1/02 **AC No.:** 00-62
Initiated by: ARS-100

1. PURPOSE. This Advisory Circular (AC) describes the process for any person or organization that provides access to aviation weather and Notices to Airmen (NOTAMs) via the Public Internet to become a Qualified Internet Communications Provider (QICP).

The FAA Aerospace Weather Standards Division (ARS-200) is responsible for establishing and maintaining a current list of all QICPs on a designated Web page accessible by the general public.

This AC pertains only to Internet communications between a civil aviation user and a QICP. This AC addresses data quality only to the extent of considering QICP security practices to protect data from unauthorized modification and encouraging the identification of the operational or experimental status of QICP products. The FAA Web page containing the current list of all QICPs contains a notice that being listed as a QICP does not mean that the quality of the QICP data (e.g., accuracy, timeliness or content) is certified or otherwise approved by the FAA.

Like all advisory material, this AC is not mandatory and does not constitute a regulation. Definitions used in this AC are contained in Appendix 1.

2. GENERAL. A person or organization that accomplishes and maintains the following as they pertain to the provider's facility (i.e., all hardware, software and Internet connectivity under the applicant's direct control) may become an approved QICP:

a. **Reliability** means users are able to retrieve requested data from the provider with no outage lasting longer than 10 minutes, and no more than 30 minutes of total outages (including outages due to maintenance) in any continuous 3-month period.

b. **Accessibility** means turnaround time within the provider's facility. The provider should be capable of initiating transmission of requested data during transactions with 100% of its users within 2 minutes.

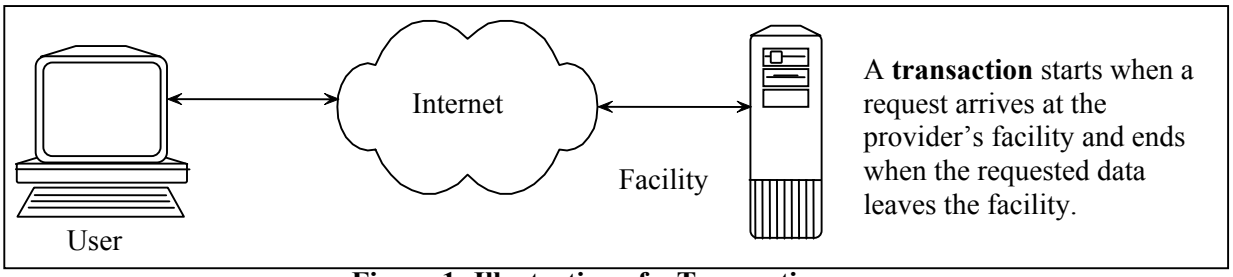

Figure 1: Illustration of a Transaction

c. **Security** means providing Internet site authentication and maintaining data integrity. The provider should implement security technology such as server digital certificate technology (such as X.509) and Secure Sockets Layer protocol consistent with current accepted Internet standards if using the hypertext transfer protocol, and equally secure technology if using an alternative Internet application protocol. In addition, the provider should establish and implement security practices to prevent unauthorized access to or modification of provider data, software and hardware.

1) Use of the Public Internet carries certain risks to both QICPs and users. Below are some of the more common risks:

a) The user receives intentionally corrupted data from an invalid source instead of original data from a legitimate source, not detecting the difference. The invalid source captured the original data en route and replaced it with intentionally corrupted data.
b) The user receives forged or fake data that purports to be from a legitimate source but is actually generated by an invalid source.
c) The user gets original data from a legitimate source, but it is inaccurate; it causes a problem in the user's operation and, subsequently, the source denies sending it in order to avoid culpability for the user's loss.

2) A server digital certificate mitigates these risks by providing Internet site authentication and two-way data integrity during the transaction between the QICP and the user.

3. RECOMMENDED PRACTICES.

a. User authentication: QICPs should consider user authentication (via browser digital certificate or username/password) as needed to determine the identity of the requester. In addition, QICPs should maintain a retrievable archive of Internet server log files as well as data received and provided in each transaction for a period of no less than 15 calendar days after the date of that transaction. In the event of receipt of notification of an accident, incident or overdue aircraft, or upon the request of the FAA or the National Transportation Safety Board (NTSB), the provider should retain the data related to that aircraft indefinitely, or until such time that the destruction of the data is authorized by law. The QICP should make this data available in the form of a readable certified true copy upon request of the FAA, the NTSB or a Federal, state or local law enforcement agency.

b. Product status: With the increasing availability of developmental weather products, QICPs are encouraged to clearly identify the operational or experimental status of each product. This

may be done by partitioning the Internet site, by grouping products or by labeling each individual product. Users are encouraged to require such identification by QICPs.

4. PROCESS FOR QUALIFICATION. To become a QICP, applicants should follow the qualification process described herein.

a. **Steps to Becoming a QICP.**

1) Submit an application certified by a responsible official to ARS-200 containing the following:

a) Service Description
b) Security Plan
c) Capability Demonstration Plan
d) Ongoing Maintenance Plan
e) Warning label

2) Satisfactorily complete the Capability Demonstration.

b. **Attachments to the Letter of Application**

1) **Service Description**: Describes how the applicant intends to accomplish the items in paragraph 2 and (optionally) the recommended practices in paragraph 3. The Service Description should include, at a minimum, the following items:

a) Intended user(s) or user class(es), estimated number of users in each user class
b) Server architecture (i.e., hardware, software)
c) Network management software
d) Server digital certificate technology
e) User authentication (optional)
f) Archival of Internet server log files and transaction data (optional)
g) Identification of product status as either operational or experimental (optional)

2) **Security Plan**: Describe how the applicant plans to prevent unauthorized access to or modification of applicant's data or facility (e.g., software, hardware, networks, etc.). These practices should include, at a minimum, the following:

a) Vulnerability assessments
b) Risk assessments
c) Security tests
d) Disaster recovery and contingency measures

3) **Capability Demonstration Plan:** Describes how the applicant plans to demonstrate that it can or has accomplished the items in paragraph 2 [“General”] and (optionally) the Recommended Practices, usually through a trial period of operations. An alternate demonstration method may be accepted by ARS-200 upon request of the applicant (e.g., documentation of prior Internet site performance). The Demonstration Plan should contain the following:

a) Primary points of contact for the demonstration
b) Period of time, including starting and completion dates

c) Performance statistics to be collected during the demonstration. (Note: These statistics could be collected using the same process as in paragraph 4.b.4)c) below.)
d) Proposed reporting format

4) **Ongoing Maintenance Plan:** Describes how the applicant plans to adequately maintain its Internet service and operation. This plan should include at least the following:

a) The names, titles and resumes of responsible personnel, with descriptions of their duties and responsibilities
b) System maintenance procedures
c) Quality Assurance Plan describing the process to collect and maintain performance statistics for the items in paragraph 2 ["General"] and to provide them to ARS-200 semiannually or upon request
d) Quality of Service (QOS) agreement(s) with each user or user class, specifying the items in paragraph 2 and providing user complaint procedures in the event QICP service and operation are not adequate

5) **Warning Label:** To ensure that users fully understand that a QICP means that FAA is only approving the provider's servers and communication interface as meeting the provisions of this AC and not approving the quality of data, it is strongly encouraged that an approved QICP display a warning label on its Internet site that addresses the above. The following language is recommended:

This Qualified Internet Communication Provider's (QICP) servers and communication interfaces are approved by the FAA as secure, reliable, and accessible in accordance with AC 00-62.

1) This QICP does not ensure the quality and currency of the information transmitted to you.
2) You the user, assumes the entire risk related to the information and its use.

c. **Application Review.** Upon receipt of the application, ARS-200 acknowledges receipt, reviews the submission and requests additional information if needed. ARS-200 plans to advise the applicant in writing of its findings within 60 calendar days from receipt. If unable to complete the review within this period, ARS-200 provides the applicant with a revised completion date. If the application package is lacking in some way, ARS-200 returns the submission to the applicant with recommendations for revision. If the application package is sufficient, ARS-200 notifies the applicant to proceed with its capability demonstration.

d. **Capability Demonstration.** Upon receiving notification to proceed, the applicant may demonstrate its Internet performance capability, usually by means of a trial period. During the trial period, the provider's Internet site should be fully operational. During and after the trial period, the applicant should report demonstration results to ARS-200 to document satisfactory accomplishment of the items contained in this AC.

e. **Application Disposition**

1) Upon successful completion of the capability demonstration, ARS-200 issues a letter approving the applicant as a QICP for a period of 6 months and adds the applicant's name to the QICP list maintained by ARS-200 on a designated Web page.

2) Should the FAA find the capability demonstration to be insufficient, ARS-200 issues a Letter of Denial, indicating the reasons for the denial. The form and content of any subsequent re-application are defined in the Letter of Denial.

5. ONGOING MAINTENANCE

QICPs should demonstrate ongoing maintenance of QICP status by collecting facility performance statistics and providing them to ARS-200 semiannually or upon request (e.g., following ARS-200 receipt of a user QOS complaint). ARS-200 reviews QICP statistics to verify continued performance maintenance; if verified, ARS-200 retains the provider's name on the QICP list for an additional period of 6 months. If a QICP does not adequately maintain its service and operation, ARS-200 notifies the provider in writing that QICP status may be rescinded unless the provider provides documentation within 30 calendar days that the deficiency has been corrected. If such documentation is not received or is unsatisfactory, ARS-200 may rescind QICP status and remove the provider's name from the QICP list.

QICPs should acknowledge and address user QOS complaints within 14 calendar days of receipt, and forward user QOS complaints to ARS-200 within 30 calendar days of receipt with an explanation of actions taken. ARS-200 and QICPs may collaborate to resolve any identified performance deficiencies. QICP failure to properly process or resolve QOS complaints may result in ARS-200 taking action as described in the preceding paragraph.

6. PAPERWORK REDUCTION ACT STATEMENT. As described in this AC, the FAA collects information contained in initial QICP applications and subsequent QICP reports of semi-annual facility performance statistics, archived data and user complaint corrective actions. The information is collected to enable ARS-200 to process initial QICP applications and determine continued QICP maintenance of its service and operation for the transmission of aviation weather and NOTAMs via the Internet; collected information may also be used by the FAA, the NTSB or law enforcement agencies following an accident, incident or overdue aircraft. The reporting burden for each QICP is estimated to average 568 hours during the initial year and 274 hours each subsequent year. Information submission is totally voluntary; however, failure to provide the information may result in the denial or loss of QICP status. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number. The OMB control number for AC 00-62 is 2120-0672.

7. ADDITIONAL INFORMATION

Questions or comments concerning this AC should be directed to:
FAA, Aerospace Weather Policy Division (ARS-100)
800 Independence Avenue, SW
Washington, DC 20591
(202) 385-7704

James H. Washington
Director, Air Traffic System Requirements Service

APPENDIX 1. DEFINITIONS OF TERMS

This appendix contains definitions of terms used throughout this AC.

Browser	User program allowing access to data via the Web
Browser Digital Certificate	Electronic equivalent of an ID card obtained employing digital certificate technology and installed on a user's browser—used in conjunction with a public key encryption system to automatically authenticate the user's identity.
Facility	All hardware, software and Internet connectivity under the provider's direct control.
Hypertext Transfer Protocol	The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the Web (World Wide Web).
Internet Certificate Standard	An Internet industry standard that defines what information can go into a digital certificate and describes the information format.
Internet Site Authentication	Technique by which access to Internet site resources requires a server digital certificate as identification.
Log File	An Internet server file containing access information regarding the activity on that server.
NOTAM	Aeronautical information that could affect a pilot's decision to make a flight. It includes such information as airport or primary runway closures, changes in the status of navigational aids, radar service availability, and other information essential to planned en route, terminal or landing operations. It can also contain mandatory emergency air traffic rules issued pursuant to the Code of Federal Regulations, Title 14, Section 91.139.
Provider	A person or organization (including a government agency) which supplies aviation weather and NOTAMs to a civil aviation user.
Public Internet	Any and/or all of the Internet sites that are accessible by any Internet connection. A distinguishing feature is its use of a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol).
Secure Sockets Layer Protocol	A security protocol that provides Internet site authentication, message integrity and message privacy over the Internet—allows provider/user applications to communicate while preventing message forgery, tampering and eavesdropping.
Server Digital Certificate	Electronic equivalent of an ID card obtained employing digital certificate technology and installed on an Internet site server—used in conjunction with a public key encryption system to automatically authenticate the Internet site's identity and ensure two-way data integrity during a transaction.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	The basic communication language or protocol of the Internet.
Transaction	All data exchanged between the user and provider beginning when the user's request arrives at the provider's facility and ending when the requested data leaves the facility.
User	A person or organization that requests and receives aviation weather and NOTAMs from a provider.
User Authentication	Technique by which access to Internet site resources requires user identification by such means as a browser digital certificate, or a username and password.
Web (World Wide Web)	All the resources and users on the Internet that use the Hypertext Transfer Protocol (or compatible protocols).