ARINC Project Initiation/Modification (APIM)

1.0 Name of Proposed Project APIM 18-008

Onboard Secure Wi-Fi Network Profile Standard

1.1 Name of Originator and/or Organization

Jeffrey Rae – United Airlines

2.0 Subcommittee Assignment and Project Support

2.1 Suggested AEEC Group and Chairman

Network Infrastructure and Security (NIS) Subcommittee – Jeffrey Rae

2.2 Support for the activity (as verified)

Airlines: Alaska Airlines, American Airlines, El Al Israel Airlines, FedEx, Lufthansa Airlines, United Airlines

Airframe Manufacturers: Airbus, Boeing,

Suppliers: Astronautics Corp. of America, Astronics (TBC), AstroNova (TBC), Esterline Avionics, GE Aviation, GoGo, Honeywell, Miltope, Lufthansa Technik, Panasonic, Rockwell Collins, SatAuth, Teledyne Controls, Thales, UTAS (TBC), ZII, Zodiac Actuation Systems

2.3 Commitment for Drafting and Meeting Participation (as verified)

Airlines: Alaska Airlines, American Airlines, El Al Israel Airlines, FedEx, Lufthansa Airlines, United Airlines

Airframe Manufacturers: Airbus, Boeing,

Suppliers: Astronautics Corp. of America, Astronics (TBC), AstroNova (TBC), Esterline Avionics, GE Aviation, GoGo, Honeywell, Miltope, Lufthansa Technik, Panasonic, Rockwell Collins, SatAuth, Teledyne Controls, Thales, UTAS (TBC), ZII, Zodiac Actuation Systems

2.4 Recommended Coordination with other groups

Cabin Systems, EFB, KSAT, SAI, SDL

3.0 Project Scope (why and when standard is needed)

3.1 Description

Airlines require a secure method for operational client devices to connect and transmit encrypted data across onboard WLAN networks. A standard wireless network profile (based on network security best practices) for crew and operational connections to onboard WLAN networks is required to support consistency across airlines, IFE/IFC and airframe suppliers.

Passengers' personal devices are outside the scope of this activity.

WLAN networks may consist of shared-purpose inflight entertainment system networks operating in the PIES domain, dedicated aircraft cabin wireless networks or localized AID devices operating in the AIS domain.

Client devices requiring connections to these networks may consist of electronic flight bags, flight attendant mobile devices, onboard IoT devices, AID devices (acting as clients) and maintenance devices.

A defined wireless network profile standard adhering to security best practices would benefit both airlines and suppliers. This standard would also improve security postures of all operational onboard WLAN networks.

3.1.1 Planned usage of the envisioned specification

Note: New airplane programs must be confirmed by manufacturer prior to completing this section.

New aircraft developments planned to use this specification yes ☒ no ☐

Airbus: (aircraft & date TBD)

Boeing: (aircraft & date TBD)

Other: (manufacturer, aircraft & date)

Modification/retrofit requirement yes ☐ no ☒

Specify: (aircraft & date)

Needed for airframe manufacturer or airline project yes ☒ no ☐

Specify: United Airlines / In service Aug 2018

Mandate/regulatory requirement yes ☐ no ☒

Program and date: (program & date)

Is the activity defining/changing an infrastructure standard? yes ☐ no ☒

Specify (e.g., ARINC 429)

When is the ARINC standard required? April 2020

What is driving this date? United Airlines projects

Are 18 months (min) available for standardization work? yes ☒ no ☐

If NO please specify solution: _____

Are Patent(s) involved? yes ☐ no ☒

If YES please describe, identify patent holder: _____

3.2 Issues to be worked

The following areas will be developed and defined as part of an Onboard Secure Wi-Fi Network Profile Standard:

- Cockpit Crew, Cabin Crew, and Maintenance mobile device configuration
- IoT device configuration
- Onboard WLAN network configuration
- Assessment of new published WLAN standards (WPA3)
- Device and onboard infrastructure certificate/key management (CRL update, certificate management, filtering, etc.)
- Onboard authentication configuration and policies
- Certificate revocation management
- Wireless device removal/theft on aircraft per user group

- Network isolation and segmentation when on shared network (integration in an overall connectivity / security concept (as context information, not the focus of the standard)

Notes:

1. Several profiles and solutions may be identified for each use case
2. Some devices may connect to different WLANs and should avoid need for multiple certificates

4.0 Benefits

4.1 Basic benefits

Operational enhancements yes ☒ no ☐

For equipment standards:

(a) Is this a hardware characteristic? yes ☐ no ☒

(b) Is this a software characteristic? yes ☒ no ☐

(c) Interchangeable interface definition? yes ☒ no ☐

(d) Interchangeable function definition? yes ☒ no ☐

If not fully interchangeable, please explain: _____

Is this a software interface and protocol standard? yes ☒ no ☐

Specify: _____

Product offered by more than one supplier yes ☒ no ☐

Identify: Multiple

4.2 Specific project benefits (Describe overall project benefits.)

4.2.1 Benefits for Airlines

Airlines will benefit from a standard method for mobile crew devices to connect securely to onboard WLAN networks. Configuration across disparate IFE/IFC suppliers and/or airframe manufacturers will reduce complexity and assure adherence to security best practices for operational mobile device authentication and encryption within onboard WLAN networks.

4.2.2 Benefits for Airframe Manufacturers

Airframe manufacturers are able to design standardized equipment configuration applicable to multiple airlines.

4.2.3 Benefits for Avionics Equipment Suppliers

Avionics suppliers are able to design standardized equipment configurations applicable to multiple airlines.

5.0 Documents to be Produced and Date of Expected Result

ARINC Project Paper xxx to be prepared per the table in the following section.

5.1 Meetings and Expected Document Completion

The following table identifies the number of meetings and proposed meeting days needed to produce the documents described above.

Activity	Mtgs	Mtg-Days (Total)	Expected Start Date	Expected Completion Date
ARINC Project Paper xxx	3-4	3-4	Oct 2018	Apr 2020

Web conferences will be held.

6.0 Comments

(none)

6.1 Expiration Date for the APIM

October 2020

Completed forms should be submitted to the AEEC Executive Secretary and Program Director, Paul J. Prisaznuk (pjp@sae-itc.org)