Technical Standard Order (TSO)
Cybersecurity – Aircraft Systems Information Security Protection (ASISP)

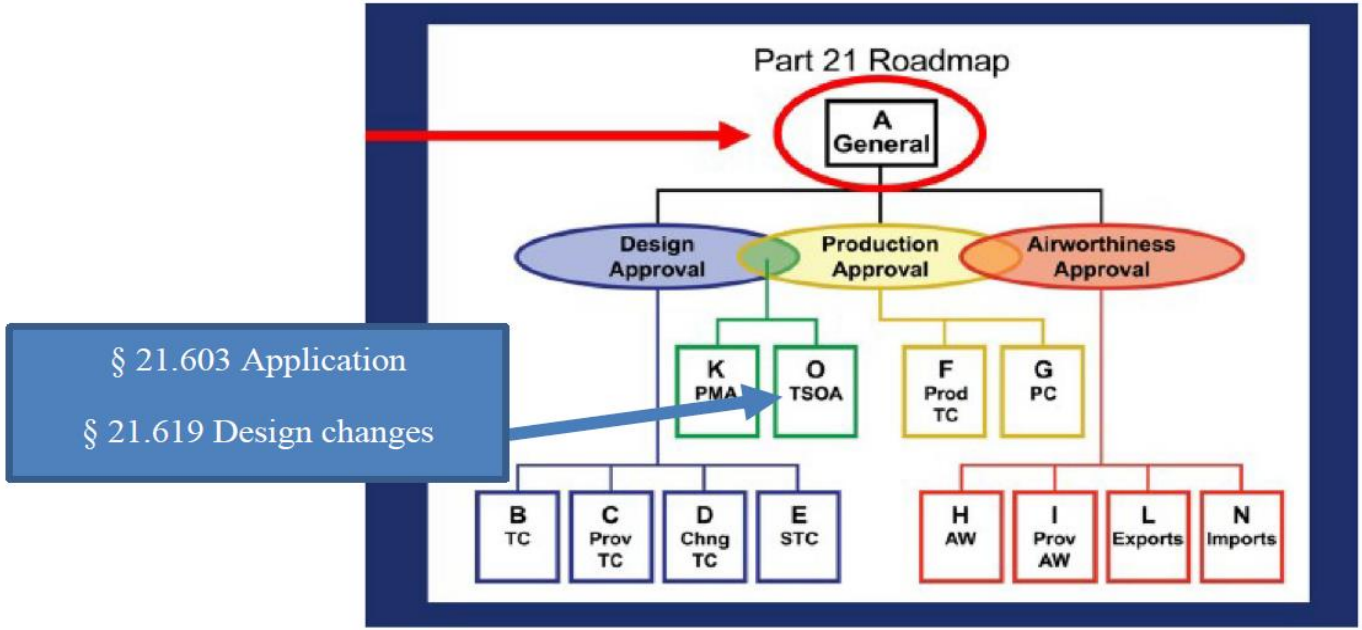
Presented to: TSO Workshop

By: Vonnie Tong, AIR-628 – Cybersecurity

Date: September 21, 2023

Federal Aviation Administration

Regulatory View for TSO Program



Current TSO Certification Program

- Recent aircraft systems design introduced electronic connectivity (e-connectivity) to “non-trusted services" and aircraft data network/avionics data buses

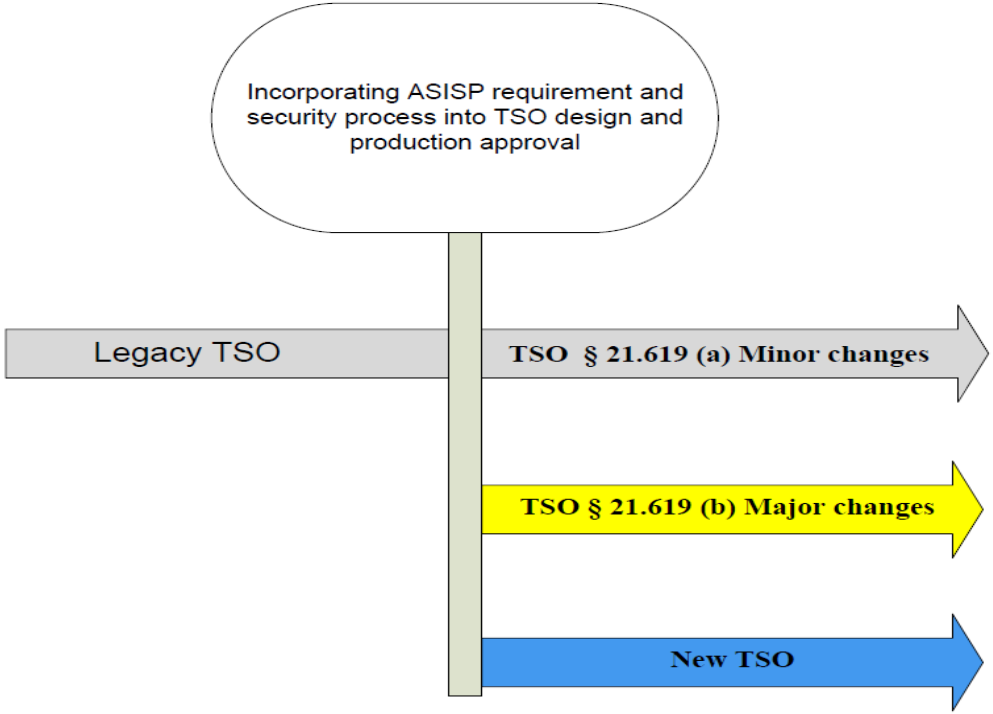
- “Connected” equipment when integrated/installed into the aircraft system, can introduce cybersecurity vulnerabilities beyond the scope of current regulation and advisory guidance. The FAA applies Special Condition and/or Means of Compliance to systems as required for safe operation

- The current regulatory basis for §§ XX.1301 and XX.1309 is applied for TSO certification program airworthiness requirements with connectivity feature (where XX = 23, 25, 27, 29)

- Unless the design change can be shown by either a change impact analysis or by a safety security summary risk assessment that an adverse cybersecurity event could not cause a failure condition effect of major, hazardous, or catastrophic, either directly or through propagation of security threats to/from any aircraft system

- Leverage existing AC 21-50, *Installation of TSOA Articles and LODA Appliances*
  - PSecAC and PSecAC Summary is required for TSOA approval for showing compliance to airworthiness requirements

Applicable ASISP Regulation



ASISP Applied to Legacy TSOs

- If minor changes are **not affecting** the ***Interface component*** - *ref.* § 21.1(b)(5) Applicability and definitions, then change impact analysis (CIA) for cybersecurity is not required

- If minor changes are **affecting** the ***Interface component***, then CIA for cybersecurity may be required as a deliverable compliance item for TSO approval

ASISP With Major Design Change

- Any TSO with major change(s) that impact the ***Interface component*** via e-connectivity or new method for interface connectivity will require CIA for security risk assessment

- If the existing TSO approval has a baseline security risk assessment and modifying connectivity interface, the security risk should be reassessed as part of the CIA

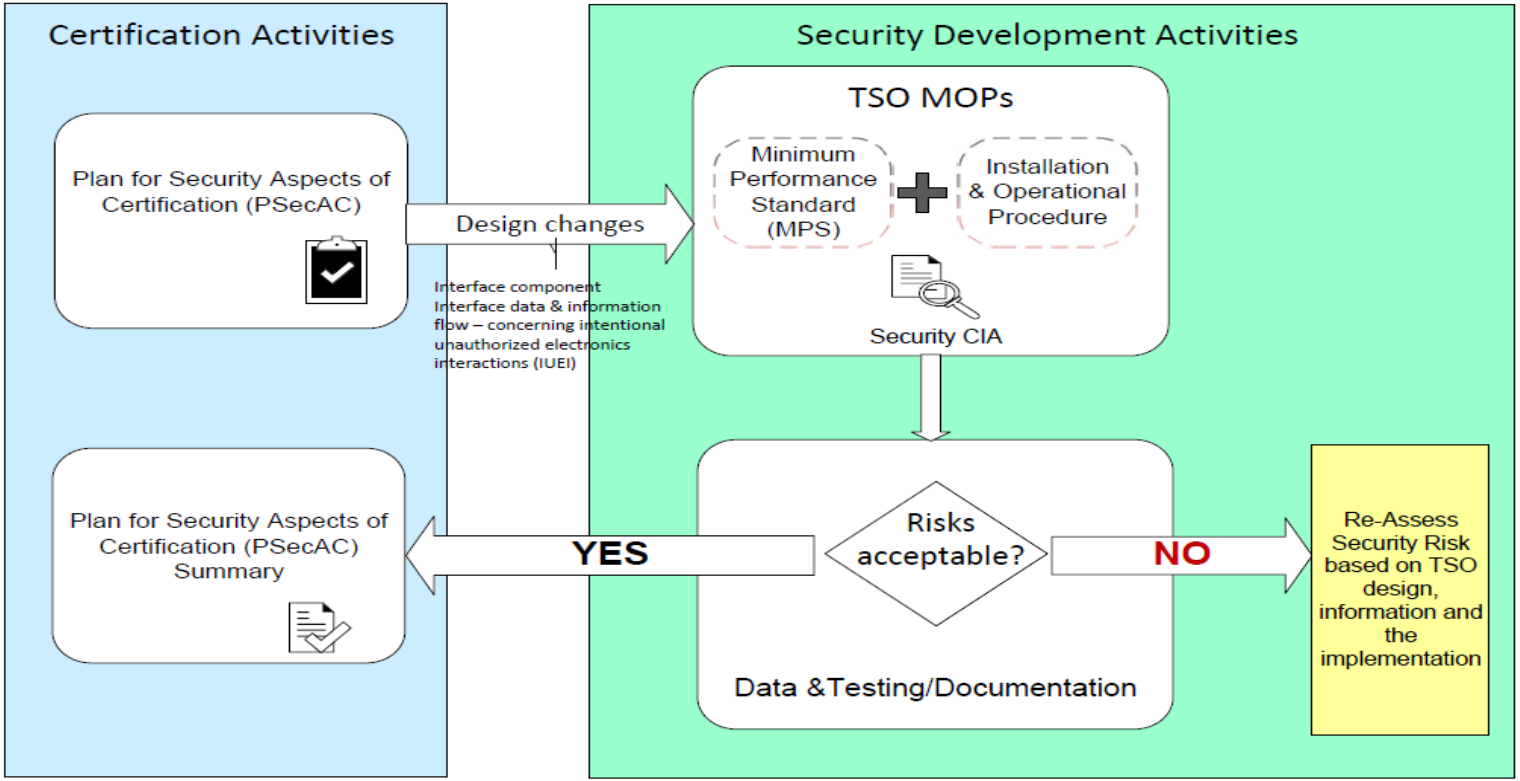
ASISP Applied to New TSOs

- Any new TSO specifies the minimum performance standard (MPS) for cybersecurity requirements and applicable industry standards compliance is required for TSO approval

- Any new TSO proposed to use a different means of compliance for cybersecurity requirements and/or industrial standards other than that indicated in the MPS will require a TSO deviation request

Change Impact Analysis (CIA)

- Applicant to use PS-AIR-21.16-02 Rev 2 as the basis for the establishment of special conditions (SC) for ASISP
- ASISP issue papers use industry standard for guidance as one of the recognizable means
- TSO projects only require ASISP issue paper if establishing new connectivity to access to previously isolated aircraft systems
- Applicants follow the industry standard and perform the security risk assessments for TSO (item level) with the new connectivity/interface and identify the impact(s) in the TSO certification plan (PSCP)
- The security risk assessments/analysis to include airworthiness security considerations for safety-security impacts
- The system safety assessment (SSA) outcome determines the need for ASISP issue paper(s) and the level of involvement from certification



ASISP for TSO Certification Program

Examples for CIA

Considerations of ASISP potential impact:

- ✓ The aircraft domain that equipment (TSO) to-be-installed resides in
- ✓ The intended function and the connectivity for interface data and data flow, including data buses, aircraft network on-board and off-board
- ✓ Electrical and RF interfaces between the equipment and the remainder of the aircraft (Internal)
- ✓ Electrical and RF interfaces between the equipment and non-governmental/governmental systems outside the Aircraft
- ✓ Phases of development, installation, operations, and maintenance that the equipment interfaces are used
- ✓ Digital data exchanged and its directions, the validity of source and destination (i.e. bi-directional, read/write)

Current FAA Delegations for ASISP

- FAA Order 8150.1D, *Technical Standard Order Program*, covers procedures for issuing TSOAs
  - DERs may not make findings of compliance to support an applicant's statement of conformance

- Technical Data approval in support of § 21.8
  - The DER / Consultant must obtain special authority to recommend/approve any data associated with compliance findings or recommend/approval of articles in accordance with § 21.8(d)
  - These recommendations/approvals, including witnessing penetration tests, are required to be coordinated and require approval with FAA assigned advisor

Delegated and Authorized Areas

Functions and areas that *can* be authorized are defined by ***white squares.*** Each DER's authority may be different and is identified in their letter of appointment.

	AUTHORIZED AREAS	Electrical Equipment/Systems	Electronic Equipment/Systems	Communications Systems/Antennas	Automatic Flight Controls/Augmentation	Instruments	Navigation Systems/Antennas	Air Data/Pitot Static	Warning Systems	Interior/Exterior Lighting	Flight Data/Voice Recording	Passenger Address/Entertainment	Special (Specify)
	DELEGATED FUNCTIONS	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
1	DETAIL DESIGN AND INSTALLATION												
2	EQUIPMENT QUALIFICATION TESTS												
3	SOFTWARE												
4	SERVICE DOCUMENTS												
5	ELECTRICAL LOAD ANALYSIS												
6	SAFETY ANALYSIS												
7	LIGHTNING/HIRF PROTECTION												
8	Aircraft System Information Security Protection (ASISP)												

Penetration Testing

Questions & Contact Info

- Questions?
- Contact Info: AIR-628, Cybersecurity
  - Email: vonnie.v.tong@faa.gov
  - Phone: 562-627-5333

Thank you!

Backup Slides

Cybersecurity Industry standards for TSO

- **RTCA Guidance Documents: (guidance mainly for part 25, 29, 33, 35)**
  1. DO-326A / ED-202A - Airworthiness Security Process Specification
  2. DO-356A / ED-203A - Airworthiness Security Methods and Considerations
  3. DO-355A / ED-204A - Information Security Guidance for Continuing Airworthiness
- **ASTM Guidance Documents: (guidance mainly for part 23, 27)**

  F3532 – 22 - Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions

- **SAE Guidance Documents:** TBD published date for SAW JA7496 & AIR7368

Definition terminology of part 21 (1/2)

§ 21.1 (b)Applicability and definitions.

- (1) *Airworthiness approval* means a document, issued by the FAA for an aircraft, aircraft engine, propeller, or article, which certifies that the aircraft, aircraft engine, propeller, or article conforms to its approved design and is in a condition for safe operation, unless otherwise specified;
- (2) *Article* means a material, part, component, process, or appliance;
- (3) *Commercial part* means an article that is listed on an FAA-approved Commercial Parts List included in a design approval holder's Instructions for Continued Airworthiness required by § 21.50;
- (4) *Design approval* means a type certificate (including amended and supplemental type certificates) or the approved design under a PMA, TSO authorization, letter of TSO design approval, or other approved design;
- (5) *Interface component* means an article that serves as a functional interface between an aircraft and an aircraft engine, an aircraft engine and a propeller, or an aircraft and a propeller. An interface component is designated by the holder of the type certificate or the supplemental type certificate who controls the approved design data for that article;
- (6) *Product* means an aircraft, aircraft engine, or propeller;
- (7) *Production approval* means a document issued by the FAA to a person that allows the production of a product or article in accordance with its approved design and approved quality system, and can take the form of a production certificate, a PMA, or a TSO authorization;
- (8) *State of Design* means the country or jurisdiction having regulatory authority over the organization responsible for the design and continued airworthiness of a civil aeronautical product or article;
- (9) *State of Manufacture* means the country or jurisdiction having regulatory authority over the organization responsible for the production and airworthiness of a civil aeronautical product or article.
- (10) *Supplier* means a person at any tier in the supply chain who provides a product, article, or service that is used or consumed in the design or manufacture of, or installed on, a product or article.

Definition terminology of part 21 (2/2)

Sec. 21.601(b) - [Applicability and definitions.]

- (1) A TSO issued by the FAA is a minimum performance standard for specified articles used on civil aircraft;
- (2) A TSO authorization is an FAA design and production approval issued to the manufacturer of an article that has been found to meet a specific TSO;
- (3) A letter of TSO design approval is an FAA design approval for an article that has been found to meet a specific TSO in accordance with the procedures of Sec. 21.621;
- (4) An article manufactured under a TSO authorization, an FAA letter of acceptance as described in Sec. 21.613(b), or an article manufactured under a letter of TSO design approval described in Sec. 21.621 is an approved article for the purpose of meeting the regulations of this chapter that require the article to be approved; and
- (5) An article manufacturer is the person who controls the design and quality of the article produced (or to be produced, in the case of an application), including any related parts, processes, or services procured from an outside source.

Definition terminology

- IUEI == “The protection of the airworthiness of an aircraft from *intentional unauthorized electronic interaction*: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems.” **RTCA DO-326A**