

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
1.	Air Force	Page 2, first bullet	<p>Replace the first bullet on page 2 under examples of non-governmental services and equipment with:</p> <p>Airline Networks through "broadcast" Airline Operations Center communications (e.g., Aircraft Communications Addressing and Reporting System (ACARS), wireless local area networks (WLAN), satellite communications (SATCOM), Communications Data Link (CDL), Automatic Dependent Surveillance Broadcast (ADS-B), Communication, Navigation, Surveillance / Air Traffic Management (CNS/ATM), and Global Positioning System (GPS))</p>			<p>Not applicable.</p> <p>The suggested change includes government services and equipment and examples already cited.</p>
2.	Air Force	Page 2, fourth bullet	<p>Replace fourth bullet with:</p> <p>Portable Electronic Devices (PEDs), Tactical Flight Bags (TFBs) or Electronic Flight Bags (EFBs) with wired or wireless connectivity</p>			Accepted
3.	Airbus	Page 1 - Section	The terminology "amended TC" should be clarified.		Add a note to clarify the meaning of the	Not applicable

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
		“Policy”- 2 nd paragraph – 1 st sentence	Upon a prior Airbus request for clarification on FAA terminology (see letter ref. M13008079 dated 2 April 2013), FAA (AIR 100) had clarified the definition of “an amendment to the TC” as a “major change in the Type Design”. As such, a minor change does not constitute an amendment to TC but it constitutes a change to the TC.		term “amended TC” in the first sentence of the 2 nd paragraph as follows : <i>“Note : amended TC corresponds to a major change in Type design as defined in 14 CFR 21.93.”</i>	This policy statement does not provide guidance on a major or minor change in the type design.
4.	Airbus	Page 1 - Section “Policy”- 2 nd paragraph – 1 st sentence	The policy should clarify that, in accordance with 14 CFR 21.93, security is not a criteria for classifying a change in Type design as a major change (or amended TC). In the same way, security is not a criteria for classifying a change as Level 1 when FAA is a Validation Authority (VA). In other words, only applications submitted to FAA based on existing classification criteria (as per 14 CFR 21.93, or based on existing Validation Items applicable to the aircraft model) might be subject to a Special Condition for Cyber Security. De facto, minor changes will be excluded.		Add a note to clarify the classification criteria about “amended TC” in the first sentence of the 2 nd paragraph as follows : <i>“Note : This policy does not change the criteria of classification of changes in type design as defined in 14 CFR 21.93 and it does not change the involvement of FAA as</i>	Not applicable This policy statement does not provide guidance on a major or minor change in the type design.

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			Note : harmonization between the Certificating (or Primary) Authority and FAA, as Validation Authority, could be necessary, notably to make the compliance determination when applicable.		<u>Validation Authority in validations.</u>	
5.	Airbus	Page 1 - Section "Policy"- 2 nd paragraph – 1 st sentence	<p>About <i>"to an aircraft system with a failure condition classification of "major" or higher."</i></p> <p>The classification of "major" is considered as too stringent. Generally, a Special Condition is raised when there is a risk of "unsafe condition" which corresponds to a failure condition classification of "Hazardous" or "Catastrophic."</p> <p>On the other side, acceptability of a security risk is not limited to the safety effects, indeed, threat likelihood should be considered as well. Security risk acceptability matrix (already accepted by FAA in the frame of already existing FAA security special conditions) show that a security risk is unacceptable only for Cat and Haz safety effects as long as the threat likelihood is not classified as</p>		<p>Change the 1st sentence of the 2nd paragraph as follows :</p> <p><i>"The Federal Aviation Administration (FAA) will issue special conditions for initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications involving any product whose system architecture allows connectivity to non-governmental services and equipment to have read-write</i></p>	<p>Not applicable</p> <p>The FAA believes this guidance should include a major failure condition classification. See definition below.</p> <p>Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the</p>

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			“very unlikely” or “unlikely”.		<i>connectivity to an aircraft system with a failure condition classification of “<u>hazardous</u>” or higher.”</i>	extent that there would be a significant reduction in safety margins or functional capabilities. In addition, the failure condition has a significant increase in crew workload or in conditions impairing crew efficiency; or a discomfort to the flight crew or physical distress to passengers or cabin crew, possibly including injuries.
6.	Airbus	Page 1 - Section “Policy”-	About : “The FAA will use the issue paper processes in Order 8110.112 to establish acceptable means of		Policy should refer international standards describing the	Not applicable This policy

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
		2 nd paragraph – 2 nd sentence	compliance.” Airbus highlights that acceptable means of compliance should be harmonized as much as possible between applicants, and more particularly between the TC holder and the STC applicants. Indeed, without OEM (or TC holder) data package and/or without the same security risk acceptability matrix, a STC applicant can invalidate the demonstration done by the TC holder, and even degrade the global aircraft security level with possible significant adverse safety effects.		airworthiness security process such as Eurocae ED-202A / RTCA DO-326A, otherwise similar FAA Advisory Circular if any.	statement is only intended to provide guidance when special conditions should be applied.
7.	Airbus	Page 2 - Section “Policy”- 3 rd paragraph	About the sentence : <i>“The Aircraft Certifications Offices can recommend to the applicant to submit preliminary information to determine special conditions will not be issued.”</i> The policy should clarify that, in accordance with Order 8110.112 §§ 2-2 –c (1), Special Condition is not used to upgrade the applicable airworthiness standards when novel or unusual design features are not involved. Thus, a Special Condition for Cyber Security should not be raised for a		Add a note as follows : <i>“Special Conditions will not be issued for systems already certified on similar aircraft (eg. derivatives) and/or for similar architecture and intended functions.”</i>	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<p>system, already certified on an aircraft model and to be installed on a derivative. If necessary, a reversion dossier could be submitted.</p> <p>In the same way, similarity in terms of intended functions and architecture, can justify that the design features are not novel or unusual and therefore, and that the Special Conditions for cyber security is not relevant.</p>			
8.	Airbus	Page 2 - Section "Policy"- 4th paragraph ("examples of non-governmental services and equipment"	<p>Only, the following non-governmental services and equipment should be considered :</p> <ul style="list-style-type: none"> • wireless communications using IP protocol • wired connections with PED/COTS <p>Indeed, specific private aeronautical protocols make the security threat much more unlikely.</p> <p>For instance, ACARS has been used over 3 decades on an Airbus fleet which reaches now 7400 aircraft in operation. No unsafe condition has been reported so far due to a security issue with ACARS. ACARS cannot be considered as a novel</p>		<p>Remove the following example from the list : <i>"Airline Networks including Airline Operations Center communications (e.g., Aircraft Communication Addressing and Reporting Systems (ACARS))"</i></p> <p>Modify the following example from the list as follows :</p>	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<p>or unusual design feature as per Order 8110.112 §§ 2-2 –c (1).</p> <p>In addition, the airframer alone cannot fully protect the ACARS communications because it cannot control the originator and the ACARS means of communication. A full ACARS protection would require that the transmission be encrypted by the service provider. Only a new regulation could enforce it.</p> <p>Note : security of ACARS communication shall be addressed from an end-to-end perspective in SESAR and NextGen programmes.</p>		<p><i>“Satellite Communications (<u>IP transmissions for passengers</u>)”</i></p>	
9.	Boeing	Page: 1 Section: Policy (2nd paragraph)	<p>The proposed text states: “The Federal Aviation Administration (FAA) will issue special conditions for initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications involving any product whose system architecture allows connectivity to non-governmental services and equipment to have read-write connectivity to an aircraft system with a failure condition classification of ‘major’</p>	<p>The proposed policy statement needs to reflect the current precedence of certifying LRUs with network connections that cross domain boundaries under Special</p>	<p>Boeing suggests that the text be revised to state that Special Conditions apply to Line Replaceable Units (LRU) with network connections that cross domain boundaries. Non-networked LRUs could be addressed</p>	<p>Not applicable</p> <p>This policy statement should only be applied to aircraft systems with a failure effect classification of “major” or higher that</p>

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<p>or higher. ...”</p> <p>Boeing suggests that the text be revised to state that Special Conditions apply to Line Replaceable Units (LRU) with network connections that cross domain boundaries. Non-networked LRUs could be addressed under existing regulations, such as 14 CFR §25.1309, without Special Conditions. Our suggestion is consistent with existing precedent.</p>	<p>Conditions, and non-networked LRU’s under existing regulations, such as §25.1309. This policy should continue until rulemaking is completed to address “Cyber Security” for networked LRUs.</p>	<p>under existing regulations, such as 14 CFR §25.1309, without Special Conditions. Our suggestion is consistent with existing precedent.</p> <p>We request that this Policy Statement take into consideration the means of compliance and applications from previous Special Conditions issued on “Cyber Security.”</p> <p>We recommend that, for the longer term, the FAA form or assign an Aviation Rulemaking Advisory Committee (ARAC) to provide industry input into updating §25.1309 and</p>	<p>directly connects and receives information from non-governmental services regardless of the aircraft system connectivity across domain boundaries.</p> <p>Policy statements that provide guidance when special conditions should be applied have never been published.</p> <p>The FAA Standards Management Team (SMT) has decided to</p>

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
					associated advisory material to include “Cyber Security” as a hazard.	maintain the status of quo of publishing special conditions to address cyber security vulnerabilities.
10.	Boeing	Page: 2 Section: Policy (2nd paragraph, bulleted list)	The proposed text states: “The following are examples of non-governmental services and equipment: <ul style="list-style-type: none"> • Airline Networks including Airline Operations Center communications (e.g., Aircraft Communication Addressing and Reporting Systems (ACARS)) • Airport Gate Link Networks (e.g. Gatelink) • Public Networks (e.g. Internet) • Portable Electronic Devices (PEDs) or Electronic Flight Bags (EFBs) with wired or wireless connectivity • Wireless Aircraft Sensors and Sensor Networks • Wireless Ground Support Equipment (GSE) 	Special Conditions are deemed necessary because of “novel and unusual” features for which existing regulations are not considered adequate. Existing regulations adequately address ACARS, legacy satellite communications, and other systems.	Boeing suggests that the FAA reconsider the list of services and equipment, given that some are legacy systems (e.g., ACARS, Satellite Communications, etc.) and there may be others in a similar situation. Special Conditions focus on “novel and unusual” features (ref. 14 CFR §21.16) where current regulations do not provide adequate	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<ul style="list-style-type: none"> • Universal Serial Bus (USB) devices • Maintenance lap tops • Satellite Communications • Cellular Networks” 		coverage. Since this is not the case for these legacy systems, they should be removed from the list of equipment/services specifically called out in the policy.	
11.	Cessna		Cessna is pleased to see the FAA address this topic and provide a threshold for when Special Conditions apply to a project.		None	
12.	Cessna	Page 1, paragraph 4	Rationale of this text change: BASED on the recent text drafted for RTCA/SC-216, Aeronautical Systems Security, DO-326A, FRAC.		Cessna recommends that the text “...read-write connectivity to an aircraft system with a failure condition classification of “major” or higher.” be drafted as “...read-write connectivity to an aircraft system with an aircraft security Impact of “major” or higher.”	Not applicable This policy statement only provides guidance when special conditions should be applied. The modifications recommended are referenced from the draft RTCA SC-216

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
						documents.
13.	Garmin	General	The review period of 30 days for this policy statement is not consistent with FAA Order 8100.16 paragraph 2-6 on Required Coordination for policy statements.	FAA Order 8100.16 paragraph 2-6 policy on policy statements states: “The standard period for public comment is 60 calendar days, unless otherwise required.”	Extend the public comment period to 60 days.	Accepted The public comment period has been extended to 60 days.
14.	Garmin	General	The policy as written, forces all equipment that is field-loadable to be scrutinized for cyber-security.	Because this policy forces a Special Condition to be written and reviewed up the line; no project can be less than 40 Hours of FAA involvement. This policy will force even the smallest project into “Sequencing”.	Redraft the policy to narrow its scope to address only particular areas of concern.	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				The FAA needs to better evaluate how they want to spend their limited resources.		
15.	Garmin	Pg 1, Policy, Pa 1	<p>The Policy states, “Current regulations may not be adequate for products ...”</p> <p>By starting at the “product”, this language has been written to force the use of a Special Condition where just a Means Of Compliance Issue Paper may suffice.</p>	<p>xx.1301 and xx.1309 are very broad-based rules designed to cover various unforeseen technologies.</p> <p>xx.1301 and xx.1309 are sufficient rules; it is only the Means Of Compliance to meet these rules that are in question.</p> <p>If these rules are not sufficient, then is there an NPRM activity started to address the deficiency?</p>	<p>Consider re-stating as follows:</p> <p>Systems architectures are being proposed that allow interface between aircraft systems and wired or wireless electronic influences that can potentially affect safety of the aircraft.</p>	<p>Accepted</p> <p>The FAA Standards Management Team (SMT) has decided to maintain the status of quo of publishing special conditions to address cyber security vulnerabilities.</p>

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
16.	Garmin	Pg 1, Policy, Pa 2	<p>The Policy states, “The Federal Aviation Administration (FAA) will issue special conditions...”</p> <p>Per 21.16, a Special Condition is used for a new or novel design feature for the product; cyber-security is only trying to better control user access to existing systems.</p> <p>Rather than a Special Condition, it seems, per FAA Order 8110.112, that a “Means Of Compliance” Issue Paper should suffice.</p>	<p>A Special Condition is onerous for the FAA and the applicant. It requires public review in the Federal Register (time consuming) and therefore forces a more generic (less applicant-specific) Issue Paper. It also may force the applicant to respond to several items that may not be applicable, again wasting time and effort.</p> <p>Also, by using the Means Of Compliance Issue Paper, each ACO and Directorate is</p>	<p>Change the wording to read, “The Federal Aviation Administration (FAA)” may use an Issue Paper to establish appropriate Means of Compliance...</p>	<p>Not applicable</p> <p>The FAA Standards Management Team (SMT) has decided to maintain the status quo of publishing special conditions to address cyber security vulnerabilities.</p>

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				allowed more flexibility to apply guidance based on the type of appliance and category of product.		
17.	Garmin	Pg 1, Policy, Pa 2	The Policy states, ‘...allows connectivity to non-governmental services and equipment to have read-write connectivity to an aircraft system with a failure condition classification of “major” or higher.’ As written, this statement captures long-established items such as database updates and field loadable software.	Database updates were the subject of a recent revision to 14 CFR Part 43 to add 43.3(k). This update was specifically intended to make the database update process easier. The proposed policy runs counter to the intent of that update. Additionally, procedures for database updates and field loadable	Update the policy to exclude long-established items such as database updates and field loadable software.	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				software are already subject to equipment manufacturer's specifications and operator guidance.		
18.	Garmin	Pg 1, Policy, Pa 2	The Policy states, '...allows connectivity to non-governmental services and equipment to have read-write connectivity to an aircraft system with a failure condition classification of "major" or higher.'	Mandating a special condition for all systems with a given failure classification is painting with a broad brush. This will likely impose an undue burden on many aircraft TC projects, especially Part 23 and 27 aircraft, as well as many STC projects. There are far more STC projects than there are TC projects, and the FAA may not have the	The material being prepared by RTCA SC-216 includes guidance on both TCs and STCs. Await the publication of that material.	Not applicable The RTCA SC-216 documents do not provide guidance when special conditions should be applied.

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				resources to handle issue papers and special conditions for each STC project		
19.	Garmin	Pg 1, Policy, Pa 2	The Policy states, ‘...allows connectivity to non-governmental services and equipment to have read-write connectivity to an aircraft system with a failure condition classification of “major” or higher.’	It is unclear whether the policy relates only to equipment that has a failure classification of “major” or higher’ AND whose system architecture allows read-write connectivity to non-governmental services and equipment, or whether the policy applies to any system where the read-write connectivity to non-governmental services itself is	Rephrase the statement to make clear the scope of the policy.	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				deemed to have a failure classification of “major” or higher.’		
20.	Garmin	Pg 2, Policy, Pa 1	The Policy states, “The Aircraft Certification Offices can recommend to the application to submit preliminary information to determine special conditions will not be issued.” However, no discussion of the type of information or recommended schedule is provided.	In a recent experience with the issue paper process, the standard security issue papers were presented verbatim with little to no tailoring by the ACO. Additionally, the issue papers were provided at the end of the certification process, long past any reasonable timeframe to change design decisions or execute additional	Add recommendations on the timing of the exchange of data between the applicant and the ACO. Add recommendations on the type of data that the ACO should request. Note that the precise nature of this information is currently being debated in RTCA SC-216; consequently, the ability to precisely define this information seems pre-mature with respect to levying this policy in such a broad manner. Add recommendations on when issue papers	Not applicable The policy statement only provides guidance when special conditions should be applied. The last recommendation is addressed in the policy statement.

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				testing.	should be levied on the applicant.	
21.	Garmin	Pg 2, Policy, Pa 1	The Policy states, “The Aircraft Certification Offices can recommend to the application to submit preliminary information to determine special conditions will not be issued.”	The wording of this statement is awkward.	Rephrase to, “The Aircraft Certification Offices should recommend that applicants submit preliminary information to assist with determining the need for a special condition.”	Non-applicable Section has been removed.
22.	Garmin	Pg 2, Policy, Bullet list item 1	The Policy lists, “Airline Networks including Airline Operations Center communications (e.g., Aircraft Communication Addressing and Reporting System (ACARS))” as a system that would drive a special condition. ACARS systems accessing safety services as defined in ARINC 623 may have failure classifications of “major” on some aircraft. These systems have decades of operational history, as well as interoperability requirements with ground systems that will likely preclude the imposition of additional security requirements through the aircraft-level	ACARS systems have been used in airline and non-airline environments for decades and have many interoperability requirements. Unless an explicit issue has been identified, an extra regulatory burden will not increase safety.	Remove ACARS systems from the list.	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			TC/STC process. Additionally, the same system			
23.	Garmin	Pg 2, Policy, Bullet list item 4	The Policy lists, “Portable Electronic Devices (PEDs) or Electronic Flight Bags (EFBs) with wired or wireless connectivity” as a system that would drive a special condition.	A separate Advisory Circular (AC 120-76B) discusses the integration of electronic flight bags. This AC has a substantial amount of detail, including requirements for interfacing with aircraft systems. The AC also contains a discussion of when security should be considered. This AC has been in use for years and is accepted by both the FAA and industry	Remove EFBs from the list, and note that EFBs are already covered by their own Advisory Circular.	Not applicable AC 120-76B does not provide guidance about mitigating cyber security exploits from threat sources with malicious intent.
24.	Garmin	Pg 2, Policy,	The Policy lists, “Wireless Ground	The two items	Remove “Maintenance	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
		Bullet list items 6 and 8	Support Equipment (GSE)” and “Maintenance lap tops” as systems that would drive a special condition.	should be combined in to one item.	lap tops” from the list. Rephrase “Wireless Ground Support Equipment” to “Wired or wireless Ground Support	
25.	Garmin	Pg 2, Policy, Bullet list item 9	The Policy lists, “Satellite Communications” as a system that would drive a special condition. Commonly used satellite communications systems such as Inmarsat and Iridium have failure classifications of Minor as defined in TSO-C132 item 3.b and TSO-C159a item 3.b	Since the TSOs already define the failure classification for some types of satcom systems as Minor, and this policy states that only Major or higher systems will be considered, including all satcom systems is inappropriate.	Add language specifically stating that some satcom systems covered by TSOs are defined as minor and are outside the scope of this policy.	Accepted
26.	Garmin	Pg 2, Effect of Policy, Pa 1	The Effect of Policy states, “Whenever a proposed method of compliance is outside of this established policy, that individual has to coordinate it with the responsible certification office.” The phrase “has to” is inconsistent with other described actions.	The phrase “has to” does not follow established terminology.	Change “has to” to “must”	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
27.	Garmin	Pg 2, Effect of Policy, Pa 1	<p>The Policy states, “The responsible certification office must notify the policy-issuing office of an approved method of compliance outside of this established policy.”</p> <p>There is no approved method of compliance provided; there is no guidance provided for a method of compliance that might be approvable.</p> <p>This will result in a built-in bottleneck for certification projects, since all projects must be reviewed by Washington D.C</p>	<p>This policy is counter-productive.</p> <p>Since there is no approved method of compliance provided, this forces all methods of compliance to be sent to Washington D.C. for evaluation, which will result in a built-in bottleneck for certification projects.</p>	<p>Guidance for acceptable means of compliance need to be added. If this cannot be done, then FAA ACOs must be trained to be able to provide clear acceptable “means”, without having to go to Washington D.C.</p>	<p>Not applicable</p> <p>The policy statement only provides guidance when special conditions should be applied.</p> <p>Training will accompany the policy statement.</p>
28.	Garmin	Pg 2, Effect of Policy, Pa 4	<p>The Effect of Policy states, “...this statement of policy identifies one means, but not the only means, of demonstrating compliance.” No means of compliance are identified in the body of this policy.</p>	<p>The policy generally states that a special condition should be issued by an ACO for aircraft with certain types of interconnected systems. It does</p>	<p>The FAA has drafted two generic security issue papers – one for internal security issues, and one for external security issues. Those generic draft issue papers should be updated</p>	<p>Not accepted</p> <p>The policy statement only provides guidance when special conditions should be</p>

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				not state what the content of that special condition is likely to be and does not assist either the applicant or the ACO with the content of the special condition. The applicant has no guidance as to what the ACO will request, nor when it will be requested.	(some of the content of the draft issue papers is several years out of date) and included as an appendix to this policy. These draft issue papers can then serve as “one means, but not the only means, of demonstrating compliance.”	applied.
29.	L3	Page 2	The sentence “The Aircraft Certifications Offices can recommend to the applicant to submit preliminary information to determine special conditions will not be issued.” is unclear.	Does the “will not be issued” indicate that the ACO will NOT recommend a submittal from the applicant or that the applicant’s submittal to determine special conditions will not	Perhaps the phrase “will not be issued” should be dropped.	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				cause a change in the white paper? Or is there another interpretation?		
30.	Rockwell Collins		Rockwell Collins fully supports the FAA's intention to provide consistent guidance to the Aircraft Certification Offices when special conditions should be applied to address cyber security vulnerabilities in aircraft certification programs. We agree that Special Conditions are needed as a temporary measure until additional standards, such as the work being conducted by RTCA SC-216 and EUROCAE WG-72, become available. We urge adoption of applicable cyber security guidelines and methods from these committee activities as they mature.		Such special conditions, guidelines and methods should not be applicable to new system designs or changes in the aircraft control domains that do not introduce new electronic access points or affect previously accepted means for cyber security protection.	Accepted
31.	Rockwell Collins	Page 2	The draft Policy Statement includes a list of examples of non-governmental services and equipment.		Rockwell Collins seeks clarification on what is the definition of "non-governmental services and equipment" and what constitutes "governmental	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
					services and equipment.” For example, does access to an approved FAA information source via a non-certified Portable Electronic Device constitute a governmental service?	
32.	Rockwell Collins		While this policy is meant to address special conditions for Type Certificates (TC), Supplemental Type Certificates (STC), and amended TC, opportunities exist for “non-governmental services and equipment” installed or used on the flight deck as uncertified aftermarket devices to interface to certified avionics.		Rockwell Collins urges the FAA to adopt corresponding policy for the aftermarket devices.	Accepted The FAA agrees with the suggested change but the intent of this policy statement is to only provide guidance when special conditions should be applied at this time. There are plans to adopt corresponding policy for the

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
						aftermarket devices.
33.	Rockwell Collins		While the Policy Memorandum addresses an integrated solution, technology, applications, and services are moving quickly to provide additional functionality for the flight deck, including providing information to the pilot without direct connection to aircraft systems.		We believe additional insight needs to be included outlining conditions of use, data retrieval, the writing of data to certified avionics, etc. to help guide both the policy and the execution of the policy by the field offices.	Accepted The FAA agrees with the suggested change but the intent of this policy statement is to only provide guidance when special conditions should be applied at this time. There are plans to provide additional guidance that will address the suggested change.
34.	GAMA	General	GAMA agrees that Special Conditions are needed in cases where novel data architectures are utilized or where critical software can be affected by publically		GAMA believes the FAA must determine when a special condition must apply	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			accessible interfaces. It is important to note that general aviation products are handled with completely different security standards than the scheduled commercial carriers and this difference in operations must be considered when setting appropriate design side requirements. It is unacceptable to introduce certification complexities and hurdles that will prevent simple designs from coming to market.		based upon design features that have not been historically considered (such as a common data backbone) but it would be inappropriate to force every applicant to prove there is no need for a special condition simply because they have external data inputs.	
35.	GAMA				Such special conditions, guidelines and methods should not be applicable to new system designs or changes in the aircraft control domains that do not introduce new electronic access points nor should it apply to previously accepted means for cyber security	Accepted Rockwell Collins submitted a similar comment (see #30).

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
					protection.	
36.	GAMA		Further, as written, this policy forces all equipment that is field-loadable to be scrutinized for cyber-security. Because this policy forces a Special Condition to be written and reviewed up the line; no project can be less than 40 Hours of FAA involvement. Therefore as written, this policy will also impose unnecessary additional burdens on FAA resources by forcing even the smallest project into "Sequencing".		GAMA requests the FAA redraft the policy's scope so it focuses on the appropriate areas of concern as described above.	Accepted Garmin submitted a similar comment (see #14).
37.	GAMA	Page 1, paragraph 1	The Policy states, "Current regulations may not be adequate for products ..." By starting at the "product" level, this language has been written to force the use of a Special Condition where as a Means of Compliance Issue Paper may suffice. XX.1301 and XX.1309 are very broad-based rules designed to cover various unforeseen technologies. XX.1301 and XX.1309 are sufficient rules; it is only the Means of Compliance to meet these rules that are in question.	GAMA questions that if these rules are not sufficient, then is there an NPRM activity started to address the deficiency?	Therefore, GAMA respectfully requests the FAA consider re-stating such as to state "New and novel systems architectures are being proposed that allow interface between aircraft systems and wired or wireless electronic influences that can potentially affect safety of the aircraft."	Accepted Garmin submitted a similar comment (see #15). The FAA Standards Management Team (SMT) has decided to maintain the status of quo of publishing special conditions to

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
						address cyber security vulnerabilities.
38.	GAMA	Page 1, paragraph 2	<p>The Policy states, “The Federal Aviation Administration (FAA) will issue special conditions...” . Per 21.16, a Special Condition is used for a new or novel design feature for the product; cyber-security is only trying to better control user access to existing systems. Rather than a Special Condition, it seems, per FAA Order 8110.112, that a “Means Of Compliance” Issue Paper should suffice.</p> <p>A Special Condition is onerous for the FAA and the applicant. It requires public review in the Federal Register (time consuming) and therefore forces a more generic (less applicant-specific) Issue Paper. It also may force the applicant to respond to several items that may not be applicable, again wasting time and effort.</p>	Also, by using the Means Of Compliance Issue Paper, each ACO and Directorate is allowed more flexibility to apply guidance based on the type of appliance and category of product.	GAMA requests the FAA change the wording to read, “The Federal Aviation Administration (FAA)” may use an Issue Paper to establish appropriate Means of Compliance...	Not applicable Garmin submitted a similar comment (see #16). The FAA Standards Management Team (SMT) has decided to maintain the status quo of publishing special conditions to address cyber security vulnerabilities.
39.	GAMA	Page 1,	The Policy states, ,,...allows connectivity		GAMA requests the	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
		paragraph 2	<p>to non-governmental services and equipment to have read-write connectivity to an aircraft system with a failure condition classification of “major” or higher.” As written, this may impose an undue burden on many aircraft TC projects, especially Part 23 and 27 aircraft, as well as many STC projects.</p> <p>This statement will also impact long-established items such as database updates and field loadable software. Database updates were the subject of a recent revision to 14 CFR Part 43 to add 43.3(k). This update was specifically intended to make the database update process easier and this proposed policy runs counter to the intent of that update. Additionally, procedures for database updates and field loadable software are already subject to equipment manufacturer’s specifications and operator guidance. Therefore, GAMA requests that the FAA update the policy to exclude long-established items such as database updates and field loadable software.</p>		FAA rephrase the statement to clarify the scope of the policy.	Garmin submitted similar comments (see #17, #18, and #19).

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			It is unclear whether the policy relates only to equipment that has a failure classification of „major” or higher” AND whose system architecture allows read-write connectivity to non-governmental services and equipment, or whether the policy applies to any system where the read-write connectivity to non-governmental services itself is deemed to			
40.	GAMA	Page 2, paragraph 2	The Policy states, “The Aircraft Certification Offices can recommend to the application to submit preliminary information to determine special conditions will not be issued.” However, no discussion of the type of information or recommended schedule is provided.			Accepted Garmin submitted a similar comment (see #20).
41.	GAMA	Page 2, paragraph 2	GAMA believes it is unacceptable to introduce certification complexities and hurdles that will prevent simple designs from coming to market. GAMA believes the FAA must determine when a special condition must apply based upon design features that have not been historically considered (such as a common data backbone) but it would be inappropriate to force every applicant to prove there is			Accepted The section has been removed.

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			no need for a special condition simply because they have external data inputs.			
42.	GAMA	Page 2, bulleted list	The draft Policy Statement includes a list of examples of non-governmental services and equipment. GAMA respectfully requests clarification on what is the definition of “non-governmental services and equipment” and what constitutes “governmental services and equipment.” For example, does access to an approved FAA information source via a non-certified Portable Electronic Device constitute a governmental service?			Accepted Rockwell Collins submitted a similar comment (see #31.)
43.	GAMA	Page 2, bullet 1	The Policy lists, “Airline Networks including Airline Operations Center communications (e.g., Aircraft Communication Addressing and Reporting System (ACARS))” as a system that would drive a special condition. ACARS systems accessing safety services as defined in ARINC 623 may have failure classifications of “major” on some aircraft. These systems have decades of operational history, as well as interoperability requirements with ground systems that will likely preclude the imposition of additional security		Therefore, GAMA requests the FAA remove the ACARS systems from the list.	Accepted

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			<p>requirements through the aircraft-level TC/STC process. Additionally, the same system generally handles both ATS and AOC communications.</p> <p>ACARS systems have been used in airline and non-airline environments for decades and have many interoperability requirements. Unless an explicit issue has been identified, an extra regulatory burden will not increase safety.</p>			
44.	GAMA	Page 2, bullet 4	The Policy lists, “Portable Electronic Devices (PEDs) or Electronic Flight Bags (EFBs) with wired or wireless connectivity” as a system that would drive a special condition.	A separate Advisory Circular (AC 120-76B) discusses the integration of electronic flight bags. This AC has a substantial amount of detail, including requirements for interfacing with aircraft systems. The AC also contains a discussion of	GAMA requests the FAA remove EFBs from the list, and note that EFBs are already covered by their own Advisory Circular.	Not applicable Garmin submitted a similar comment (see #23). AC 120-76B does not provide guidance about mitigating cyber security exploits from threat sources with malicious intent.

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
				when security should be considered. This AC has been in use for years and is accepted by both the FAA and industry.		
45.	GAMA	Page 2, bullet 6	The Policy lists, “Wireless Ground Support Equipment (GSE)” and “Maintenance lap tops” as systems that would drive a special condition.		GAMA believes the two items should be rephrased from “Wireless Ground Support Equipment” to “Wired or wireless Ground Support Equipment (GSE) including maintenance laptops”	Accepted Garmin submitted a similar comment (see #24).
46.	GAMA	Page 2, bullet 9	The Policy lists, “Satellite Communications” as a system that would drive a special condition. Commonly used satellite communications systems such as Inmarsat and Iridium have failure classifications of Minor as defined in TSO-C132 item 3.b and TSO-C159a item 3.b		Since the TSOs already define the failure classification for some types of satcom systems as Minor, and this policy states that only Major or higher systems will be considered,	Accepted Garmin submitted a similar comment (see #25).

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office: AIR-120	Document Description: Policy Statement: Establishment of Special Conditions for Cyber Security	Project Lead/Reviewer	Reviewing Office:	Date of Review:
---------------------------------------	--	------------------------------	--------------------------	------------------------

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
					including all satcom systems is inappropriate. GAMA requests the FAA add clarifying language that specifically states that some satcom systems covered by TSOs are defined as minor and are outside the scope of this policy.	
47.	GAMA	Page 2, Effect of Policy paragraph	The Policy states, "The responsible certification office must notify the policy-issuing office of an approved method of compliance outside of this established policy." Since there is no approved method of compliance provided, this forces all methods of compliance to be sent to Washington D.C. for evaluation, which will result in a built-in bottleneck for certification projects. Guidance for acceptable means of compliance should therefore be added. If this cannot be done, then FAA ACOs must be trained to be able to provide clear		Guidance for acceptable means of compliance should therefore be added. If this cannot be done, then FAA ACOs must be trained to be able to provide clear acceptable "means", without having to go to Washington D.C.	Not applicable Garmin submitted a similar comment (see #27). The policy statement only provides guidance when special conditions should be applied.

Public Comment Log
Policy Statement: Establishment of Special Conditions for Cyber Security

Originating Office:	Document Description:	Project Lead/Reviewer	Reviewing Office:	Date of Review:
AIR-120	Policy Statement: Establishment of Special Conditions for Cyber Security			

#	Commenter	Page & Para. No.	Comment	Reason for Comment	Suggested Change	Comment Resolution
			acceptable “means”, without having to go to Washington D.C.			
48.	GAMA	Page 2, Effect of Policy paragraph	The Effect of Policy states, “...this statement of policy identifies one means, but not the only means, of demonstrating compliance.” GAMA notes that no means of compliance are actually identified in the body of this policy but rather this policy generally states that a special condition should be issued by an ACO for aircraft with certain types of interconnected systems. It does not state what the content of that special condition is likely to be and does not assist either the applicant or the ACO with the content of the special condition. The applicant has no guidance as to what the ACO will request, nor when it will be requested.		The FAA has drafted two generic security issue papers – one for internal security issues, and one for external security issues. Those generic draft issue papers should be updated (some of the content of the draft issue papers is several years out of date) and included as an appendix to this policy. These draft issue papers can then serve as “one means, but not the only means, of demonstrating compliance.”	Not applicable Garmin submitted a similar comment (see #28). The policy statement only provides guidance when the special conditions should be applied.