ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1370.90

8/1/03

SUBJ: Internet Access Point Configuration Management

1. **PURPOSE.** This order establishes the Federal Aviation Administration's (FAA) minimum configuration requirements for recognized FAA Internet Access Points (IAPs). This order does not relieve FAA organizations of the responsibility to complete the FAA certification and accreditation (C&A) process.

2. **DISTRIBUTION.** This order is distributed to the division level in Washington headquarters, regions, and centers, with a limited distribution to all field offices and facilities.

3. **BACKGROUND.** Order 1370.82, Information Systems Security (ISS) Program, as amended, provides the Office of the Assistant Administrator for Information Services and Chief Information Officer (AIO-1) with the authority to establish policy and assign organization and management for information and ISS-related issues. The FAA provides Internet access to its employees and on-site contractors through arrangements with commercial Internet Service Providers (ISPs). This service is routed through recognized IAPs described in FAA Order 1370.83, Internet Access Points. This order serves as the implementation directive to FAA Order 1370.83.

4. **DEFINITIONS.** The appendix contains specialized terms, definitions, relevant abbreviations, and acronyms.

5. **SCOPE.** This order applies to the following:

a. FAA offices, services, regions, centers, employees, contractors, support personnel, and users of FAA systems, applications, data, information, and other resources;

b. FAA systems, including systems within the National Airspace System, devices, networks, and applications that establish a connection to the Internet or use Internet resources;

c. Existing and future FAA Internet connections; and

d. Centralized configuration management of FAA IAPs through a cooperative effort between the designated approving authorities (DAAs) and AIO-1.

6. **RESPONSIBILITIES.** The following delineates roles and responsibilities.

a. **Director, Office of Information Systems Security, AIS-1,** must perform the following actions:

(1) Provide ISS policy and guidance to IAPs through the IAP Configuration Control Committee (CCC), and ISS Managers (ISSMs);

(2) Monitor and ensure compliance with this FAA order;

FOR OFFICIAL USE ONLY
(Public Availability To Be Determined Under 5 USC 552)

(3) Provide resources to IAP sponsors to purchase, maintain, and support product life cycle to meet the security requirements of this order;

(4) Coordinate with IAP administrators to verify effectiveness of security configuration(s); and

(5) Provide recommendations for perimeter routers to filter traffic before it gets to the internal FAA network.

b. IAP-Sponsoring Organizations must perform the following actions:

(1) Assign responsibilities to and manage the IAP administrators;

(2) Purchase products needed to meet the required protection as referenced in section 7a, with funding provided by AIS;

(3) Ensure IAP administrator positions have been designated critical-sensitive;

(4) Ensure each IAP administrator's background investigation has been completed under FAA Order 1600.1D, Personnel Security Program;

(5) Ensure IAP administrators have at a minimum the following skills:

(a) Sound understanding of network concepts and implementation;

(b) Knowledge of transmission control and Internet protocols; and

(c) Hands-on experience with networking concepts, design, and implementation so that IAP equipment is configured correctly and administered properly.

(6) Ensure IAP administrators receive regular training on all resources within the IAP(s) in use. This includes training on network security principals and practices to ensure accuracy;

(7) Ensure overall IAP system responsibility resides within the FAA and that only FAA employees are assigned to the role of IAP administrator;

(8) Ensure at least two IAP administrators (one primary and alternate(s)) are designated by the IAP sponsor. The IAP administrators are responsible for the maintenance of all IAP equipment;

(9) Provide the Computer Security Incident Response Center (CSIRC) with pertinent information necessary to contact the IAP administrator, designated alternate(s), or ISSM. These individuals may need to be contacted for notification of outages or security events and for coordination to ensure a timely response.

(10) Ensure major changes to IAP components (except firewalls) are approved through a sponsoring organization's configuration management control board before implementation;

(11) Establish and maintain controls for disaster recovery and availability of personnel in the event of an outage or incident. This activity ensures compliance with the continuity of operations and contingency planning guidelines described in FAA Orders 1370.82 and 1370.83, as amended;

(12) Ensure systems are in compliance with the guidelines in their system C&A plans; and

(13) Ensure that availability, integrity, and confidentiality of FAA resources are maintained and that individuals and organizations are accountable for the use of IAP services.

c. The IAP administrator must perform the following actions:

(1) Maintain a high level of knowledge about the configuration of the IAP system, inherent security weaknesses in the use of the system components, and FAA security policy;

(2) Create secure IAP administrative controls, access privileges, session controls, timeout controls, and software and account management controls in concert with the ISSM;

(3) Ensure new firewalls, virus filters, and routers are installed according to this order;

(4) Implement and maintain the security controls defined in this order for all equipment under IAP management;

(5) Maintain current inventory and point of contact information for all equipment and interfaces located within the IAP, including systems hosted in the demilitarized zone (DMZ);

(6) Each IAP administrator is required to implement and maintain the configuration of the components defined in Figure 1, Required IAP Configuration, and described in paragraph 7. The IAP CCC must review any deviations to this order for acceptance. All components must address security-hardening procedures; and

(7) Each IAP administrator is responsible for the operation and maintenance of the IAPs.

d. The ISSM for the line of business (LOB) operating the IAP must provide security information to the IAP administrator and take necessary risk-mitigating actions.

e. The Chief Information Officer of an IAP tenant must ensure that all of its Internet services operated within the DMZ are registered per FAA Order 1370.84, Internet Services.

7. PROCEDURES. Each IAP must implement the equipment and management procedures outlined below:

a. Required Protection. The following are the required minimum configuration protections necessary at each IAP:

(1) **Perimeter Router**. IAP sites are required to install and manage a local, FAA-controlled, external (frontwall) router at each IAP. Perimeter routers will contain access lists for defense in-depth posture on the frontwall routers completed within 90 days dependent on their required needs and services. All other routers (e.g., backwall routers) connected directly to an ISP are unauthorized. Only FAA personnel or FAA on-site contractors will manage perimeter routers. The IAPs will create a subcommittee for access lists that reports directly to the IAP CCC.

(2) **Switches**. A 10/100 or greater Ethernet switch will be installed between the perimeter router and the redundant firewalls. A second switch will be installed between the redundant firewalls and the backwall router. These switches will be used to connect the intrusion detection system (IDS) devices, as well as network and traffic analyzers.

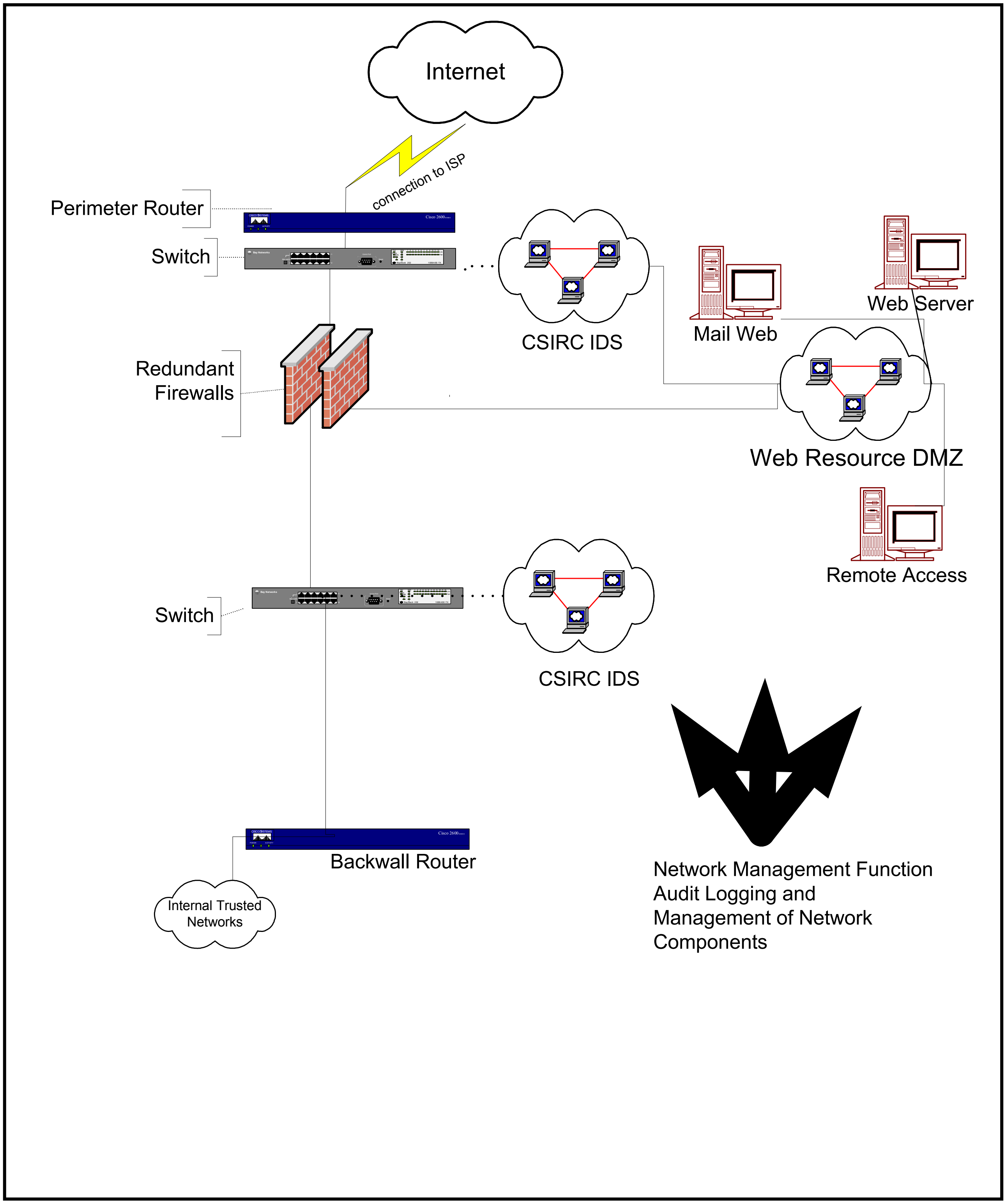

Figure 1 - Required IAP Configuration

The switches must have the ability and be configured to accomplish the following actions:

(a) Unused ports are disabled to prevent unauthorized access;

(b) Restrict a port to a particular Internet protocol address or number;

(c) Create multiple span ports to direct all network traffic to a specific port;

(d) Restrict administrative access to the device; and

(e) Block transmission of data from a given port while in span mode.

(3) **Redundant Firewalls**. IAP sites are required to have redundant firewalls to support multiple interfaces with a minimum of one external interface, one internal interface, and one DMZ interface. One interface can also include an out-of-band management interface.

(4) **DMZ**. IAPs are required to establish a dedicated DMZ for all resources made available to the public. DMZ resources must be connected to each of the redundant firewall interfaces. DMZ devices are prohibited from initiating connections anywhere, unless explicitly permitted in the firewall by the IAP administrator. Any site requiring multiple DMZs is required to establish, at a minimum, the same level of security for each DMZ or DMZ segment as described in this order. Creation of an extended DMZ within an IAP is acceptable provided each connection into the extended DMZ is configured under this order. For configuration purposes, the FAA considers any DMZ to be a hostile network to the internal FAA networks. Routing within the DMZ is permitted, whereas permanent physical connections circumventing the firewall are not permitted.

(5) **IDS.** IDS sensors installed at all IAPs will be non-intrusively managed, monitored, and maintained by the CSIRC. IDS sensors will be placed in front of and behind the redundant firewalls. Additional IDS sensors are permitted.

(6) **Network Management**. All IAP devices are administered out-of-band or using a secure transport protocol, such as secure shell or secure sockets layer.

(7) **Virus Filter**. All IAP sites must have a virus filter in the DMZ to search incoming hypertext transport protocol, file transfer protocol, and simple mail transfer protocol for binary signatures (patterns) of known viruses.

(8) **Vulnerability Scanning**. Each IAP site will be scanned under established processes and procedures. Scanning parties will conduct vulnerability scanning per the written agreement (e.g., Memorandum of Agreement, etc.) between AIO, the IAP administrators, and the IAP tenants. Scanning parties include the CSIRC and other authorized scanners, such as the Inspector General and/or LOBs. Each IAP tenant is responsible to ensure that vulnerabilities discovered in its systems are remediated. Each DAA retains authority to accept residual risk.

(9) **Load Balancing and Disaster Recovery**. Services hosted at the IAPs will require a plan for dependable customer access. The process for developing an enterprisewide disaster recovery plan (DRP) involves several phases, which must be coordinated through the IAP CCC. As each phase is generated, it will be added to the DRP. The phases are as follows:

(a) **Phase I:** Identification of services for disaster recovery in the event an IAP is lost. Each registered service in an IAP will be classified into one of five categories to facilitate planning for dependable service:

1. **Category 1**: No apparent break in services is expected even if the primary hosting facility is disabled.

2. **Category 2**: No more than a two-hour outage can be tolerated before switching to an alternate IAP.

3. **Category 3**: No more than a one-business day outage can be tolerated before switching to an alternate IAP.

4. **Category 4**: No more than a five-business day outage can be tolerated before switching to an alternate IAP.

5. **Category 5**: Greater than a five-business day outage can be tolerated before switching to an alternate IAP.

(b) **Phase II:** Determination of recovery resource requirements based on identification in Phase I (details to be determined after completion of Phase I).

(c) **Phase III:** Development of a draft enterprise IAP disaster recovery plan (EIAP DRP) (details to be determined after completion of Phase II).

(d) **Phase IV:** Development of the testing plan component of the EIAP DRP (details to be determined after completion of Phase III).

(e) **Phase V:** Development of the schedule component for EIAP DRP testing, testing and reporting lessons learned (details to be determined after completion of Phase IV).

b. Optional IAP Enhancements. There are three optional configuration protections available to be used by the IAPs. One is Virtual Private Networks (VPNs). VPNs use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or Extranets. Each type requires written rules of behavior or a memorandum of understanding between the parties. Any external VPN connection must terminate so that it can be monitored by the IDS. Any new VPN service(s) must utilize two-factor authentication. Existing VPN services must migrate to two-factor authentication. The other two types are cache engines and proxy servers. Appendix 1 contains current technical definitions for cache engines and proxy servers.

8. IAP PHYSICAL SECURITY. All IAP equipment is subject to FAA regulations for physical security under FAA Order 1600.69, FAA Facility Security Management Program, as amended. Physical access to routers, firewalls, and switches must be tightly controlled to preclude any unauthorized changes to the firewall configuration or operational status and to eliminate any potential for unauthorized monitoring of firewall or router activity.

9. INFORMATION DISCLOSURE. The implementation of this order may assemble information that is subject to protection under the certain exemptions contained in the Freedom of Information Act 5 USC 552; therefore, any requests must be reviewed for these considerations.

10. CONTACT INFORMATION. Information requests concerning this order may be addressed to the Office of Information Systems Security, AIS-1.

Daniel J. Mehan
Assistant Administrator for Information Services
and Chief Information Officer

APPENDIX. DEFINITIONS

Cache Engines. Referred to as content delivery devices, these are devices close to users that save (cache) Web pages and possibly file transfer protocol (FTP) and other files that all server users have requested so that successive requests for these pages or files can be satisfied by the cache server rather than requiring the use of the Internet. A cache server not only serves its users by getting information more quickly but also reduces Internet traffic. Cache engines are essential for enhancing performance in saturated networks and accelerate content delivery. A cache server is almost always also a proxy server.

Computer Security Incident Response Center (CSIRC). The CSIRC is FAA's 24/7 computer security center. The CSIRC monitors FAA network activity and outages, processes all reports of computer security incidents against FAA Internet access points (IAPs); installs, operates, and maintains intrusion detection systems (IDSs) at the IAPs; and provides the local IAP administrators with access to IDS data relative to their IAP.

Configuration Control Committee (CCC). A committee designed to provide guidance for all issues relating to IAP configuration management and access to FAA systems and resources, perform comprehensive reviews of IAP justification papers, and review requests for deviation from IAP standards. This committee also makes recommendations on network, hardware, and software requirements; equipment standards; component configurations; and protocols and services authorized at each IAP.

Dedicated Point-to-Point Virtual Private Network (VPN) Tunnels. High-speed broadband connections that provide a cost-effective solution for connecting remote offices and extranets.

Demilitarized Zone (DMZ). A computer host or small network inserted as a "neutral zone" between an organization's private network and the outside public network. In practice, DMZs act as proxy servers to prevent outside users from getting direct access to a server containing proprietary data, while supplying publicly available information.

Internal Users to External Enterprises VPNs. IAPs that allow FAA personnel to access external enterprises in support of an FAA business need.

Internet Access Point (IAP). Any physical or logical connection to the public Internet. An IAP includes any direct or permanent connection or any dial-up or temporary connection to the Internet.

IAP Administrator. An individual responsible for the configuration, account management, and performance of a computer network.

IAP Tenants. Organizations (lines of business or staff offices) who own or possess servers located within the DMZ(s) of the IAPs.

Internet Access. The connection to the public Internet or access to any Internet resource or information using any application, program, software, utility, or tool, for any reason or duration. Internet access includes any permanent or temporary connection to the Internet.

Internet Service Provider (ISP). The connection point or organization outside the FAA, connected either physically or logically to an IAP, that is the means by which the IAP gains access to the Internet.

Internet. A global network of independent hosts and communications facilities that connect users to those hosts. The term "Internet" also may refer to the content presented on the hosts or transmitted through the network. The FAA may contribute information and resources to the Internet for public consumption.

Intranet. The FAA's internal or private network used to share information and resources within the FAA community. Information and resources on the Intranet are not made available to the public.

Intrusion Detection Systems (IDS). A type of security management system for computers and networks that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Network. Communications hardware and software that allow a user or system to connect to another user or system and can be part of a system or a separate system. Examples include local area networks, wide area networks, and public networks such as the Internet.

Perimeter Router. A device that routes data between one or more networks and a third-party Internet gateway. A perimeter router is sometimes contrasted with a core router, which forwards packets to computer hosts within a network (but not between networks). A perimeter router is an example of an edge device and is sometimes referred to as a boundary router.

Proxy Servers. Proxy servers represent users by intercepting their Internet requests and managing them. Proxy servers are required because Agency Data Telecommunication Network 2000 does not enable default routing. A proxy server helps match incoming messages with outgoing requests and is in a position to also cache the files that are received for later recall by any user. To the user, the proxy and cache servers are invisible; all Internet requests and returned responses appear to be coming from the addressed place on the Internet.

Redundant Firewalls. A set of related programs, located at a network gateway server, protecting the resources of a private network from users from other networks. A firewall examines each network packet to determine whether to forward it toward its destination. The firewall allows remote access in to the private network or DMZ by the use of secure logon procedures and authentication certificates. Redundant firewalls allow all of the above measures to happen by working in series. If one firewall fails, the redundant firewall next in the series will take over the functionality. Redundant firewalls provide a measure of security so that there is no single point of failure.

User-to-Enterprise Virtual Private Networks (VPNs) for Telecommuters. VPNs that allow mobile workers, telecommuters, and FAA authorized users to gain access to the FAA intranet, providing users significant flexibility and efficiency.

Virtual Private Networks (VPNs). A connection between a remote computer and a server on a private network that uses the Internet as its network medium or a remote network and another network that uses the Internet as its network medium is known as a VPN. The remote computer and the network server then establish a secured connection that protects the data exchanged between them as it travels over the Internet. This technique is called tunneling, because the connection runs across the Internet inside a secure conduit, protecting the data in the way that a tunnel under a river protects cars from the water above it.