U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
National Policy

ORDER 1370.108

Effective Date
09/21/09

SUBJ: Voice Over Internet Protocol (VoIP) Security Policy

1. Purpose of This Order. This Order establishes the Federal Aviation Administration's (FAA) Voice over Internet Protocol (VoIP) security policy, and assigns responsibilities for establishing a secure VoIP Program. This Order will ensure that security requirements are known to support VoIP technology securely on FAA information systems.

2. Whom This Order Affects. This Order applies to those who are responsible for planning, implementing, maintaining, or securing FAA-owned or FAA-controlled VoIP systems and services. This order also applies to grantees, consultants, licensees, and any person or entity, domestic or foreign, having a formal written agreement with the FAA to plan, implement, maintain, or secure FAA-owned or FAA-controlled VoIP systems and services.

3. Where Can I Find This Order? This Order is available on the FAA's Intranet website at the URL https://employees.faa.gov/tools_resources/orders_notices/.

4. Scope. This Order applies to all FAA-owned or FAA-controlled information systems, telecommunication networks, and VoIP-enabled systems, devices, or components that process, store, or transmit VoIP traffic. This Order also applies to all personnel accessing FAA-owned or FAA-controlled information systems that process, store, receive or transmit VoIP. This Order provides oversight of the FAA enterprise implementation of security for VoIP services and hardware components. This order does not apply to National Security Systems, classified communications or the protection of classified information.

5. General. VoIP is a general term for a family of transmission technologies that deal with the delivery of voice communications over the Internet or other packet-switched networks. VoIP networks are IP-based networks that transmit voice data. VoIP systems usually interface with the traditional Public Switched Telephone Network (PSTN), allowing for transparent voice communications. The same security considerations and controls applied to an IP data network must be applied to a VoIP network. The ease of access to and prolific nature of VoIP connections, along with the ability to easily intercept and analyze network data will lead to unnecessary risk and compromise of FAA information.

6. Statutory Policy and Regulatory Mandates.

a. Code of Federal Regulations, Title 47, Chapter I Telecommunications, Federal Communications Commission (FCC), Part 9.5 Interconnected Voice over Internet Protocol Services, provides service requirements and conditions applicable to interconnected Voice over Internet Protocol service providers.

b. The Federal Information Security Management Act of 2002 (FISMA) states that each Federal department and agency must identify and provide information security protections

commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

c. The OMB Circular A-130, Appendix III, Management of Federal Information Resources, states that a minimum set of controls are to be included in Federal automated information security programs assigns Federal agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems. Federal departments and agencies must implement policies, standards, requirements, and procedures that are consistent with standards and guidance issued by the National Institute of Standards and Technology (NIST).

7. References. References are contained in Appendix A of this Order**.**

8. Definitions. Definitions of specialized terms used in this subject area, with relevant abbreviations and acronyms, are listed in this Order in Appendix B. All other definitions located in this Order that pertain to information systems security are stated in the FAA Order 1370.82A, Information Systems Security Program, Appendix B.

9. Notice of Exception or Noncompliance. This Order establishes policy to comply with statutory and regulatory requirements, including the NIST Special Publications made mandatory by the FISMA. Compliance with the policy established by this Order is mandatory.

10. VoIP Policy. The integration of voice and data into a single physical network is a complex process that may introduce vulnerabilities and risk. In order to mitigate these risks, the following policy statements must be adhered to as stated below:

a. VoIP systems and networks must adhere to a common security configuration recommended by the NIST Security Checklist Program (http://nvd.nist.gov/ncp.cfm), the FCC, and FISMA security requirements.

b. VoIP equipment used to transmit or discuss sensitive unclassified information must be protected with FIPS 140-2 encryption standards and in accordance with FAA Order 1370.103, Encryption Policy and FAA Order 1600.75, Protecting Sensitive Unclassified Information.

c. Use only cryptographic modules that are FIPS 140-2 compliant and approved by the NIST Cryptographic Module Validation Program (http://csrc.nist.gov/groups/STM/cmvp) list to protect FAA SUI and SPII data in digital form.

d. VoIP systems must follow the NIST SP 800-58 security guidance on the separation of data and voice networks.

11. Roles and Responsibilities. All FAA organizations must comply with the roles and responsibilities per the FAA Order 1370.82A, and carry out the additional responsibilities as follows:

a. The FAA Chief Information Security Officer must (CISO):

(1) Oversee the VoIP security implementation and management process;

(2) Develop the FAA VoIP security policy and approve LOB/SO VoIP security methodologies;

(3) Review and approve the VoIP security implementation plans as submitted by the LOBs/SOs; and,

(4) Ensure the FAA enterprise VoIP technologies are implemented in accordance with this Order.

b. LOBs/SOs must:

(1) Submit the VoIP security implementation plans to the CISO for approval.

(2) Implement, manage, and maintain the VoIP security infrastructure;

(3) Ensure the security implementation, management, and maintenance of the VoIP infrastructure is in accordance with this Order;

(4) Develop internal security processes and procedures for the security implementation, management, and maintenance of the VoIP infrastructure; and

(5) Ensure usage restrictions are documented for VoIP technology and equipment implemented within or utilized by a network or system.

12. Administrative Information.

a. The FAA AIO/CIO can issue changes to the FAA Information Systems Security Program. The AIO/CIO's office approves changes that set policy, delegate authority, and assign responsibility.

b. Each LOB/SO may develop additional guidance and procedures to ensure compliance with this Order. Any LOB/SO doing so must provide a copy of the supplement to this Order to the Director of AIS. All FAA organizations are encouraged to go beyond the requirements of this Order to address business, operational, or security needs, but the requirements of this Order must not be reduced.

13. Distribution. This Order is distributed to divisions in headquarters, regions, and centers with information systems or information systems security responsibility. Headquarters, regions, and centers must send this Order to all field offices and facilities within 30 days.

David M. Bowen
Assistant Administrator for Information Services
and Chief Information Officer

Appendix A. – References

- Federal Management Regulation, Subchapter F, Part 102-172 Telecommunications Management Policy.
- Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003.
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
- NIST, SP 800-53, Recommended Security Controls for Federal Information Systems, December, 2007, Revision 2.
- NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008.
- NIST SP 800-58, Security Considerations for Voice over Internet Protocol, January 2005.
- NIST SP 800-63, Electronic Authentication Guideline, April 2006
- FAA Order 1280.1B, Protecting Personally Identifiable Information (PII), December 17, 2008.
- FAA Order 1370.82A, FAA Information Systems Security Program, September 11, 2006.
- FAA Order 1370.89 Information Operations Conditions, August 25, 2003.
- FAA Order 1370.90 Internet Access Point Configuration Management, August 1, 2003.
- FAA Order 1370.91, Patch Management, May 19, 2004.
- FAA Order 1370.103, Encryption Policy, November 14, 2008.
- FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI), February 1, 2005.

Appendix B. Definitions and Acronyms

Interconnected VoIP Service. An interconnected Voice over Internet Protocol (VoIP) service is a service that provides IP-enabled voice service and

(1) Enables real-time, two-way communications;

(2) Requires a broadband connection for the user's location;

(3) Requires Internet protocol-compatible customer premises equipment (CPE); and

(4) Permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.

Public Safety Answering Point (PSAP). The PSAP is the dispatch office that receives emergency calls from the public. A PSAP may be a local fire or police department, an ambulance service, or a regional office covering all services.

Public Switched Telephone Network (PSTN). The world's collection of interconnected voice-oriented public telephone networks, both commercial and government-owned. It's the aggregation of circuit-switching telephone networks.

Pseudo Automatic Number Identification (Pseudo-ANI). A number consisting of the same number of digits as ANI that is not a North American Numbering Plan telephone directory number and may be used in place of an ANI to convey special meaning. This special meaning assigned to the pseudo-ANI is determined by agreements, as necessary, between the system originating the call, intermediate systems handling and routing the call, and the destination system.

Sensitive Unclassified Information (SUI). SUI is any unclassified information in any form including: print, electronic, and visual and audio forms that must be protected from unauthorized disclosure outside of the FAA. The SUI is subject to limited, controlled distribution within the FAA as determined by the information steward. This includes personally identifiable information, aviation and homeland security, and protected critical infrastructure information, all of which may qualify for withholding from the public under the FOIA, 5 United States Code #552.

Sensitive Personally Identifiable Information (SPII). SPII is the personally identifiable information that, if released for unauthorized use, is likely to result in substantial harm to the individual to whom such information relates.

Voice over Internet Protocol (VoIP). VoIP is a general term for a family of transmission technologies for delivery of voice communications over the Internet or other packet-switched networks. This technology uses the Internet IP instead of traditional analog systems to transmit voice over packet-switched IP networks. VoIP systems carry telephony signals as digital audio encapsulated in a data-packet stream over IP.

Wireline Network. A wired network, traditionally using copper wire or even fiber for transmission, as opposed to a wireless network, which uses radio frequencies to carry data.