U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

ORDER
JO 1370.124

National Policy

Effective date:
12/12/2022

SUBJ: National Airspace System (NAS) Wireless Use

This order establishes direction and policies for the supply and use of wireless communications technologies to support National Airspace System (NAS) operational service threads within the NAS domain of the FAA Enterprise. While a significant portion of the NAS telecommunications infrastructure relies heavily on analog and digital Time Division Multiplexing/Pulsed Code Modulation (TDM/PCM) technologies, the telecommunications industry is evolving from offering T-Carrier/Synchronous Optical Network (SONET) to Ethernet/Multi-Protocol Label Switching (MPLS)/Internet Protocol (IP)-based services over optical fiber. With this commercial transition at several remote locations, there may be a significant increase of FAA reliance on wireless technologies. Therefore, this order intends to establish guidelines and policies for the use of such wireless communications technologies to assist with this transition.

This order and intended guidelines and policies are applicable to all Headquarters, Technical Center, Logistics Center, Service Areas, Service Centers, Control Center, District and System Support Center personnel associated with the NAS.

TIMOTHY L AREL
Digitally signed by TIMOTHY L AREL
Date: 2022.12.12 08:46:17 -05'00'

Timothy L. Arel
Chief Operating Officer
Air Traffic Organization

Table of Contents

Chapter 1 – General Information

1. Purpose of this Order. This Order establishes guidance and policies for the provisioning and use of wireless communications technologies to support National Airspace System (NAS) operational service threads within the NAS domain of the FAA Enterprise.

2. Audience. This order applies to all Headquarters, Technical Center, Logistics Center, Academy, Service Area, Service Center, Control Center and District and System Support Center personnel associated with the NAS.

3. Where Can I Find This Order? You can find an electronic copy of this order on the Directives Management System (DMS) website: https://employees.faa.gov/tools_resources/orders_notices/ or go to the MyFAA employee website, select, "Tools and Resources', then select 'Orders and Notices.

4. Background. A significant portion of the NAS telecommunications infrastructure historically depends on analog and digital Time Division Multiplexing / Pulsed Code Modulation (TDM/PCM) technologies.

The telecommunications industry formally announced plans to evolve their network infrastructure (access and transport segments) from T-carrier/Synchronous Optical Network (SONET) to Ethernet/Multi-Protocol Label Switching (MPLS)/Internet Protocol (IP)-based services over optical fiber. As part of this strategy the commercial carriers are:

a. Retiring copper and copper-based infrastructure**;**

b. Retiring Integrated Services Digital Network (ISDN) and Digital Subscriber Line (xDSL) in access segment and SONET in Metropolitan Area Network/Wide Area Network (MAN/WAN) transport segment; and

c. Providing wireless access to locations where fiber is impractical or too expensive**.**

The FAA is simultaneously reducing its use of legacy communications systems.

The rollout of this commercial technology evolution has initiated. While the full commercial evolution will be spread over a significant time period the FAA has already begun to see the impacts.

The commercial transition to wireless access services at many remote locations where fiber lines may not be practical, may significantly increase FAA reliance on wireless technology. This order is intended to establish guidelines and policies for the use of wireless communications technologies within the National Airspace System.

5. Definition of Terms. Definitions are provided to clarify the requirements of this order. These definitions are included to provide a commonality of language in establishing service availability and resiliency plans and can be found in Appendix 1.

6. Scope. This order applies to NAS Internet Protocol-based (IP) communications services using wireless transport which consists of a wide range of non-wired technologies and protocols including but not limited to:

a. Wireless Personal Area Networks (WPANs), which include infrared, Radio Frequency Identification (RFID) and low power Bluetooth technologies (IEEE 802.15.X);

b. Wireless Local Area Networks (WLANs), which include various forms of Wi-Fi technology (IEEE 802.11YY);

c. Wireless Metropolitan Area Networks (WMANs), which include Worldwide Interoperability for Microwave Access (WiMAX) technology (IEEE 802.16); and

d. Wireless remote facility NAS network access and Wireless Wide Area Networks (WWANs), which include but are not limited to: Satellite, Terrestrial Microwave, and Long Term Evolution (LTE) services. For the purposes of this order, the various WWAN and WWAN access technologies have been categorized based on implementation characteristics which vary from implementation to implementation, including but not limited to:

(1) Shared capacity Commercial Off-the-Shelf (COTS) solutions (e.g. commercial LTE services, Iridium, etc.). A key characteristic of the shared capacity COTS concept of operations is that network capacity is shared among all service users, and typically cannot be dedicated or reserved for a particular user set, such as the NAS Domain of the FAA Enterprise; and

(2) Dedicated capacity COTS service: (e.g., commercial Very Small Aperture Terminal (VSAT) and tailored LTE applications such as FirstNet). Dedicated capacity COTS services are assumed to have the capability to allocate/reserve and prioritize service capacity for specialized users such as the NAS Domain of the FAA Enterprise. Service infrastructure can either be dedicated to a particular application or shared with other users of the services, but in a manner that can ensure required capacity for reserved and prioritized applications.

It should be noted that the requirements as stated in this wireless use order address the capability and operational concepts of the overall NAS domain infrastructure, associated service thread implementations, and how they should or should not use various wireless technologies. As such, the requirements are intended to be addressed by a combination of the overall telecommunications network leveraging wireless technologies (and in some cases user systems) rather than individual wireless subsystems.

7. Policy.

a. Wireless Personal Area Networks Use

(1) The use of Wireless Personal Area Networks (WPAN) and protocols to establish WPAN services for interactions between users, systems, or system components within the NAS domain must adhere to the following restrictions:

(a) The use of WPAN technology and associated protocols to support interactions between users, systems, or system components within the NAS domain and any entity not in the NAS domain is prohibited;

(b) The use of WPAN technology and associated protocols to control and manage NAS infrastructure is prohibited, unless limited for a specific application and pre-approved by the Air Traffic Organization (ATO) Authorizing Official Designated Representative (AODR). Any application of WPAN technology for control and management of NAS infrastructure must be isolated (as defined in FAA Order 1370.121, NAS Information Security and Privacy Programs & Services) from the telecommunications network infrastructure used to support either intra-facility or inter-facility communications services in the NAS Domain;

(c) The use of WPAN technology and associated protocols to inject any form of data or information into the NAS domain is prohibited. All inter-domain interactions are required to leverage approved NAS Domain Boundary Protections (DPB) infrastructure and security controls; and

(d) Application of WPAN technology and associated protocols to connect portable NAS devices to the NAS Operational IP Network must be limited to one-way information flows from NAS infrastructure to the portable NAS device.

(2) Any proposed use of WPAN-based capabilities for interactions between users, systems, or system components within the NAS domain, that utilize frequencies that the Federal Communications Commission (FCC) did not designate as unlicensed, or licensed with a blanket license to use anywhere, must be coordinated with the Director of Technical Operations Air Traffic Control (ATC) Spectrum Engineering Services in order to ensure the proposed use of licensed or unlicensed spectrum is evaluated and certified for integration into NAS operations as required by the current/latest revision(s) of the following: (i) FAA Order 6050.19, *Radio Spectrum Management*; and (ii) FAA Order 6050.32, *Spectrum Management Regulations and Procedures Manual*.

Coordination with the Spectrum Management Office must be of sufficient detail to ensure the envisioned WPAN application and services are capable of operating within required performance levels without imposing any spectrum interference or operational degradation to the NAS systems using the application or any other NAS systems or services.

(3) Any proposed use of WPAN technology within the NAS domain must be approved prior to development activities by the ATO Authorizing Official Designated Representative (AODR) and be Authorized to Operate by the ATO Authorizing Official (AO) prior to implementation within the NAS.

(4) Any proposed use of WPAN technology within the NAS domain must be reviewed and approved by the FAA's Communications, Information, and Network Programs (CINP) Architecture Review Board, where it must be demonstrated that:

(a) The envisioned WPAN application satisfies the required level of data integrity and data confidentiality of NAS data (as stated in FAA Order 1370.121*, FAA Information Security and Privacy Program & Policy*) while being transported by the WPAN application;

(b) The envisioned WPAN application satisfies all functional and performance service level agreements (SLAs) of the required communication service;

(c) The supported NAS service thread does not compromise the data integrity or data confidentiality level of the NAS systems leveraging the WPAN application;

(d) The supported NAS service thread does not degrade any other NAS service thread or supporting communications service; and

(e) The WPAN infrastructure and operations include controls and associated processes and procedures to inhibit any entity from accessing the WPAN infrastructure via the Internet.

b. Wireless LAN Use

(1) The use of Wireless Local Area Networks (WLAN) and protocols to establish WLAN services for interactions between users, systems, or system components within the NAS domain must adhere to the following restrictions:

(a) The use of WLAN technology and associated protocols to support interactions between users, systems, or system components within the NAS domain and any entity not in the NAS domain is prohibited;

(b) The use of WLAN technology and associated protocols to control and manage NAS infrastructure is prohibited, unless limited for a specific application and pre- approved by the AODR;

(c) The use of WLAN technology and associated protocols to inject any form of data or information into the NAS domain is prohibited, unless limited for a specific application and pre-approved by the AODR; and

(d) Application of WLAN technology and associated protocols to connect portable NAS devices (e.g. laptops or mobile devices) to the NAS infrastructure must be limited to one-way information flows from NAS infrastructure to the portable NAS devices, unless limited for a specific application and pre-approved by the AODR.

(2) Any proposed use of WLAN-based capabilities for interactions between users, systems, or system components within the NAS domain, that utilize frequencies that the FCC did not designate as unlicensed, or licensed with a blanket license to use anywhere, must be coordinated with the Director of Technical Operations ATC Spectrum Engineering Services in order to ensure the proposed use of licensed or unlicensed spectrum is evaluated and certified for integration into NAS operations as required by: (i) FAA Order 6050.19F, *Radio Spectrum Management*; and (ii) FAA Order 6050.32B, *Spectrum Management Regulations and Procedures Manual*.

Coordination with the Spectrum Management Office must be of sufficient detail to ensure the envisioned WLAN infrastructure and services are capable of operation without proposing any spectrum interference or operational degradation to the NAS systems using the application or any other NAS system or services within range of the WLAN transmissions.

(3) Any proposed use of WLAN technology within the NAS domain must be approved prior to development activities by the ATO AODR and be Authorized to Operate by the ATO Authorizing Official (AO) prior to implementation within the NAS.

(4) Any proposed use of WLAN technology within the NAS domain must be reviewed and approved by the FAA's Communications, Information, and Network Programs (CINP) Architecture Review Board, where it must be demonstrated that:

(a) The envisioned WLAN application satisfies the required level of data integrity and data confidentiality of NAS data (as stated in FAA Order 1370.121*, FAA Information Security and Privacy Program & Policy*) while being transported by the WLAN application;

(b) The envisioned WLAN application satisfies all functional and performance SLAs of the required communication service;

(c) The supported NAS service thread does not compromise the data integrity or data confidentiality level of the NAS systems leveraging the WLAN application; and

(d) The supported NAS service thread does not degrade any other NAS service thread or supporting communications service.

c. Wireless Metropolitan Area Network (WMAN) Use

(1) NAS Metropolitan Area Networks (MAN) telecommunications provided by wire-based technologies have become costly to implement, maintain, and expand. To address this issue, the FAA has implemented an enterprise NAS dedicated WiMAX service to support NAS WMAN requirements. This service, known as Aeronautical Mobile Airport Communication System (AeroMACS), is currently provided via the FAA Telecommunications Infrastructure (FTI) contract and is envisioned to be supported by any FTI follow-on or replacement program. The AeroMACS service is currently the only Authorized WMAN service for NAS use.

(2) If it is determined that AeroMACS services are not the most appropriate for a particular NAS MAN telecommunications service need, additional WMAN technologies service offerings and concepts may be proposed, authorized and implemented per the guidelines defined in the following paragraphs.

(3) Any proposed use of additional WMAN technology for NAS MAN telecommunications services must be approved prior to development and implementation activities by the ATO AODR, and must be Authorized to Operate by the ATO AO prior to use within the NAS.

(4) Any proposed use of additional WMAN technology for NAS MAN telecommunications services must be reviewed and approved by the FAA's CINP Architecture Review Board, where it must be demonstrated that:

(a) The envisioned WMAN application satisfies the required level of data integrity and data confidentiality of NAS data (as stated in FAA Order 1370.121*, FAA Information Security and Privacy Program & Policy*) while being transported by the WMAN application;

(b) The envisioned WMAN application satisfies all functional and performance SLAs of the required communication service;

(c) The supported NAS service thread does not compromise the data integrity or data confidentiality level of the NAS systems leveraging the WMAN application;

(d) The supported NAS service thread does not degrade any other NAS service thread or supporting communications service;

(e) The envisioned WMAN infrastructure and operations include controls and associated processes and procedures to inhibit any entity from accessing the WMAN infrastructure via the Internet and

(f) The envisioned WMAN infrastructure and operations include controls and associated processes and procedures to inhibit interactions between users, systems, or system components within the NAS domain and any entity not in the NAS domain.

(5) Any proposed use of additional WMAN infrastructure for interactions between users, systems, or system components within the NAS domain must be coordinated with the Director of Technical Operations ATC Spectrum Engineering Services in order to ensure the proposed use of licensed or unlicensed spectrum is evaluated and certified for integration into NAS operations as required by: (i) FAA Order 6050.19F, *Radio Spectrum Management*; and (ii) FAA Order 6050.32B, *Spectrum Management Regulations and Procedures Manual*.

Coordination with the Spectrum Management Office must be of sufficient detail to ensure the proposed use of additional WMAN infrastructure and services are capable of operation without proposing any spectrum interference or operational degradation to the NAS systems using the application or any other NAS system or services within range of the additional WMAN infrastructure transmissions.

d. Wireless Wide Area Networks (WWAN) and Remote Facility Wireless Network Access Use

It is becoming necessary for the FAA to supplement wired access services at remote locations with a combination of owned, dedicated, leased, and shared commercial wireless access services in order to address the decommissioning of commercial Time Division Multiplexing (TDM)-based access services at these remote locations. This is particularly true when the remote locations support high availability NAS service threads that require diverse access at these facilities.

(1) All proposed use of wireless technologies to support remote facility NAS network access services and/or WWAN capabilities must be approved prior to development and implementation activities by the ATO AODR, and must be Authorized to Operate by the ATO AO prior to operational use within the NAS domain.

(2) All proposed use of wireless technologies to support remote facility NAS network access services and WWAN capabilities must be approved by the FAA's CINP Architecture Review Board, where it must be demonstrated that:

(a) The envisioned wireless NAS network access services and/or WWAN application satisfies the required level of data integrity and data confidentiality of NAS data (as stated in FAA Order 1370.121, FAA Information Security and Privacy Program & Policy) while being transported by the WMAN application;

(b) The envisioned use of the wireless NAS network access services and/or WWAN application within the overall network design and operational concepts satisfies all functional and performance SLAs of the required communication service; and

i. The envisioned wireless NAS network access services and/or WWAN application must satisfy all functional and performance SLAs allocated to it via its role in the overall communications service design.

ii. Any wireless NAS network access service and/or WWAN application and associated concept of operation must sufficiently prioritize the envisioned NAS service requests on the Radio Access Channel and assignments on the Operational Transmissions Channels, to ensure NAS services are not blocked during the service connection or service operations phase of the wireless service.

iii. Any wireless NAS network access services and/or WWAN application and associated concept of operation must reserve sufficient transmission resources for the NAS application to support all envisioned services.

iv. Any proposed used of WWAN services within the overall network infrastructure and concepts of operations must be preapproved by a safety panel.

(c) The supported NAS service thread does not compromise the data integrity or data confidentiality level of the NAS systems leveraging the wireless NAS network access services and/or WWAN application.

i. Segmented encryption is allowed on dedicated capacity COTS WWAN service implementations, provided unencrypted information only traverses dedicated service segments (i.e. end-to-end encryption is not required for services that cannot support end-to-end encryption, such as dedicated VSAT services).

ii. The supported NAS service thread does not degrade any other NAS service thread or supporting communications service.

(3) Wireless NAS network access services and/or WWAN infrastructure and operations must include controls and associated processes and procedures to inhibit any interactions between systems connected to the WWAN services and the Internet via the WWAN service.

(4) Wireless NAS network access or WWAN services must satisfy all functional and performance SLAs of the required communication service including any required path/equipment diversity and avoidance requirement.

(a) In cases where wireless NAS network access services and/or WWAN- based technology is used as one of the avoided paths providing path diversity for a single high availability NAS service, the overall network infrastructure design and concepts of operations must be demonstrated to provide alternative transmission paths that have no single point of failure in either their forwarding plane (including transmission paths and equipment) or their route control plane (including no common mode of failure of either route determination or route management resources) that would simultaneously impact both paths.

(b) In cases where wireless NAS network access services and/or WWAN- based transmission is used to provide remote site connectivity for one service of a pair of avoided services, the implementation of the wireless-based service must ensure there is no single point of failure between the WWAN-based access service and the other access service in either their forwarding plane (including avoided transmission paths and components) or route control plane (including no common mode of failure of either route determination or route management resources) that would simultaneously impact both access services.

(c) Requirements (a) and (b) above do not imply that an individual WWAN service must provide network diversity, but rather that the overall design of the network incorporating the WWAN service must support network diversity when leveraging the wireless technologies.

(5) Any proposed use of WWAN-based capabilities for interactions between users, systems, or system components within the NAS domain, that utilize frequencies that the FCC did not designate as unlicensed, or licensed with a blanket license to use anywhere, must be coordinated with the Director of Technical Operations ATC Spectrum Engineering Services, in order to ensure the proposed use of licensed spectrum is evaluated and certified for integration into NAS operations as required by: (i) FAA Order 6050.19F, Radio Spectrum Management; and ii FAA Order 6050.32B, Spectrum Management Regulations and Procedures Manual.

Coordination with the Spectrum Management Office must be of sufficient detail to ensure the envisioned WWAN application and services are capable of operation within required performance levels without proposing any spectrum interference or operational degradation to the NAS systems using the application or any other NAS systems or services.

e. Wireless Technology Security Requirements

(1) For all wireless technology applications identified in paragraphs (a)-(d) above, the NAS wireless application must follow the standard ATO architecture review and approval process, which includes approval via the CINP Architecture Review Board (ARB).

(2) Any use of commercial provider wireless capabilities must include a formally documented SLA to be a part of the wireless infrastructure architecture review that defines how the provider will address the following requirements:

(a) Shared capacity COTS and FAA owned wireless infrastructure must provide reserved resources and resource management capabilities to guarantee the required data rate and any associated SLA (e.g. availability and latency) required by the NAS services being supported;

(b) Shared capacity COTS and FAA owned wireless service operations must include radio access channel prioritization schemes for NAS services and sufficient transmission service capacity to prevent pre-emption and /or degradation of NAS services by non-NAS traffic;

(c) Use of shared capacity COTS service must be pre-approved by a safety panel;

(d) Wireless infrastructure and operations must provide logically isolated end-to-end NAS services;

(e) Wireless infrastructure and operations must prevent Denial of Service attacks from other users of any shared infrastructure, capabilities or resources; and

(f) Wireless infrastructure and operations must not include any Layer 3 association between any shared resources or resource management assets and dedicated FAA resources or resource management assets.

(3) All use of wireless infrastructure and operations must include Federal Information Processing Standard (FIPS)140-2, or current version, encryption across the wireless infrastructure to:

(a) Provide NAS data confidentiality by preventing the disclosure of NAS data to unauthorized entities while being transported via the wireless infrastructure;

(b) Provide data integrity by preventing the insertion/deletion/modification of NAS data by unauthorized entities while being transported via the wireless infrastructure; and

(c) Segmented encryption is allowed, provided unencrypted information only traverses dedicated service segments (i.e. end to end encryption is not required for services that cannot support end to end encryption, such as VSAT services).

(4) All dedicated infrastructure implemented to provide NAS IP-based services via wireless infrastructure must be:

(a) Designed to adapt for emerging technology and policy changes;

(b) Be security patched/updated in accordance with ATO requirements;

(c) Be implemented with commercial-grade (or better) equipment;

(d) Provide security event log data to NAS Cyber Operations (NCO) to support security monitoring;

(e) Utilize equipment on the FAA approved equipment list where appropriate;

(f) Be subject to regular audits for vulnerabilities and rogue connectivity;

(g) Include system hardening in accordance with ATO approved Secure Configuration Baseline Standards; and

(h) Not use protocols that have been deprecated by the Federal Government or industry technical committees/organizations.

(5) All machine-to-machine interactions between NAS End Systems transported via wireless technologies for all or a subset of their physical layer transmissions must use strong authentication when establishing an application layer end-to-end association.

(a) Certificates and management provided by the Identity Access Management (IAM) program are required for authentication solutions.

(b) Use of a system other than IAM will require AO approval.

(c) For legacy systems that utilize TDM interfaces, or do not exercise end to end authentication, the overall network infrastructure and concepts of operations (FTI, FAA Enterprise Network Services (FENS), etc.) must utilize point to point encryption over the wireless transmission segment.

Segmented encryption is allowed for legacy systems that utilize TDM interfaces, or do not exercise end to end authentication, provided unencrypted information only traverses dedicated service segments (i.e. end to end encryption is not required for services that cannot support end to end encryption, such as VSAT services).

(6) In general, wired communications services are preferred for NAS service flows, whenever feasible and the used of wireless capabilities to support NAS services must only be implemented:

(a) In situations where wired solutions are not feasible and to support NAS services where it is a cost advantage to the program;

(b) To provide a diverse access capability to a wired service; and

(c) As a backup to a wired solution.

8. Roles and Responsibilities.

a. The ATO Authorizing Official (AO) is responsible for the security of all NAS systems.

The AO must provide Authority to Operate (ATO) for approved wireless technologies and applications prior to implementation in the NAS domain.

b. The ATO Authorizing Official Designated Representative (AODR) must:

(1) Approve wireless development activities prior to implementation within the NAS domain;

(2) Provide a recommendation to the AO whether the wireless technology should be Authorized to Operate in the NAS domain.

c. The NAS Information System Security Officer (ISSO) must:

(1) Assist the Information System Owner (ISO) and Information System Security Engineer (ISSE) in reviewing wireless technology implementations to determine NAS security compliance; and

(2) Provide a recommendation to the AODR whether the wireless technology should be Authorized to Operate in the NAS domain

d. The NAS Information Systems Owners (ISO) and Information System Security Engineer (ISSE) must:

(1) Comply with all FAA Orders, National Institute of Standards and Technology (NIST) standards, and published ATO wireless security guidelines;

(2) Utilize AO approved enterprise wireless services when available;

(3) Provide for physical security of the wireless equipment; and

(4) Submit a design to the ISSO for AODR approval**.**

Appendix A: Definition of Requirements and Terms

Aeronautical Mobile Airport Communication System (AeroMACS) is an FAA Wireless Metropolitan Area Network (WMAN) technology that is currently standardized in accordance with the Worldwide Interoperability for Microwave Access (WiMAX) technology. AeroMACS is authorized for use for communication on the airport surfaces, i.e. fixed wireless broadband access and mobile wireless subscribers on the airport surfaces.

Bluetooth is an open standard for short-range Radio Frequency (RF) communications. It is used for low-cost and low-power RF communications to wirelessly link phones, computers, and other network devices over short distances.

Classified Information is official information that has been determined, pursuant to Executive Order or Act of Congress, to require protection against unauthorized disclosure in the interest of national security. The term includes National Security Information (NSI), Restricted Data (RD), Formerly Restricted Data (FRD) and Foreign Government Information (FGI).

Infrared Peripheral Device (IPD*)* is any device that is connected to or part of a computer with an infrared hardware port. An IPD is not capable of full functionality in a stand-alone configuration. An IPD can include printers, scanners, facsimile machines, CD-ROM drive, floppy drives, modems, keyboards, mice, speakers, stylus pens, and others.

Institute of Electrical and Electronics Engineers (IEEE) is a worldwide professional association for electrical and electronics engineers that sets standards for telecommunications and computing applications.

IEEE 802.11a is a physical layer standard in the 5 GHz radio band. It specifies eight available radio channels (in some countries, 12 channels are permitted). The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is about half of that, and the throughput is shared by all users of the same radio channel.

IEEE 802.11b is a physical layer standard in the 2.4 GHz radio band. It specifies three available radio channels. Maximum link rate is 11 Mbps per channel, but maximum user throughput is about half of this because the throughput is shared by all users of the same radio channel.

IEEE 802.11g is a physical layer standard for Wireless Local Area Networks (WLANs) in the2.4 GHz and 5 GHz radio band. It specifies three available radio channels. The maximum link rate is 54 Mbps per channel, whereas 11b has 11Mbps. The IEEE 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with 11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolution coding (PBCC) modulation.

IEEE 802.11i is a standard for WLANs that provides improved encryption for networks that use the popular IEEE 802.11a, IEEE 802.11b (which includes Wi-Fi) and IEEE 802.11g standards. The IEEE 802.11i standard requires new encryption key protocols known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

IEEE 802.11x represents the family of Wi-Fi protocols including but not limited to, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n.

National Security System (NSS) is any telecommunications or information system operated by the U.S. Government. NSS functions and operations encompass the following activities:

Intelligence Activities; Crypto logic activities related to national security; Command and control of military forces; Processing and storage of classified information; Equipment that is an integral part of a weapon or weapons system; or, Information critical to the direct fulfillment of military or intelligence missions.

National Airspace System (NAS) System is a NAS-controlled information system or device that, although owned by another entity (such as a contractor), is used in performing NAS functions.

Network Diversity – Network implementation property that uses a combination of telecommunications access diversity, telecommunications transport diversity and operational redundancy to eliminate service flow single-points-of-failure, and minimizes common vulnerabilities (including unpredictable faults, natural disasters and human-caused errors) for high availability telecommunications service flows ordered with diversity and avoided service flow pairs within the following elements of the network architecture:

- Data Plane Architecture including (as applicable to specific service flow types):
  - Physical Layer (including Telecommunications Access Diversity and Telecommunication Transport Diversity).
  - Media Access Control (MAC) Layer (including frame forwarding functionality and protocols).
  - Network (IP) Layer (including packet forwarding functionality and protocols).
- Control Plane Architecture including (as applicable to specific service flow types):
  - MAC Layer path selection/determination protocols and resources.
  - Network Layer routing and route determination protocols and resources.
- Management Plane Architecture (as applicable to specific service flow types)
  - Functions and resources used to monitor, maintain situational awareness and control Media Access Layer infrastructure.
  - Functions and resources used to monitor, maintain situational awareness and control Network Layer infrastructure.

Personal Digital Assistant (PDA) is a handheld computer that serves as an organizer for personal information. It includes at least a name-and-address database, checklist, and note taker. The PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit includes a small on-screen keyboard that is tapped with the pen, so data is synchronized between a user's PDA and desktop computer by cable or wireless transmission.

Telecommunications Access Diversity – A service delivery location has *Telecommunications Access Diversity* when it has two or more telecommunications access capabilities that have no single point of failure by virtue of employing one or more of the following forms of access diversity, but not limited to:

- Physical Diversity
- Media Diversity
- Electrical Diversity

One or more of these forms of Telecommunications Access Diversity may be used to achieve the Availability and Survivability requirements required to provide overall network diversity.

Wireless Access Point (WAP). A WAP provides users with a mobile capability allowing users to freely move within an access point coverage area while maintaining connectivity between the user's client device and the access point. Configured appropriately, access points are linked together using wired infrastructure to allow users to "roam" between access points within a building.

Wireless devices provide users with the technical means of implementing various non-wired protocols and technologies including, but not limited to: (i) Wireless Personal Area Networks (WPANs), which include infrared, (IEEE 802.11), Radio Frequency Identification (RFID) (IEEE 802.15.4) and Bluetooth technologies (IEEE 802.15.1); (ii) Wireless Local Area Networks (WLANs), which include various forms of Wi-Fi technology (IEEE 802.11); (iii) Wireless Metropolitan Area Networks (WMANs), which include WiMAX technology (IEEE 802.16); and (iv) Wireless remote facility NAS network access and Wireless Wide Area Networks (WWANs), which include Satellite, terrestrial microwave, and Long Term Evolution (LTE) services.

Wireless Local Area Network (WLAN*)* is a group of wireless networking nodes within a limited geographic area (such as an office building or building campus) that are capable of radio communication. A WLAN is usually implemented as an extension of an existing wired local area network to provide increased mobility and network access.

Wireless Personal Area Network (WPAN) is a low powered, short-distance wireless network for interconnecting devices in a confined workspace. A WPAN is typically used to enable a few devices in a single room to communicate without the need to physically connect the devices with cables.

Wireless Metropolitan Area Network (WMAN) is a network used to provide services and technology focused on connecting both wired/wireless local area networks (LANs) within a defined geographical coverage area to each other. Connectivity to a WMAN is typically limited to network infrastructure resources, as opposed to individual systems in a WLAN or WPAN. For the purposes of this document WMANs are to be limited to a specific geographic region (e.g. on and around an airport), and some WMAN technologies (e.g. AeroMACS) are limited by policy or technology such that they cannot be used over long distances. As a result, not all WMAN technologies could be part of an overall FAA WMAN solution.

Wireless Wide Area Networks (WWAN) is a large (in terms of distance and/or complexity) network of wireless links used to connect facilities. WWAN technologies are typically used to connect smaller regional (e.g. WMAN) or single facility networks (e.g. WLAN) together. Individual computer nodes typically do not join a WLAN but would join a local network which was connected to the WWAN. The key difference between a WMAN and a WWAN is that a WWAN could be an entity that provides connectivity over great distances, while a WMAN is limited to a defined geographic region or campus.

World Interoperability for Microwave Access (WiMAX) is a standard (802.16) to implement Wireless Metropolitan Area Networks (WMAN). The WMAN provides connectivity to users located in multiple facilities, generally within a few miles of each other.

Appendix B: References

The following related publications are applicable to this notice. Other Federal laws, regulations, and guidance not listed here, such as Executive Orders, may apply.

FAA Order 1200.22E, External Requests for NAS Data, January 20, 2012

FAA Order 1370.114, Implementation of FTI Services and Information Security Requirements in the NAS, January 4, 2012

FAA Order 1800.66, Configuration Management Policy, September 19, 2007

FAA Order 1830.10, Managing New Telecommunications Requirements, December 5, 2005

FAA Registration Authority Registration Practices Statement (RPS) [in development]

Federal CIO Council, Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0 November 2009

Federal CIO Council, Personal Identity Verification Interoperability for Non-Federal Issuers, Version 1.1, July 2010

Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 2001

Federal Public Key Infrastructure Policy Authority, X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 2.25, December 9, 2011

Federal Public Key Infrastructure Policy Authority, X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 3647 - 1.17, December 9, 2011

Public Law 107-347, Federal Information Security Management Act of 2002, December 17, 2002

Public Law 107-296, Critical Information Infrastructure Act of 2002

OMB Circular Number A-130, Management of Federal Information Resources, November 28, 2000

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006

OMB Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011

National Strategy for Trusted Identities in Cyberspace, the White House, April 2011

NIST Special Publication 800-21 2nd edition, Guideline for Implementing Cryptography in the Federal Government, December 2005

NIST Special Publication 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000

NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001

NIST Special Publication 800-53, revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

NIST Special Publication 800-57, Recommendation for Key Management, March 2007

NIST Special Publication 800-63, Electronic Authentication Guideline, April 2006

NIST Special Publication 800-73-3, Interfaces for Personal Identity Verification, Feb. 2010

NIST Special Publication 800-48 Rev.1 Guide to Securing Legacy IEEE 802.11 Wireless Networks, October 2018

NIST Special Publication 800-98, Guide for Securing Radio Frequency Identification Systems, April 2007

NIST Special Publication 800-187, Guide to LTE Security, January 2018

NIST Special Publication 800-127, Guide to Securing WiMAX Wireless Communications, October 2018

Appendix C: Acronyms

AeroMACS - Aeronautical Mobile Airport Communication System

AIS – Office of Information Security & Privacy Service

AIT – Office of the Deputy Assistant Administrator for Information & Technology and Chief Information Officer

ANG – Office of NextGen AO – Authorizing Official

AODR – Authorizing Official Designated Representative

ASH – Assistant Administrator for Security and Hazardous Material Safety ATC – Air Traffic Control

ATO – Air Traffic Organization

ATO – Authority to Operate

CIO – Chief Information Officer

CISO – Chief Information Security Officer

COTS – Commercial Off-the-Shelf

DHS NCCIC – Department of Homeland Security National Cybersecurity and Communications Integration Center

DSL – Digital Subscriber Line

DoD – Department of Defense

FCC – Federal Communications Commission

FENS – FAA Enterprise Network Services

FIPS – Federal Information Processing Standard

FISMA – Federal Information Security Management Act

IAM – Identity Access Management

IP – Internet Protocol

IS – Information Steward

ISDN – Integrated Services Digital Network ISO – Information System Owner

ISSE – Information System Security Engineer

ISSO – Information System Security Officer

LOB – Line of Business

LTE – Long-Term Evolution

MAN – Metropolitan Area Network

MPLS – Multi-Protocol Label Switching

NIST – National Institute of Standards and Technology

NAS – National Airspace System

OPIP – Operational Internet Protocol

POA&Ms – Plan of Action and Milestones

R&D – Research and Development

SCA – Security Control Assessor

SO – Staff Office

SONET – Synchronous Optical Network

TDM – Time Division Multiplexing

VSAT – Very Small Aperture Terminal

WAN – Wide Area Network

WAP – Wireless Access Point

WiMAX – Worldwide Interoperability for Microwave Access

WLAN – Wireless Local Area Network

WMAN – Wireless Metropolitan Area Network

WPAN – Wireless Personal Area Network

WWAN – Wireless Wide Area Network