This text is meant purely as a documentation tool and has no legal effect. The Union's institutions do not assume any liability for its contents. The authentic versions of the relevant acts, including their preambles, are those published in the Official Journal of the European Union and available in EUR-Lex. Those official texts are directly accessible through the links embedded in this document

►B

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1998

of 5 November 2015

laying down detailed measures for the implementation of the common basic standards on aviation security

(Text with EEA relevance)

(OJ L 299, 14.11.2015, p. 1)

Amended by:

		Official Journal		
		No	page	date
►M1	Commission Implementing Regulation (EU) 2015/2426 of 18 December 2015	L 334	5	22.12.2015
►M2	Commission Implementing Regulation (EU) 2017/815 of 12 May 2017	L 122	1	13.5.2017
►M3	Commission Implementing Regulation (EU) 2017/837 of 17 May 2017	L 125	3	18.5.2017
►M4	Commission Implementing Regulation (EU) 2018/55 of 9 January 2018	L 10	5	13.1.2018
►M5	Commission Implementing Regulation (EU) 2019/103 of 23 January 2019	L 21	13	24.1.2019
►M6	amended by Commission Implementing Regulation (EU) 2020/910 of 30 June 2020	L 208	43	1.7.2020
►M7	Commission Implementing Regulation (EU) 2019/413 of 14 March 2019	L 73	98	15.3.2019
►M8	Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019	L 246	15	26.9.2019
►M9	amended by Commission Implementing Regulation (EU) 2020/910 of 30 June 2020	L 208	43	1.7.2020
►M10	Commission Implementing Regulation (EU) 2020/111 of 13 January 2020	L 21	1	27.1.2020
►M11	Commission Implementing Regulation (EU) 2020/910 of 30 June 2020	L 208	43	1.7.2020
►M12	Commission Implementing Regulation (EU) 2021/255 of 18 February 2021	L 58	23	19.2.2021
►M13	Commission Implementing Regulation (EU) 2022/421 of 14 March 2022	L 87	1	15.3.2022
►M14	Commission Implementing Regulation (EU) 2022/463 of 22 March 2022	L 94	3	23.3.2022

►**M15**	Commission Implementing Regulation (EU) 2022/1174 of 7 July 2022	L 183	35	8.7.2022
►**M16**	Commission Implementing Regulation (EU) 2023/566 of 10 March 2023	L 74	47	13.3.2023

▼B

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1998

of 5 November 2015

laying down detailed measures for the implementation of the common basic standards on aviation security

(Text with EEA relevance)

Article 1

The detailed measures for the implementation of the common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation, referred to in Article 4(1) of Regulation (EC) No 300/2008, and the general measures supplementing those common basic standards, referred to in Article 4(2) of that Regulation, are set out in the Annex.

Article 2

Regulation (EU) No 185/2010 is repealed. References to the repealed Regulation shall be construed as a reference to this Regulation.

Article 3

This Regulation shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 1 February 2016.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

▼B

ANNEX

1. **AIRPORT SECURITY**

1.0 GENERAL PROVISIONS

1.0.1 Unless otherwise stated, the authority, airport operator, air carrier or entity responsible in accordance with the national civil aviation security programme referred to in Article 10 of Regulation (EC) No 300/2008 shall ensure the implementation of the measures set out in this Chapter.

1.0.2 For the purposes of this Chapter, an aircraft, bus, baggage cart or other means of transport, or a walkway or jetway, shall be regarded as a part of an airport.

For the purposes of this Chapter, 'secured baggage' means screened departing hold baggage that is physically protected so as to prevent the introduction of any objects.

▼M2

1.0.3 Without prejudice to the criteria for derogations as set out in Part K of the Annex to Commission Regulation (EC) No 272/2009 ([1]), the appropriate authority may allow special security procedures or exemptions for the protection and security of airside areas at airports on days on which there is not more than one aircraft to be loaded, unloaded, boarded or disembarked at any one time either within the critical part of the security restricted area or at an airport that falls outside of the scope of point 1.1.3.

▼B

1.0.4 For the purposes of this Annex 'items carried by persons other than passengers' refers to the belongings intended for the personal use of the person that carries them.

1.0.5 References to third countries in this Chapter and where applicable in Commission Implementing Decision C(2015) 8005 final ([2]) include other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, the Title VI of Part Three of that Treaty does not apply.

▼M8

1.0.6. The appropriate authority shall establish and implement procedures to share, as appropriate and in a practical and timely manner, relevant information to assist other national authorities and agencies, airport operators, air carriers and other entities concerned, to conduct effective security risk assessments relating to their operations.

▼B

1.1 AIRPORT PLANNING REQUIREMENTS

1.1.1 **Boundaries**

1.1.1.1 Boundaries between landside, airside, security restricted areas, critical parts and, where applicable, demarcated areas shall be clearly identifiable at each airport in order to enable the appropriate security measures to be taken in each of those areas.

([1]) Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council (OJ L 91, 3.4.2009, p. 7).

([2]) Commission Implementing Decision C(2015) 8005 final laying down detailed measures for the implementation of the common basic standards on aviation security containing information, as referred to in point (a) of Article 18 of Regulation (EC) No 300/2008, and repealing Decision (2010) 774 of 13 April 2010.

▼B

1.1.1.2 The boundary between landside and airside shall be a physical obstruction that is clearly visible to the general public and which denies a person unauthorised access.

1.1.2 **Security restricted areas**

1.1.2.1 Security restricted areas shall include at least the following:

(a) a part of an airport to which screened departing passengers have access; and

(b) a part of an airport through which screened departing hold baggage may pass or in which it may be held, unless it concerns secured baggage; and

(c) a part of an airport designated for the parking of aircraft to be boarded or loaded.

1.1.2.2 A part of an airport shall be regarded as a security restricted area at least for the period of time that the activities referred to in point 1.1.2.1 are taking place.

When a security restricted area is established, a security search of the parts that could have been contaminated shall be carried out immediately before such an area is established in order to reasonably ensure that it does not contain prohibited articles. This provision shall be considered to be met for aircraft that are subject to an aircraft security search.

▼M15

Persons carrying out a security search in areas different than those used by disembarking passengers not screened to the common basic standards, must be trained in accordance with point 11.2.3.1, 11.2.3.2, 11.2.3.3, 11.2.3.4 or 11.2.3.5.

▼B

1.1.2.3 Whenever unauthorised persons may have had access to security restricted areas, a security search of the parts that could have been contaminated shall be carried out as soon as possible in order to reasonably ensure that it does not contain prohibited articles. This provision shall be considered to be met for aircraft that are subject to an aircraft security search.

1.1.3 **Critical parts of security restricted areas**

▼M2

1.1.3.1 Critical parts shall be established at airports where more than 60 persons hold airport identification cards giving access to security restricted areas.

▼B

1.1.3.2 Critical parts shall include at least the following:

(a) all parts of an airport to which screened departing passengers have access; and

(b) all parts of an airport through which screened departing hold baggage may pass or in which it may be held, unless it concerns secured baggage.

A part of an airport shall be regarded as a critical part at least for the period of time that the activities referred to in points (a) or (b) are taking place.

1.1.3.3 When a critical part is established, a security search of the parts that could have been contaminated shall be carried out immediately before such a part is established in order to reasonably ensure that it does not contain prohibited articles. This provision shall be considered to be met for aircraft that are subject to an aircraft security search.

▼M5

1.1.3.4 A security search of those critical parts that could have been contaminated shall be carried out as soon as possible in order to reasonably ensure that they do not contain prohibited articles, wherever access to critical parts has occurred by any of the following:

(a) unscreened persons;

(b) passengers and crew members arriving from third countries other than those listed in Attachment 4-B;

▼M5

(c) passengers and crew members arriving from Union airports where the relevant Member State has derogated from the common basic standards as provided for in Article 1 of Commission Regulation (EU) No 1254/2009 ([1]), unless they are met upon their arrival and escorted outside those areas in accordance with point 1.2.7.3.

This point shall be considered to be met for aircrafts that are subject to an aircraft security search, and it shall not apply when persons covered by point 1.3.2 and point 4.1.1.7 have had access to critical parts.

As far as points (b) and (c) are concerned, this provision shall only apply to those critical parts that are used by screened hold baggage and/or screened departing passengers not departing on the same aircraft as these passengers and crew members.

▼B

1.2 ACCESS CONTROL

1.2.1 **Access to airside**

1.2.1.1 Access to airside may only be authorised if persons and vehicles have a legitimate reason to be there. Guided tours of the airport escorted by authorised persons shall be considered to have a legitimate reason.

1.2.1.2 In order to be granted access to airside a person shall carry an authorisation.

1.2.1.3 In order to be granted access to airside a vehicle shall display a vehicle pass.

1.2.1.4 Persons who are airside shall, upon request, present their authorisation for control.

1.2.2 **Access to security restricted areas**

1.2.2.1 Access to security restricted areas may only be granted if persons and vehicles have a legitimate reason to be there. Guided tours of the airport escorted by authorised persons shall be considered to have a legitimate reason.

1.2.2.2 In order to be granted access to security restricted areas a person shall present one of the following authorisations:

(a) a valid boarding card or equivalent; or

(b) a valid crew identification card; or

(c) a valid airport identification card; or

(d) a valid national appropriate authority identification card; or

(e) a valid compliance authority identification card recognised by the national appropriate authority.

Alternatively, access may also be granted after positive identification via biometric data verification.

1.2.2.3 In order to be granted access to security restricted areas a vehicle shall display a valid vehicle pass.

1.2.2.4 The boarding card or equivalent referred to in point 1.2.2.2(a) shall be checked before a person is granted access to security restricted areas in order to reasonably ensure that it is valid.

([1]) Commission Regulation (EU) No 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures (OJ L 338, 19.12.2009, p. 17).

▼B

The card referred to in points 1.2.2.2(b)-(e), respectively, shall be checked before a person is granted access to security restricted areas in order to reasonably ensure that it is valid and corresponds to the holder.

Where biometric identification is used, the verification shall ensure that the person seeking access to security restricted areas holds one of the authorisations listed under point 1.2.2.2 and that this authorisation is valid and was not disabled.

1.2.2.5 In order to prevent unauthorised access to security restricted areas access points shall be controlled by:

(a) an electronic system which limits access to one person at a time; or

(b) authorised persons implementing access control.

The appropriate authority may define in its national aviation security programme that the limitation to one person at a time under point (a) does not apply at access points exclusively used by law enforcement officers.

1.2.2.6 The vehicle pass shall be checked before a vehicle is granted access to security restricted areas to ensure that it is valid and corresponds to the vehicle.

1.2.2.7 Access to security restricted areas shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼M5

1.2.3 **Requirements for Union crew identification cards and airport identification cards**

1.2.3.1 A crew identification card of a crew member employed by a Union air carrier and an airport identification card may only be issued to a person who has an operational need and has successfully completed an enhanced background check in accordance with point 11.1.3.

1.2.3.2 Crew and airport identification cards shall be issued for a period not exceeding five years.

1.2.3.3 The identification card of a person who fails an enhanced background check shall be immediately disabled or withdrawn, as applicable, and returned to the competent authority, operator or issuing entity, as appropriate.

1.2.3.4 The identification card shall be worn in a visible place at least whenever the holder is in security restricted areas.

A person who is not displaying his identification card in security restricted areas other than those areas where passengers are present shall be challenged by persons responsible for the implementation of point 1.5.1(c) and, as appropriate, be reported.

1.2.3.5 The identification card shall be returned immediately in the following circumstances:

(a) upon request of the competent authority, operator or issuing entity as appropriate;

(b) upon termination of employment;

(c) upon change of employer;

(d) upon change of the need to have access to areas for which an authorisation has been given;

(e) upon expiry of the card;

(f) upon withdrawal of the card.

1.2.3.6 The issuing entity shall be notified immediately of the loss, theft or failure to return an identification card.

▼M5

1.2.3.7 An electronic card shall be immediately disabled following return, expiry, withdrawal or notification of loss, theft or failure to return.

▼B

1.2.4 **Supplementary requirements for Union crew identification cards**

1.2.4.1 A crew identification card of a crew member employed by a Union air carrier shall display:

(a) the name and photograph of the holder; and

(b) the name of the air carrier; and

(c) the word ‘crew’ in English; and

(d) the expiry date.

1.2.5 **Supplementary requirements for airport identification cards**

1.2.5.1 An airport identification card shall display:

(a) the name and photograph of the holder; and

(b) the name of the employer of the holder, unless electronically programmed; and

(c) the name of either the issuing entity or the airport; and

(d) the areas for which the holder is authorised to have access; and

(e) the expiry date, unless electronically programmed.

The names and areas of access may be replaced by an equivalent identification.

1.2.5.2 In order to prevent the misuse of airport identification cards, a system shall be in place to reasonably ensure that attempted use of cards that have been lost, stolen or not returned is detected. Upon detection, appropriate action shall be taken.

1.2.6 **Requirements for vehicle passes**

1.2.6.1 A vehicle pass may only be issued where an operational need has been established.

1.2.6.2 A vehicle pass shall be specific to the vehicle and display:

(a) the areas for which it is authorised to have access; and

(b) the expiry date.

▼M2

_____

1.2.6.3 An electronic vehicle pass shall, either:

(a) be fixed to the vehicle in a manner which ensures that it is non-transferable; or

▼M5

(b) be linked to the company or individual registered vehicle user through a secure vehicle registration database.

▼M2

Electronic vehicle passes need not display the areas for which the vehicle is authorised to have access nor the expiry date, provided that this information is electronically readable and checked before granting access to security restricted areas. ►M5 Electronic vehicle passes shall also be electronically readable airside. ◄

▼B

1.2.6.4 The vehicle pass shall be displayed in a visible place whenever the vehicle is airside.

1.2.6.5 The vehicle pass shall be returned immediately to the issuing entity:

(a) upon request of the issuing entity; or

(b) when the vehicle is no longer to be used for access to airside; or

(c) upon expiry of the pass, unless the pass is automatically invalidated.

1.2.6.6 The issuing entity shall be notified immediately of the loss, theft or failure to return a vehicle pass.

1.2.6.7 An electronic vehicle pass shall be immediately disabled following return, expiry or notification of loss, theft or failure to return.

1.2.6.8 In order to prevent the misuse of vehicle passes, a system shall be in place to reasonably ensure that attempted use of vehicle passes that have been lost, stolen or not returned is detected. Upon detection, appropriate action shall be taken.

1.2.6.9 Vehicles that are only used airside and have no permission to drive on public roads may be exempted from application of points 1.2.6.2 to 1.2.6.8 provided that they are clearly marked externally as operational vehicles in use at that airport.

1.2.7 **Escorted access**

1.2.7.1 Crew members, other than those holding a valid airport identification card, shall be escorted at all times when in security restricted areas other than:

(a) areas where passengers may be present; and

(b) areas in the immediate proximity of the aircraft on which they have arrived or will depart; and

(c) areas designated for crews; and

(d) distances between the terminal or access point and the aircraft on which crew members have arrived or will depart.

1.2.7.2 Exceptionally, a person may be exempted from the requirements of point 1.2.5.1 and obligations on background checks on condition that that person is escorted at all times when in security restricted areas. A person may be exempted from the requirement to be escorted if that person displays an authorisation and is a holder of a valid airport identification card.

1.2.7.3 An escort shall:

(a) hold a valid identification card as referred to in point 1.2.2.2(c), (d) or (e); and

(b) be authorised to escort in security restricted areas; and

(c) have the escorted person or persons in direct line of sight at all times; and

(d) reasonably ensure that no security breach is committed by the person or persons being escorted.

1.2.7.4 A vehicle may be exempted from the requirements of point 1.2.6 on condition that it is escorted at all times when airside.

1.2.7.5 Whenever a passenger does not travel as a result of an air carriage contract resulting in the delivery of a boarding pass or equivalent, a crew member escorting this passenger may be exempted from the requirements of point 1.2.7.3(a).

▼B

1.2.8 **Other exemptions**

Other exemptions shall be subject to provisions laid down in Commission Implementing Decision C(2015) 8005.

1.3 SCREENING OF PERSONS OTHER THAN PASSENGERS AND ITEMS CARRIED

1.3.1 **Screening of persons other than passengers and items carried**

1.3.1.1 Persons other than passengers shall be screened by one of the following means:

(a) hand search;

(b) walk-through metal detection equipment (WTMD);

(c) explosive detection dogs;

(d) explosive trace detection (ETD) equipment;

(e) security scanners which do not use ionising radiation;

▼M5

(f) explosive trace detection (ETD) equipment combined with hand held metal detection (HHMD) equipment;

(g) shoe metal detection (SMD) equipment;

(h) shoe explosive detection (SED) equipment.

SMD and SED equipment may only be used as a supplementary means of screening.

▼B

1.3.1.2 Points 4.1.1.3 – 4.1.1.6 and 4.1.1.10 – 4.1.1.11 shall apply to the screening of persons other than passengers.

▼M5

1.3.1.3 Explosive detection dogs, ETD equipment and ETD equipment in combination with SED equipment may only be used as a supplementary means of screening of persons other than passengers or in unpredictable alternation with hand searches, hand searches in combination with SMD equipment, WTMD or security scanners.

▼M16

1.3.1.4 Items carried by persons other than passengers shall be screened by one of the following means:

(a) hand search;

(b) x-ray equipment;

(c) explosive detection systems (EDS) equipment;

(d) automated prohibited items detection (APID) software in combination with point (c);

(e) explosive detection dogs;

(f) explosive trace detection (ETD) equipment.

Where the screener cannot determine whether or not the items carried contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

1.3.1.5 Points 4.1.2.4 to 4.1.2.7 and 4.1.2.11 to 4.1.2.12 shall apply to the screening of items carried by persons other than passengers.

▼B

1.3.1.6 Explosive detection dogs and ETD equipment may only be used as a supplementary means of screening of items carried by persons other than passengers or in unpredictable alternation with hand searches, x-ray equipment or EDS equipment.

▼B

1.3.1.7 Where persons other than passengers and items carried have to be screened on a continuous random basis, the frequency shall be established by the appropriate authority on the basis of a risk assessment.

▼M2

1.3.1.8 Animals used for operational needs and handled by a person carrying a valid airport identification card shall be subjected to a visual check before access to security restricted areas is granted.

1.3.1.9 The screening of persons other than passengers and items carried shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼B

1.3.2 **Exemptions and special screening procedures**

1.3.2.1 The appropriate authority may, for objective reasons, allow persons other than passengers to be exempted from screening, or to be subjected to special screening procedures, provided that they are escorted by a person authorised to escort in accordance with point 1.2.7.3.

1.3.2.2 Screened persons other than passengers who temporarily leave critical parts may be exempted from screening on their return provided that they have been under constant observation by authorised persons sufficient to reasonably ensure that they do not introduce prohibited articles into those critical parts.

1.3.2.3 Exemptions and special screening procedures shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

1.4 EXAMINATION OF VEHICLES

1.4.1 **Vehicles entering critical parts**

1.4.1.1 All vehicles shall be examined before entering critical parts. They shall be protected from unlawful interference from after examination until entering critical parts.

1.4.1.2 The driver and any other occupants of the vehicle shall not be in the vehicle when the examination takes place. They shall be required to take their personal belongings out of the vehicle with them for screening.

1.4.1.3 There shall be defined methodologies to ensure the randomness of selection of the areas to be examined.

1.4.1.4 Vehicles entering critical parts shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

1.4.2 **Vehicles entering security restricted areas other than critical parts**

1.4.2.1 The driver and any other occupants of the vehicle shall not be in the vehicle when the examination takes place. They shall be required to take their personal belongings out of the vehicle with them for screening.

1.4.2.2 There shall be defined methodologies to ensure the randomness of selection of both vehicles and the areas to be examined.

1.4.2.3 Vehicles entering security restricted areas other than critical parts shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

1.4.3 **Methods of examination**

1.4.3.1 A hand search shall consist of a thorough manual check of the areas selected, including contents, in order to reasonably ensure that they do not contain prohibited articles.

1.4.3.2 The following methods may only be used as a supplementary means of examination:

(a) explosive detection dogs; and

(b) explosive trace detection (ETD) equipment.

▼B

1.4.3.3 Methods of examination shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

1.4.4 **Exemptions and special examination procedures**

1.4.4.1 The appropriate authority may, for objective reasons, allow vehicles to be exempted from examination, or to be subjected to special examination procedures, provided that they are escorted by a person authorised to escort in accordance with point 1.2.7.3.

▼M15

1.4.4.2 Examined vehicles that temporarily leave critical parts may be exempted from examination on their return provided that they have been under constant observation by authorised persons sufficient to reasonably ensure that no prohibited articles have been introduced into the vehicles.

1.4.4.3 Exemptions and special examination procedures shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼B

1.5 SURVEILLANCE, PATROLS AND OTHER PHYSICAL CONTROLS

1.5.1 Surveillance or patrols shall be undertaken in order to monitor:

(a) the boundaries between landside, airside, security restricted areas, critical parts and, where applicable, demarcated areas; and

(b) areas of, and in proximity of, the terminal that are accessible to the public, including parking areas and roadways; and

(c) the display and validity of persons' identification cards in security restricted areas other than those areas where passengers are present; and

(d) the display and validity of vehicle passes when airside; and

(e) hold baggage, cargo and mail, in-flight supplies and air carrier mail and materials in critical parts waiting to be loaded.

1.5.2 The frequency and means of undertaking surveillance and patrols shall be based on a risk assessment and shall be approved by the appropriate authority. They shall take into account:

(a) the size of the airport, including the number and nature of the operations; and

(b) the layout of the airport, in particular the interrelationship between the areas established at the airport; and

(c) the possibilities and limitations of means of undertaking surveillance, and patrols.

The parts of the risk assessment relating to the frequency and means of undertaking surveillance and patrols shall, upon request, be made available in writing for compliance monitoring purposes.

1.5.3 Surveillance and patrols shall not follow a predictable pattern. The validity of identification cards shall be checked on a random basis.

1.5.4 Measures shall be in place that both deter persons from breaching security checkpoints and, should such a breach occur, promptly enable the breach and its repercussions to be resolved and rectified.

▼M15

1.5.5 Procedures shall be established in order to deal with unidentified baggage and suspicious objects in accordance with a security risk assessment carried out or approved by the relevant national authorities.

▼B

1.6 PROHIBITED ARTICLES

1.6.1 Persons other than passengers shall not be permitted to carry into security restricted areas the articles listed in Attachment 1-A.

▼B

1.6.2 An exemption to point 1.6.1 may be granted on condition that the person is authorised to carry prohibited articles into security restricted areas in order to undertake tasks that are essential for the operation of airport facilities or of aircraft, or for performing in-flight duties.

1.6.3 In order to allow reconciliation of the person authorised to carry one or more articles as listed in Attachment 1-A with the article carried:

(a) the person shall have an authorisation and shall carry it. The authorisation shall either be indicated on the identification card that grants access to security restricted areas or on a separate declaration in writing. The authorisation shall indicate the article(s) that may be carried, either as a category or as a specific article. If the authorisation is indicated on the identification card, then it shall be recognisable on a need-to-know basis; or

(b) a system shall be in place at the security checkpoint indicating which persons are authorised to carry which article(s), either as a category or as a specific article.

▼M2

1.6.4 Reconciliation shall be performed before the person is allowed to carry the article(s) concerned into security restricted areas and upon being challenged by persons performing surveillance or patrols under point (c) of point 1.5.1.

▼B

1.6.5 Articles as listed in Attachment 1-A may be stored in security restricted areas provided they are kept in secure conditions. Articles as listed in points (c), (d) and (e) of Attachment 4-C may be stored in security restricted areas provided they are not accessible to passengers.

▼M8

1.7 IDENTIFICATION AND PROTECTION OF CIVIL AVIATION CRITICAL INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS AND DATA FROM CYBER THREATS

1.7.1 The appropriate authority shall ensure that airport operators, air carriers and entities as defined in the national civil aviation security programme identify and protect their critical information and communications technology systems and data from cyber-attacks which could affect the security of civil aviation.

1.7.2 Airport operators, air carriers and entities shall identify in their security programme, or any relevant document cross-referenced in the security programme, the critical information and communications technology systems and data described in 1.7.1.

The security programme, or any relevant document cross-referenced in the security programme shall detail the measures to ensure the protection from, detection of, response to and recovery from cyber-attacks, as described in 1.7.1.

1.7.3 The detailed measures to protect such systems and data from unlawful interference shall be identified, developed and implemented in accordance with a risk assessment carried out by the airport operator, air carrier or entity as appropriate.

1.7.4 Where a specific authority or agency is competent for measures related to cyber threats within a single Member State, this authority or agency may be designated as competent for the coordination and/or monitoring of the cyber-related provisions in this Regulation.

▼M8

1.7.5 Where airport operators, air carriers and entities as defined in the national civil aviation security programme are subjected to separate cybersecurity requirements arising from other EU or national legislation, the appropriate authority may replace compliance with the requirements of this regulation by compliance with the elements contained in the other EU or national legislation. The appropriate authority shall coordinate with any other relevant competent authorities to ensure coordinated or compatible oversight regimes.

▼B

ATTACHMENT 1-A

PERSONS OTHER THAN PASSENGERS

LIST OF PROHIBITED ARTICLES

(a) *guns, firearms and other devices that discharge projectiles* — devices capable, or appearing capable, of being used to cause serious injury by discharging a projectile, including:

— firearms of all types, such as pistols, revolvers, rifles, shotguns,

— toy guns, replicas and imitation firearms capable of being mistaken for real weapons,

— component parts of firearms, excluding telescopic sights,

— compressed air and CO_2 guns, such as pistols, pellet guns, rifles and ball bearing guns,

— signal flare pistols and starter pistols,

— bows, cross bows and arrows,

— harpoon guns and spear guns,

— slingshots and catapults;

(b) *stunning devices* — devices designed specifically to stun or immobilise, including:

— devices for shocking, such as stun guns, tasers and stun batons,

— animal stunners and animal killers,

— disabling and incapacitating chemicals, gases and sprays, such as mace, pepper sprays, capsicum sprays, tear gas, acid sprays and animal repellent sprays;

▼B

(c) *explosives and incendiary substances and devices* — explosives and incendiary substances and devices capable, or appearing capable, of being used to cause serious injury or to pose a threat to the safety of aircraft, including:

— ammunition,

— blasting caps,

— detonators and fuses,

— replica or imitation explosive devices,

— mines, grenades and other explosive military stores,

— fireworks and other pyrotechnics,

— smoke-generating canisters and smoke-generating cartridges,

— dynamite, gunpowder and plastic explosives.

(d) any other article capable of being used to cause serious injury and which is not commonly used in security restricted areas, e.g. martial arts equipment, swords, sabres, etc.

2. **DEMARCATED AREAS OF AIRPORTS**

No provisions in this Regulation.

3. **AIRCRAFT SECURITY**

3.0 GENERAL PROVISIONS

3.0.1 Unless otherwise stated, an air carrier shall ensure the implementation of the measures set out in this Chapter as regards its aircraft.

3.0.2 Third countries where the security standards applied are recognised as equivalent to the common basic standards as regards aircraft security are listed in Attachment 3-B.

3.0.3 An aircraft need not be subjected to an aircraft security check. It shall be subjected to an aircraft security search in accordance with point 3.1.

3.0.4 An air carrier shall, upon request, be notified by the airport operator whether or not its aircraft is in a critical part. When this is not clear, it shall be assumed that the aircraft is in a part other than a critical part.

3.0.5 When an area is no longer considered to be a critical part because of a change of security status then the airport shall inform those carriers that are affected.

▼M2

3.0.6 The list of prohibited articles for aircraft security searches of the interior of aircraft is the same as the one set out in Attachment 1-A. Assembled explosive and incendiary devices shall be considered as prohibited articles for aircraft security searches of the exterior of aircraft.

3.0.7 For the purpose of this Chapter, ‘aircraft service panels and hatches’ means aircraft external access points and compartments that have external handles or external clip-down panels and are routinely used for providing aircraft ground handling services.

3.0.8 References to third countries in this Chapter and in Commission Implementing Decision C(2015) 8005 include other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply.

▼B

3.1 AIRCRAFT SECURITY SEARCH

3.1.1 **When to perform an aircraft security search**

3.1.1.1 An aircraft shall at all times be subjected to an aircraft security search whenever there is reason to believe that unauthorised persons may have had access to it.

3.1.1.2 An aircraft security search shall consist of an examination of defined areas of an aircraft that are laid down in Commission Implementing Decision C(2015) 8005.

3.1.1.3 An aircraft arriving into a critical part from a third country not listed in Attachment 3-B shall be subjected to an aircraft security search any time after passenger disembarkation from the area to be searched and/or the unloading of the hold. ►M15 The search may not start until the aircraft has reached its final parking position. ◄

3.1.1.4 An aircraft arriving from a Member State where it was in transit after having arrived from a third country not listed in Attachment 3-B shall be considered as an aircraft arriving from a third country.

3.1.1.5 When to perform an aircraft security search shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

3.1.2 **How to perform an aircraft security search**

How to perform an aircraft security search shall be subject to the provisions laid down in Commission Implementing Decision C(2015) 8005.

▼M15

3.1.3 **Information on the aircraft security search**

The following information on the aircraft security search performed of a departing flight shall be recorded and kept at a point not on the aircraft for the duration of the flight or for 24 hours, whichever is longer:

(a) flight number;

(b) origin of the previous flight;

(c) date and time that the aircraft security search was completed;

(d) the name and signature of the person responsible for the performance of the aircraft security search.

Recording of the information listed in the first paragraph may be held in electronic format.

▼B

3.2 PROTECTION OF AIRCRAFT

3.2.1 **Protection of aircraft — General**

3.2.1.1 Regardless of where an aircraft is parked at an airport, each of its external doors shall be protected against unauthorised access by:

(a) ensuring that persons seeking to gain unauthorised access are challenged promptly; or

(b) having the external door closed. Where the aircraft is in a critical part, external doors that are not accessible by a person from the ground shall be considered closed if access aids have been removed and placed sufficiently far from the aircraft as to reasonably prevent access by a person; or

▼B

(c) having electronic means which will immediately detect unauthorised access; or;

(d) having an electronic airport identification card access system at all doors leading directly to the passenger boarding bridge, adjacent to an open aircraft door, which only allows access for persons that are trained in accordance with point 11.2.3.7. Such persons must ensure that unauthorised access is prevented, during their use of the door.

3.2.1.2 Point 3.2.1.1 shall not apply to an aircraft parked in a hangar that is locked or otherwise protected from unauthorised access.

3.2.2 **Additional protection of aircraft with closed external doors in a part other than a critical part**

3.2.2.1 Where external doors are closed and the aircraft is in a part other than a critical part, each external door shall also:

(a) have access aids removed; or

(b) be sealed; or

(c) be locked; or

(d) be monitored.

Point (a) shall not apply for a door that is accessible from the ground by a person.

3.2.2.2 Where access aids are removed for doors that are not accessible by a person from the ground, they shall be placed sufficiently far from the aircraft as to reasonably prevent access.

3.2.2.3 Where external doors are locked, only persons with an operational need shall be able to unlock these doors.

3.2.2.4 Where external doors are monitored, the monitoring shall ensure that unauthorised access to the aircraft is immediately detected.

3.2.2.5 The protection of aircraft with closed external doors in a part other than a critical part shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 3-A

AIRCRAFT SECURITY SEARCH

Detailed provisions for an aircraft security search are laid down in Commission Implementing Decision C(2015) 8005.

▼M7

ATTACHMENT 3-B

AIRCRAFT SECURITY

THIRD COUNTRIES, AS WELL AS OTHER COUNTRIES AND TERRITORIES TO WHICH, IN ACCORDANCE WITH ARTICLE 355 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, TITLE VI OF PART THREE OF THAT TREATY DOES NOT APPLY, THAT ARE RECOGNISED AS APPLYING SECURITY STANDARDS EQUIVALENT TO THE COMMON BASIC STANDARDS ON CIVIL AVIATION SECURITY

As regards aircraft security, the following third countries, as well as other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply, have been recognised as applying security standards equivalent to the common basic standards on civil aviation security:

▼M7

Canada

Faroe Islands, in regard to Vagar airport

Greenland, in regard to Kangerlussuaq airport

Guernsey

Isle of Man

Jersey

Montenegro

▼M13

Republic of Serbia, in regard to Belgrade Nikola Tesla Airport

▼M7

Republic of Singapore, in regard to Singapore Changi Airport

▼M13

State of Israel, in regard to Ben Gurion International Airport

▼M7

United Kingdom of Great Britain and Northern Ireland

United States of America

The Commission shall immediately notify the appropriate authorities of the Member States if it has information indicating that security standards applied by the third country or other country or territory concerned with a significant impact on overall levels of aviation security in the Union are no longer equivalent to the common basic standards of the Union.

The appropriate authorities of the Member States shall be notified without delay when the Commission has information about actions, including compensatory measures, confirming that the equivalency of relevant security standards applied by the third country or other country or territory concerned is re-established.

▼B

4. PASSENGERS AND CABIN BAGGAGE

4.0 GENERAL PROVISIONS

4.0.1 Unless otherwise stated, the authority, airport operator, air carrier or entity responsible in accordance with the national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 shall ensure the implementation of the measures set out in this Chapter.

4.0.2 Third countries where the security standards applied are recognised as equivalent to the common basic standards as regards passengers and cabin baggage are listed in Attachment 4-B.

▼M5

4.0.3 Passengers and their cabin baggage arriving from a Member State where the aircraft was in transit after having arrived from a third country not listed in Attachment 4-B or from a Union airport where the relevant Member State has derogated from the common basic standards as provided for in Article 1 of Regulation (EU) No 1254/2009, shall be considered as passengers and cabin baggage arriving from a third country, unless there is a confirmation that these passengers and their cabin baggage were screened in accordance with this Chapter.

▼B

4.0.4 For the purpose of this Annex:

(a) ‘liquids, aerosols and gels’ (LAGs) shall include pastes, lotions, liquid/solid mixtures and the contents of pressurised containers, such as toothpaste, hair gel, drinks, soups, syrups, perfume, shaving foam and other items with similar consistencies;

(b) ‘security tamper-evident bag’ (STEB) is a bag that conforms to the recommended security control guidelines of the International Civil Aviation Organisation;

▼B

(c) ‘liquid explosive detection systems (LEDS) equipment’ is a piece of equipment capable of detecting threat materials that meets the provisions of point 12.7 of the Annex to Commission Implementing Decision C(2015) 8005.

4.0.5 References to third countries in this Chapter and where applicable in Commission Implementing Decision C(2015) 8005 include other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply.

▼M5

4.0.6 Passengers and their cabin baggage arriving from a Union airport where the relevant Member State has derogated from the common basic standards as provided for in Article 1 of Regulation (EU) No 1254/2009 shall be considered as passengers and cabin baggage arriving from a third country, unless there is confirmation that these passengers and their cabin baggage were screened in accordance with this Chapter.

▼B

4.1 SCREENING OF PASSENGERS AND CABIN BAGGAGE

4.1.1 **Screening of passengers**

▼M16

4.1.1.1 Before screening, outer wear shall be taken off and shall be screened as cabin baggage, unless the concept of operations of equipment allows for outer wear to be kept on. The screener may request the passenger to undertake further divesting as appropriate.

▼B

4.1.1.2 Passengers shall be screened by at least one of the following methods:

(a) hand search;

(b) walk-through metal detection equipment (WTMD);

(c) explosive detection dogs;

(d) explosive trace detection (ETD) equipment;

(e) security scanners which do not use ionising radiation;

▼M5

(f) ETD equipment combined with hand held metal detection (HHMD) equipment;

(g) shoe metal detection (SMD) equipment;

(h) shoe explosive detection (SED) equipment.

▼B

Where the screener cannot determine whether or not the passenger is carrying prohibited articles, the passenger shall be denied access to security restricted areas or rescreened to the screener's satisfaction.

4.1.1.3 When a hand search is performed it shall be carried out so as to reasonably ensure that the person is not carrying prohibited articles.

4.1.1.4 When WTMD equipment alarms, the cause of the alarm shall be resolved.

4.1.1.5 Hand-held metal detection (HHMD) equipment may only be used as a supplementary means of screening. It shall not replace the requirements of a hand search.

▼B

4.1.1.6 Where a live animal is permitted to be carried in the cabin of an aircraft, it shall be screened either as a passenger or as cabin baggage.

4.1.1.7 The appropriate authority may create categories of passengers that, for objective reasons, shall be subject to special screening procedures or may be exempted from screening. The Commission shall be informed of the categories created.

4.1.1.8 The screening of passengers shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼M5

4.1.1.9 Explosive detection dogs, ETD equipment, SMD equipment and SED equipment may only be used as a supplementary means of screening.

▼B

4.1.1.10 When a security scanner with a human reviewer, as defined under the second paragraph of point 12.11.1, is used for screening of passengers, all of the following minimum conditions shall be complied with:

(a) security scanners shall not store, retain, copy, print or retrieve images. However, any image generated during the screening can be kept for the time needed for the human reviewer to analyse it and shall be deleted as soon as the passenger is cleared. Any unauthorised access and use of the image is prohibited and shall be prevented;

(b) the human reviewer analysing the image shall be in a separate location so that he/she cannot see the screened passenger;

(c) any technical devices capable of storing, copying or photographing or otherwise recording images shall not be allowed into the separate location where the image is analysed;

(d) the image shall not be linked to any data concerning the screened person and his/her identity shall be kept anonymous;

(e) a passenger may request that the image of his/her body is analysed by a human reviewer of the gender of his/her choice;

(f) the image shall be blurred or obscured to prevent the identification of the face of the passenger.

Paragraphs (a) and (d) shall also apply to security scanners with automatic threat detection.

Passengers shall be entitled to opt out from a security scanner. In this case the passenger shall be screened by an alternative screening method including at least a hand search in accordance with Attachment 4-A of Commission Implementing Decision C(2015) 8005. When the security scanner alarms, the cause of the alarm shall be resolved.

Before being screened by a security scanner, the passenger shall be informed of the technology used, the conditions associated to its use and the possibility to opt out from a security scanner.

4.1.1.11 Explosive trace detection (ETD) equipment in combination with hand held metal detection (HHMD) equipment may only be used in cases where the screener considers a hand search of a given part of the person to be inefficient and/or undesirable.

▼B

4.1.2 **Screening of cabin baggage**

4.1.2.1 Before screening, portable computers and other large electrical items shall be removed from cabin baggage and shall be screened separately, unless the cabin baggage is to be screened with Explosive Detection Systems (EDS) equipment meeting standard C2 or higher.

4.1.2.2 The appropriate entity at all airports shall screen, upon entry to the security restricted area (SRA), at least LAGs obtained at an airport or on board an aircraft that are sealed in a STEB inside which is displayed satisfactory proof of purchase at airside at an airport or on board an aircraft, as well as LAGs to be used during the trip for medical purposes or a special dietary requirement, including baby food.

Before screening, LAGs shall be removed from cabin baggage and shall be screened separately from other items of cabin baggage, unless the equipment used for the screening of cabin baggage is also capable of screening multiple closed LAGs containers inside baggage.

Where LAGs have been removed from cabin baggage, the passenger shall present:

(a) all LAGs in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent resealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably and the bag is completely closed; and

(b) all other LAGs, including STEBs containing LAGs.

Appropriate authorities, airlines and airports shall provide appropriate information to passengers in respect of the screening of LAGs at their airports.

▼M16

4.1.2.3 Cabin baggage shall be screened by at least one of the following methods:

(a) a hand search;

(b) x-ray equipment;

(c) explosive detection systems (EDS) equipment;

(d) automated prohibited items detection (APID) software in combination with point (c);

(e) explosive detection dogs in combination with point (a);

(f) ETD equipment.

Where the screener cannot determine whether or not the cabin baggage contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

▼B

4.1.2.4 A hand search of cabin baggage shall consist of a manual check of the baggage, including its contents, as to reasonably ensure that it does not contain prohibited articles.

▼M16

4.1.2.5 Where x-ray equipment is used, each image shall be viewed by the screener.

Where EDS equipment is used, each image shall be viewed by the screener or analysed by automated prohibited items detection (APID) software.

4.1.2.6 Where APID software is used, all alarms as referred to in point 12.13.1.1 shall be resolved to the satisfaction of the screener so as to reasonably ensure that no prohibited articles are carried into the SRA or on board an aircraft.

Where EDS equipment is used, all alarms as referred to in point 12.4.1.3 shall be resolved by screening the baggage again using an additional screening method.

Where EDS equipment has been installed before 1 July 2023 and is used without APID software, all alarms as referred to in point 12.4.1.3 shall be resolved to the satisfaction of the screener so as to reasonably ensure that no prohibited articles are carried into the SRA or on board an aircraft. When the identity of an article is unclear, the alarms shall be resolved by screening the baggage again using an additional screening method.

▼B

4.1.2.7 Where x-ray or EDS equipment is used, any item whose density impairs the ability of the screener to analyse the contents of the cabin baggage shall be taken out of the baggage. The bag shall be screened again and the item shall be screened separately as cabin baggage.

4.1.2.8 Any bag that is found to contain a large electrical item shall be screened again with the item no longer in the bag and the electrical item screened separately, unless the cabin baggage was screened with EDS equipment meeting standard C2 or higher.

4.1.2.9 Explosive detection dogs and explosive trace detection (ETD) equipment may only be used as a supplementary means of screening.

4.1.2.10 The appropriate authority may create categories of cabin baggage that, for objective reasons, shall be subject to special screening procedures or may be exempted from screening. The Commission shall be informed of the categories created.

4.1.2.11 Persons screening cabin baggage by x-ray or EDS equipment shall normally not spend more than 20 minutes continuously reviewing images. After each of these periods, the screener shall not review images for at least 10 minutes. This requirement shall only apply when there is an uninterrupted flow of images to be reviewed.

There shall be a supervisor responsible for screeners of cabin baggage in order to assure optimum team composition, quality of work, training, support and appraisal.

▼M16

4.1.2.12 Where APID software is used in combination with EDS equipment meeting either of standards C1, C1+, C2 or C2+, the operator or entity using equipment shall ensure that the procedures are in accordance with the concept of operations of these standards as regards screening of large electronic items and screening of LAGs.

▼M16

4.1.2.13 The screening of cabin baggage shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼B

4.1.3 **Screening of liquids, aerosols and gels (LAGs)**

▼M5

4.1.3.1 LAGs carried by passengers may be exempted from screening with LEDS equipment upon entry to the SRA if the LAGs are in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent resealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably and the bag is completely closed.

———————

▼M2

4.1.3.3 The appropriate authority may create categories of LAGs that, for objective reasons, shall be subjected to special screening procedures or may be exempted from screening. The Commission shall be informed of the categories created.

4.1.3.4 The screening of LAGs shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼B

4.2 PROTECTION OF PASSENGERS AND CABIN BAGGAGE

The protection of passengers and cabin baggage shall be subject to the provisions laid down in Commission Implementing Decision C(2015) 8005.

4.3 POTENTIALLY DISRUPTIVE PASSENGERS

4.3.1 An air carrier shall be notified in writing in advance by the competent authority of the plan to embark a potentially disruptive passenger on board its aircraft.

4.3.2 The notification shall contain the following details:

(a) identity and gender of the person; and

(b) reason for transportation; and

(c) name and title of escorts, if provided; and

(d) risk assessment by the competent authority, including reasons to escort or not; and

(e) prior seating arrangement, if required; and

(f) the nature of the available travel documents.

The air carrier shall make this information available to the pilot in command prior to passengers boarding the aircraft.

4.3.3 The competent authority shall ensure that persons in lawful custody are always escorted.

4.4 PROHIBITED ARTICLES

4.4.1 Passengers shall not be permitted to carry into security restricted areas or on board an aircraft the articles listed in Attachment 4-C.

4.4.2 An exemption to point 4.4.1 may be granted on condition that:

(a) the appropriate authority has given consent that the article may be carried; and

(b) the air carrier has been informed about the passenger and the article that the passenger is carrying prior to passengers boarding the aircraft; and

(c) the applicable safety rules are complied with.

These articles shall then be placed in secure conditions on board aircraft.

▼B

4.4.3 The air carrier shall ensure that passengers are informed of the prohibited articles listed in Attachment 4-C before check-in is completed.

ATTACHMENT 4-A

REQUIREMENTS FOR A HAND SEARCH

Detailed provisions for a hand search are laid down in Commission Implementing Decision C(2015) 8005.

▼M7

ATTACHMENT 4-B

PASSENGERS AND CABIN BAGGAGE

THIRD COUNTRIES, AS WELL AS OTHER COUNTRIES AND TERRITORIES TO WHICH, IN ACCORDANCE WITH ARTICLE 355 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, TITLE VI OF PART THREE OF THAT TREATY DOES NOT APPLY, THAT ARE RECOGNISED AS APPLYING SECURITY STANDARDS EQUIVALENT TO THE COMMON BASIC STANDARDS ON CIVIL AVIATION SECURITY

As regards passengers and cabin baggage, the following third countries, as well as other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply, have been recognised as applying security standards equivalent to the common basic standards on civil aviation security:

Canada

Faroe Islands, in regard to Vagar airport

Greenland, in regard to Kangerlussuaq airport

Guernsey

Isle of Man

Jersey

Montenegro

▼M13

Republic of Serbia, in regard to Belgrade Nikola Tesla Airport

▼M7

Republic of Singapore, in regard to Singapore Changi Airport

▼M13

State of Israel, in regard to Ben Gurion International Airport

▼M7

United Kingdom of Great Britain and Northern Ireland

United States of America

The Commission shall immediately notify the appropriate authorities of the Member States if it has information indicating that security standards applied by the third country or other country or territory concerned with a significant impact on overall levels of aviation security in the Union are no longer equivalent to the common basic standards of the Union.

The appropriate authorities of the Member States shall be notified without delay when the Commission has information about actions, including compensatory measures, confirming that the equivalency of relevant security standards applied by the third country or other country or territory concerned is re-established.

▼B

ATTACHMENT 4-C

PASSENGERS AND CABIN BAGGAGE

LIST OF PROHIBITED ARTICLES

Without prejudice to applicable safety rules, passengers are not permitted to carry the following articles into security restricted areas and on board an aircraft:

(a) *guns, firearms and other devices that discharge projectiles* — devices capable, or appearing capable, of being used to cause serious injury by discharging a projectile, including:

— firearms of all types, such as pistols, revolvers, rifles, shotguns,

— toy guns, replicas and imitation firearms capable of being mistaken for real weapons,

— component parts of firearms, excluding telescopic sights,

— compressed air and CO_2 guns, such as pistols, pellet guns, rifles and ball bearing guns,

— signal flare pistols and starter pistols,

— bows, cross bows and arrows,

— harpoon guns and spear guns,

— slingshots and catapults;

(b) *stunning devices* — devices designed specifically to stun or immobilise, including:

— devices for shocking, such as stun guns, tasers and stun batons,

— animal stunners and animal killers,

— disabling and incapacitating chemicals, gases and sprays, such as mace, pepper sprays, capsicum sprays, tear gas, acid sprays and animal repellent sprays;

(c) *objects with a sharp point or sharp edge* — objects with a sharp point or sharp edge capable of being used to cause serious injury, including:

— items designed for chopping, such as axes, hatchets and cleavers,

— ice axes and ice picks,

— razor blades,

— box cutters,

— knives with blades of more than 6 cm,

— scissors with blades of more than 6 cm as measured from the fulcrum,

— martial arts equipment with a sharp point or sharp edge,

— swords and sabres;

(d) *workmen's tools* — tools capable of being used either to cause serious injury or to threaten the safety of aircraft, including:

— crowbars,

— drills and drill bits, including cordless portable power drills,

— tools with a blade or a shaft of more than 6 cm capable of use as a weapon, such as screwdrivers and chisels,

— saws, including cordless portable power saws,

— blowtorches,

— bolt guns and nail guns;

▼B

(e) *blunt instruments* — objects capable of being used to cause serious injury when used to hit, including:

— baseball and softball bats,

— clubs and batons, such as billy clubs, blackjacks and night sticks,

— martial arts equipment;

(f) *explosives and incendiary substances and devices* — explosives and incendiary substances and devices capable, or appearing capable, of being used to cause serious injury or to pose a threat to the safety of aircraft, including:

— ammunition,

— blasting caps,

— detonators and fuses,

— replica or imitation explosive devices,

— mines, grenades and other explosive military stores,

— fireworks and other pyrotechnics,

— smoke-generating canisters and smoke-generating cartridges,

— dynamite, gunpowder and plastic explosives.

5. **HOLD BAGGAGE**

5.0 GENERAL PROVISIONS

5.0.1 Unless otherwise stated, the authority, airport operator, air carrier or entity responsible in accordance with the national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 shall ensure the implementation of the measures set out in this Chapter.

5.0.2 Third countries where the security standards applied are recognised as equivalent to the common basic standards as regards hold baggage are listed in Attachment 5-A.

▼M5

5.0.3 Hold baggage arriving from a Member State where the aircraft was in transit after having arrived from a third country not listed in Attachment 5-A or from a Union airport where the relevant Member State has derogated from the common basic standards as provided for in Article 1 of Regulation (EU) No 1254/2009 shall be considered as hold baggage arriving from a third country, unless there is a confirmation that the hold baggage was screened in accordance with this Chapter.

▼B

5.0.4 For the purpose of this Chapter, ‘secured baggage’ means screened departing hold baggage that is physically protected so as to prevent the introduction of any objects.

5.0.5 References to third countries in this Chapter and where applicable in Commission Implementing Decision C(2015) 8005 include other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply.

▼M5

5.0.6 Hold baggage arriving from a Union airport where the relevant Member State has derogated from the common basic standards as provided for in Article 1 of Regulation (EU) No 1254/2009 shall be considered as hold baggage arriving from a third country, unless there is a confirmation that the hold baggage was screened in accordance with this Chapter.

▼B

5.1 SCREENING OF HOLD BAGGAGE

5.1.1 The following methods, either individually or in combination, shall be used to screen hold baggage:

(a) a hand search; or

(b) x-ray equipment; or

(c) explosive detection systems (EDS) equipment; or

(d) explosive trace detection (ETD) equipment; or

(e) explosive detection dogs.

Where the screener cannot determine whether or not the hold baggage contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

5.1.2 A hand search shall consist of a thorough manual check of the baggage, including all its contents, so as to reasonably ensure that it does not contain prohibited articles.

5.1.3 Where x-ray or EDS equipment is used, any item whose density impairs the ability of the screener to analyse the contents of the baggage shall result in it being subject to another means of screening.

5.1.4 Screening by explosive trace detection (ETD) equipment shall consist of the analysis of samples taken from both the inside and the outside of the baggage and from its contents. The contents may also be subjected to a hand search.

5.1.5 The appropriate authority may create categories of hold baggage that, for objective reasons, shall be subject to special screening procedures or may be exempted from screening. The Commission shall be informed of the categories created.

5.1.6 The screening of hold baggage shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

5.1.7 Persons screening hold baggage by x-ray or EDS equipment shall normally not spend more than 20 minutes continuously reviewing images. After each of these periods, the screener shall not review images for at least 10 minutes. This requirement shall only apply when there is an uninterrupted flow of images to be reviewed.

There shall be a supervisor responsible for screeners of hold baggage in order to assure optimum team composition, quality of work, training, support and appraisal.

5.2 PROTECTION OF HOLD BAGGAGE

5.2.1 Passengers may not be allowed access to screened hold baggage, unless it is their own baggage and they are supervised to ensure that:

(a) no prohibited articles as listed in Attachment 5-B are introduced into the hold baggage; or

(b) no prohibited articles as listed in Attachment 4-C are removed from the hold baggage and introduced into the security restricted areas or on board an aircraft.

▼B

5.2.2 Hold baggage that has not been protected from unauthorised interference shall be rescreened.

5.2.3 The protection of hold baggage shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

5.3 BAGGAGE RECONCILIATION

5.3.1 **Identification of hold baggage**

5.3.1.1 An air carrier shall, during the boarding process, ensure that a passenger presents a valid boarding card or equivalent corresponding to the hold baggage that was checked in.

5.3.1.2 An air carrier shall ensure that there is a procedure in place to identify hold baggage of passengers who did not board or left the aircraft before departure.

5.3.1.3 If the passenger is not on board the aircraft, the hold baggage corresponding to his boarding card or equivalent shall be considered as unaccompanied.

5.3.1.4 An air carrier shall ensure that each item of unaccompanied hold baggage is clearly identifiable as authorised for transport by air.

5.3.2 **Factors beyond the passenger's control**

5.3.2.1 The reason that the baggage became unaccompanied shall be recorded before it is loaded onto an aircraft, unless the security controls as referred to in point 5.3.3 are applied.

5.3.2.2 Additional detailed provisions on the factors beyond the passenger's control are laid down in Commission Implementing Decision C(2015) 8005.

5.3.3 **Appropriate security controls for unaccompanied hold baggage**

5.3.3.1 Unaccompanied hold baggage not covered by point 5.3.2 shall be screened by one of the methods laid down in point 5.1.1 and, where applicable, applying additional requirements laid down in Commission Implementing Decision C(2015) 8005.

5.3.3.2 Hold baggage that becomes unaccompanied baggage due to factors other than those referred to in point 5.3.2.2 shall be removed from the aircraft and rescreened before loading it again.

5.3.3.3 Additional detailed provisions for appropriate security controls for unaccompanied hold baggage are laid down in Commission Implementing Decision C(2015) 8005.

5.4 PROHIBITED ARTICLES

5.4.1 Passengers shall not be permitted to carry in their hold baggage the articles listed in Attachment 5-B.

5.4.2 An exemption to point 5.4.1 may be granted on condition that:

(a) the appropriate authority has national rules permitting carriage of the article; and

(b) the applicable safety rules are complied with.

▼M15

An air carrier shall ensure that the carriage of firearms in hold baggage is allowed only after an authorised and duly qualified person has determined that they are not loaded. Such firearms shall be stowed in a place not accessible to any person during the flight.

▼M2

5.4.3 The air carrier shall ensure that passengers are informed of the prohibited articles listed in Attachment 5-B at any time before the check-in is completed.

▼M7

ATTACHMENT 5-A

HOLD BAGGAGE

THIRD COUNTRIES, AS WELL AS OTHER COUNTRIES AND TERRITORIES TO WHICH, IN ACCORDANCE WITH ARTICLE 355 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, TITLE VI OF PART THREE OF THAT TREATY DOES NOT APPLY, THAT ARE RECOGNISED AS APPLYING SECURITY STANDARDS EQUIVALENT TO THE COMMON BASIC STANDARDS ON CIVIL AVIATION SECURITY

As regards hold baggage, the following third countries, as well as other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply, have been recognised as applying security standards equivalent to the common basic standards on civil aviation security:

Canada

Faroe Islands, in regard to Vagar airport

Greenland, in regard to Kangerlussuaq airport

Guernsey

Isle of Man

Jersey

Montenegro

▼M13

Republic of Serbia, in regard to Belgrade Nikola Tesla Airport

▼M7

Republic of Singapore, in regard to Singapore Changi Airport

State of Israel, in regard to Ben Gurion International Airport

United Kingdom of Great Britain and Northern Ireland

United States of America

The Commission shall notify without delay the appropriate authorities of the Member States if it has information indicating that security standards applied by the third country or other country or territory concerned with a significant impact on overall levels of aviation security in the Union are no longer equivalent to the common basic standards of the Union.

The appropriate authorities of the Member States shall be notified without delay when the Commission has information about actions, including compensatory measures, confirming that the equivalency of relevant security standards applied by the third country or other country or territory concerned is re-established.

▼B

ATTACHMENT 5-B

HOLD BAGGAGE

LIST OF PROHIBITED ARTICLES

Passengers are not permitted to carry the following articles in their hold baggage:

explosives and incendiary substances and devices — explosives and incendiary substances and devices capable of being used to cause serious injury or to pose a threat to the safety of aircraft, including:

— ammunition,

— blasting caps,

— detonators and fuses,

▼B

— mines, grenades and other explosive military stores,

— fireworks and other pyrotechnics,

— smoke-generating canisters and smoke-generating cartridges,

— dynamite, gunpowder and plastic explosives.

6. CARGO AND MAIL

6.0 GENERAL PROVISIONS

6.0.1 The authority, airport operator, air carrier or entity as defined in this Chapter shall ensure the implementation of the measures set out in this Chapter.

6.0.2 Assembled explosive and incendiary devices that are not carried in accordance with the applicable safety rules shall be considered as prohibited articles in consignments of cargo and mail.

6.0.3 References to third countries in this Chapter and where applicable in Commission Implementing Decision C(2015) 8005 include other countries and territories to which, in accordance with Article 355 of the Treaty on the Functioning of the European Union, Title VI of Part Three of that Treaty does not apply.

▼M12

6.0.4 For the purposes of this Annex, 'Pre-Loading Advance Cargo Information' or 'PLACI' means the process of first risk analysis for aviation security purposes of goods to be brought into the customs territory of the Union ([1]) by air.

▼B

6.1 SECURITY CONTROLS — GENERAL PROVISIONS

6.1.1 All cargo and mail shall be screened by a regulated agent before being loaded on to an aircraft, unless:

(a) the required security controls have been applied to the consignment by a regulated agent and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or

(b) the required security controls have been applied to the consignment by a known consignor and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or

▼M15

_____

▼B

(d) the consignment is exempt from screening and has been protected from unauthorised interference from the time that it became identifiable air cargo or identifiable air mail and until loading.

6.1.2 Where there is any reason to believe that a consignment to which security controls have been applied has been tampered with or has not been protected from unauthorised interference from the time that those controls were applied, it shall be screened by a regulated agent before being loaded on to an aircraft. Consignments which appear to have been significantly tampered with or which are otherwise suspect shall be treated as high risk cargo or mail (HRCM) in accordance with point 6.7.

([1]) As Iceland is not part of the customs territory of the Union, for the purposes of point 6.8.7 of this Annex, Iceland is considered a third country.

▼M5

_____

▼M15

6.1.3 A regulated agent who rejects a consignment due to high-risk reasons shall ensure that the consignment and the accompanying documentation are marked as high risk cargo and mail before the consignment is returned to the person representing the entity delivering it. Such consignment shall not be loaded on to an aircraft unless it is treated by another regulated agent in accordance with point 6.7.

▼M12

6.1.4 Access into the security restricted areas of cargo and mail may only be granted after having established to which of the following categories the entity transporting the consignment from landside belongs:

(a) a regulated agent;

(b) a known consignor;

(c) a haulier appointed in accordance with point 6.6.1.1(c), transporting consignments to which security controls have been previously applied;

(d) neither of the entities referred to in points (a), (b) and (c).

6.1.5 Where point 6.1.4(c) applies, a copy of the signed declaration as contained in Attachment 6-E shall be made available to the regulated agent, air carrier or airport operator granting access into the security restricted areas, unless either of the following applies:

(a) the haulier is itself a regulated agent;

(b) the transport is performed on behalf of the receiving regulated agent or air carrier in the security restricted areas.

The presentation by the haulier of a copy of the signed declaration in Attachment 6-E may be replaced by an equivalent mechanism of prior notification to the access point, ensured either by the off-airport known consignor or regulated agent on whose behalf the transport is performed, or by the receiving regulated agent or air carrier in the security restricted areas.

6.1.6 Cargo or mail consignments to which security controls have not been previously applied may be allowed into the security restricted areas, provided they are subject to the implementation of one of the following options:

(a) screened before entry, in accordance with point 6.2, and under the responsibility of the receiving regulated agent or air carrier;

(b) escorted to the premises of the regulated agent or of the air carrier located in the security restricted areas, under their responsibility.

Upon delivery, such consignments shall be kept protected from unauthorised interference, until they are subjected to screening.

The personnel escorting such consignments or protecting them from unauthorised interference, shall have been recruited in accordance with point 11.1.1, and trained in accordance with at least point 11.2.3.9.

▼B

6.2 SCREENING

6.2.1 **Screening**

6.2.1.1 When screening cargo or mail:

(a) the means or method most likely to detect prohibited articles shall be employed, taking into consideration the nature of the consignment; and

(b) the means or method employed shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the consignment.

6.2.1.2 Where the screener cannot be reasonably sure that no prohibited articles are contained in the consignment, the consignment shall be rejected or be rescreened to the screener's satisfaction.

6.2.1.3 The screening of cargo and mail shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

6.2.1.4 Persons screening cargo by x-ray or EDS equipment shall normally not spend more than 20 minutes continuously reviewing images. After each of these periods, the screener shall not review images for at least 10 minutes. This requirement shall only apply when there is an uninterrupted flow of images to be reviewed.

6.2.1.5 Cargo and mail shall be screened by at least one of the following methods in accordance with Attachment 6-J:

(a) hand search;

(b) x-ray equipment;

(c) EDS equipment;

(d) explosive detection dogs (EDD);

(e) ETD equipment;

(f) visual check;

▼M16

(g) metal detection equipment (MDE);

(h) EVD equipment.

▼M2

_____

▼B

6.2.1.6 If agreed by the appropriate authority and notified to the Commission, other appropriate security controls may be applied only where it is not possible to apply any of the other means or methods specified in point 6.2.1.5 owing to the nature of the consignment.

6.2.2 **Exemptions from screening**

Provisions for exemptions from screening are laid down in Commission Implementing Decision C(2015) 8005.

▼B

6.3 REGULATED AGENTS

6.3.1 **Approval of regulated agents**

6.3.1.1 Regulated agents shall be approved by the appropriate authority.

The approval as a regulated agent shall be site specific.

Any entity that applies security controls as referred to in point 6.3.2 shall be approved as a regulated agent. This includes third party logistics providers responsible for integrated warehousing and transportation services, air carriers and handling agents.

A regulated agent may subcontract one or more of the following:

(a) any of the security controls referred to in point 6.3.2 to another regulated agent;

(b) any of the security controls referred to in point 6.3.2 to another entity, where the controls are carried out at the regulated agent's own site or at an airport, and are covered by the regulated agent's or airport security programme;

(c) any of the security controls referred to in point 6.3.2 to another entity, where the controls are carried out elsewhere than at the regulated agent's own site or at an airport, and the entity has been certified or approved and listed for the provision of these services by the appropriate authority;

(d) the protection and transportation of consignments to a haulier that meets the requirements of point 6.6.

6.3.1.2 The following procedure shall apply for the approval of regulated agents:

(a) the applicant shall seek approval from the appropriate authority of the Member State in which the sites included in the application are located.

The applicant shall submit a security programme to the appropriate authority concerned. The programme shall describe the methods and procedures which are to be followed by the agent in order to comply with the requirements of Regulation (EC) No 300/2008 and its implementing acts. The programme shall also describe how compliance with these methods and procedures is to be monitored by the agent itself. An air carrier security programme which describes the methods and procedures to be followed by the air carrier in order to comply with the requirements of Regulation (EC) No 300/2008 and its implementing acts shall be regarded as meeting the requirement for a regulated agent security programme.

The applicant shall also submit the ‘Declaration of commitments — regulated agent’ as contained in Attachment 6-A. This declaration shall be signed by the applicant's legal representative or by the person responsible for security.

▼M15

The signed declaration shall clearly state the location of the site or sites to which it refers and be retained by the appropriate authority concerned;

▼M12

(b) the appropriate authority or an EU aviation security validator acting on its behalf shall examine the security programme before carrying out an on-site verification of the sites specified in order to assess compliance of the applicant with the requirements of Regulation (EC) No 300/2008 and the implementing acts adopted on its basis.

Except for the screening requirements laid down in point 6.2, an examination of the site of the applicant by the relevant customs authority in accordance with Article 29 of Commission Implementing Regulation (EU) 2015/2447 ([1]) shall be considered as an on-site verification where it is carried out not earlier than 3 years before the date on which the applicant seeks approval as a regulated agent. The AEO authorisation and the relevant assessment of the customs authorities shall be made available by the applicant for further inspection;

▼B

(c) if the appropriate authority is satisfied with the information provided under points (a) and (b), it shall ensure that the necessary details of the agent are entered into the 'Union database on supply chain security' not later than the next working day. When making the database entry the appropriate authority shall give each approved site a unique alphanumeric identifier in the standard format.

If the appropriate authority is not satisfied with the information provided under points (a) and (b) then the reasons shall promptly be notified to the entity seeking approval as a regulated agent;

(d) a regulated agent shall not be considered as approved until its details are listed in the 'Union database on supply chain security'.

6.3.1.3 A regulated agent shall designate at least one person at each site who shall be responsible for the implementation of the submitted security programme. This person shall have successfully completed a background check in accordance with point 11.1.

6.3.1.4 A regulated agent shall be re-validated at regular intervals not exceeding 5 years. This shall include an on-site verification in order to assess whether the regulated agent still complies with the requirements of Regulation (EC) No 300/2008 and its implementing acts.

An inspection at the premises of the regulated agent by the appropriate authority in accordance with its national quality control programme may be considered as an on-site verification, provided that it covers all the requirements necessary for approval.

▼M12

Except for the screening requirements laid down in point 6.2, an examination of the site of the regulated agent by the relevant customs authority carried out in accordance with Article 29 of Implementing Regulation (EU) 2015/2447 shall be considered as an on-site verification.

6.3.1.5 Where the appropriate authority is no longer satisfied that the regulated agent complies with the requirements of Regulation (EC) No 300/2008, it shall withdraw the status of regulated agent for the specified site or sites.

([1]) Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (OJ L 343, 29.12.2015, p. 558).

▼M12

Immediately after withdrawal, and in all cases within 24 hours of withdrawal, the appropriate authority shall ensure that the former regulated agent's change of status is indicated in the 'Union database on supply chain security'.

Where the regulated agent is no longer a holder of an AEO authorisation referred to in (b) of Article 38(2) of Regulation (EU) No 952/2013 of the European Parliament and of the Council [1] and in Article 33 of Implementing Regulation (EU) 2015/2447 or where its AEO authorisation is suspended due to non-compliance with point (e) of Article 39 of Regulation (EU) No 952/2013 and Article 28 of Implementing Regulation (EU) 2015/2447, the appropriate authority shall take appropriate action to ensure compliance of the regulated agent with the requirements of Regulation (EC) No 300/2008.

The regulated agent shall inform the appropriate authority of any changes related to its AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Regulation (EU) 2015/2447.

▼B

6.3.1.6 Without prejudice to the right of each Member State to apply more stringent measures in accordance with Article 6 of Regulation (EC) No 300/2008, a regulated agent approved in accordance with point 6.3 of this Annex shall be recognised in all Member States.

6.3.1.7 The requirements of point 6.3.1, other than 6.3.1.2(d), shall not apply when the appropriate authority itself is to be approved as a regulated agent.

▼M12

6.3.1.8 The appropriate authority shall make available to the customs authority any information related to the status of a regulated agent which could be relevant to the holding an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447. That information shall include the information related to new approvals of regulated agents, withdrawal of the regulated agent status, revalidation and inspections, verification schedules and outcomes of those assessments.

The modalities for that exchange of information shall be established between the appropriate authority and the national customs authorities.

▼B

6.3.2 **Security controls to be applied by a regulated agent**

▼M15

6.3.2.1 When accepting any consignments, a regulated agent shall establish whether the entity from which it receives the consignments is a regulated agent or a known consignor or neither of those.

▼M2

6.3.2.2 The regulated agent or air carrier shall ask the person delivering any consignments to present an identity card, passport, driving licence or other document, which includes his or her photograph and which has been issued or is recognised by the national authority. The card or document shall be used to establish the identity of the person delivering the consignments.

▼B

6.3.2.3 The regulated agent shall ensure that consignments to which not all required security controls have previously been applied are:

▼M15

(a) screened in accordance with point 6.2 or 6.7, as appropriate; or

[1] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (OJ L 269, 10.10.2013, p. 1).

▼B

(b) accepted for storage under the regulated agent's exclusive responsibility, not identifiable as shipment for carriage on an aircraft before selection, and selected autonomously without any intervention of the consignor or any person or entity other than those appointed and trained by the regulated agent for that purpose.

Point (b) may only be applied if it is unpredictable for the consignor that the consignment is to be transported by air.

▼M2

6.3.2.4 After the security controls referred to in points from 6.3.2.1 to 6.3.2.3 of this Annex and point 6.3 of the Annex to Commission Implementing Decision C(2015) 8005 have been applied, the regulated agent shall ensure the protection of cargo and mail in accordance with point 6.6.

▼B

6.3.2.5 After the security controls referred to in points 6.3.2.1 to 6.3.2.4 have been applied, the regulated agent shall ensure that any consignment tendered to an air carrier or another regulated agent is accompanied by appropriate documentation, either in the form of an air waybill or in a separate declaration and either in an electronic format or in writing.

6.3.2.6 The documentation referred to in point 6.3.2.5 shall be available for inspection by the appropriate authority at any point before the consignment is loaded on to an aircraft and afterwards for the duration of the flight or for 24 hours, whichever is the longer and shall provide all of the following information:

(a) the unique alphanumeric identifier of the regulated agent as received from the appropriate authority;

(b) a unique identifier of the consignment, such as the number of the (house or master) air waybill;

(c) the content of the consignment, except for consignments listed in points 6.2.1(d) and (e) of Commission Implementing Decision C(2015) 8005;

▼M15

(d) the security status of the consignment, stating one of the following:

— ‘SPX’, meaning secure for passenger, all-cargo and all-mail aircraft;

— ‘SHR’, meaning secure for passenger, all-cargo and all-mail aircraft in accordance with high risk requirements;

▼M2

(e) the reason why the security status was issued, stating:

(i) ‘KC’, meaning received from known consignor; or

▼M15

_____

▼M2

(iii) ‘RA’, meaning selected by a regulated agent; or

▼M16

(iv) the means or method of screening used, as follows:

— hand search (PHS);

— X-ray equipment (XRY);

— EDS equipment (EDS);

— explosive detection dogs (EDD);

— ETD equipment (ETD);

▼M16

— visual check (VCK);

— metal detection equipment (CMD);

— EVD equipment (EVD);

— any other method (AOM) in accordance with point 6.2.1.6 where the method used shall be specified; or

▼M2

(v) the grounds for exempting the consignment from screening;

▼B

(f) the name of the person who issued the security status, or an equivalent identification, and the date and time of issue;

▼M12

(g) the unique identifier received from the appropriate authority, of any regulated agent who has accepted the security status given to a consignment by another regulated agent, including during transfer operations.

▼B

A regulated agent tendering consignments to another regulated agent or air carrier may also decide to only transmit the information required under points (a) to (e) and (g) and to retain the information required under point (f) for the duration of the flight(s) or for 24 hours, whichever is the longer.

▼M12

Transfer cargo or mail for which the air carrier, or the regulated agent operating on its behalf, is unable to confirm in the accompanying documentation the information required by this point, or by point 6.3.2.7 as applicable, shall be subject to screening before being loaded on board an aircraft for the subsequent flight.

▼B

6.3.2.7 In the case of consolidations, the requirements of points 6.3.2.5 and 6.3.2.6 shall be considered as met if:

(a) the regulated agent performing the consolidation retains the information required under points 6.3.2.6(a) to (g) for each individual consignment for the duration of the flight(s) or for 24 hours, whichever is the longer; and

(b) the documentation accompanying the consolidation includes the alphanumeric identifier of the regulated agent who performed the consolidation, a unique identifier of the consolidation and its security status.

Point (a) shall not be required for consolidations that are always subject to screening or exempted from screening in line with points 6.2.1(d) and (e) of Commission Implementing Decision C(2015) 8005 if the regulated agent gives the consolidation a unique identifier and indicates the security status and a single reason why this security status was issued.

6.3.2.8 When accepting consignments to which not all required security controls have previously been applied, the regulated agent may also elect not to apply the security controls as referred to in point 6.3.2, but to hand the consignments over to another regulated agent to ensure the application of these security controls.

▼B

6.3.2.9 ►M15 A regulated agent shall ensure that all staff are recruited in accordance with the requirements of Chapter 11 and appropriately trained in accordance with the relevant job specifications. For the purposes of training, staff with unsupervised access to identifiable air cargo or identifiable air mail to which the required security controls have been applied shall be considered as staff implementing security controls. Persons previously trained in accordance with point 11.2.7 shall have their competences upgraded to those referred to in point 11.2.3.9 by 1 January 2023 at the latest. ◄

Security controls to be applied by a regulated agent shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

6.4 KNOWN CONSIGNORS

6.4.1 **Approval of known consignors**

6.4.1.1 Known consignors shall be approved by the appropriate authority.

The approval as a known consignor shall be site specific.

6.4.1.2 The following procedure shall apply for the approval of known consignors:

▼M2

(a) the applicant shall seek approval from the appropriate authority of the Member State in which its site is located.

The applicant shall submit a security programme to the appropriate authority concerned. The programme shall describe the methods and procedures which are to be followed by the consignor in order to comply with the requirements of Regulation (EC) No 300/2008 and its implementing acts. The programme shall also describe how compliance with these methods and procedures is to be monitored by the consignor itself.

The applicant shall be provided with the 'Guidance for known consignors' as contained in Attachment 6-B and the 'Validation checklist for known consignors' as contained in Attachment 6-C;

(b) the appropriate authority, or EU aviation security validator acting on its behalf, shall examine the security programme and then make an on-site verification of the sites specified in order to assess whether the applicant complies with the requirements of Regulation (EC) No 300/2008 and its implementing acts.

In order to assess whether the applicant complies with these requirements, the appropriate authority, or EU aviation security validator acting on its behalf, shall make use of the 'Validation checklist for known consignors' as contained in Attachment 6-C. This checklist includes a declaration of commitments which shall be signed by the applicant's legal representative or by the person responsible for security at the site.

Once the validation checklist is completed, the information contained in the checklist shall be handled as classified information.

▼M2

The signed declaration shall be retained by the appropriate authority concerned or retained by the EU aviation security validator and made available to the appropriate authority concerned;

▼M12

(c) an examination of the site of the applicant by the relevant customs authority in accordance with Article 29 of Implementing Regulation (EU) 2015/2447 shall be considered as an on-site verification where it is carried out not earlier than 3 years before the date on which the applicant seeks approval as a known consignor. In those cases, the applicant shall complete the information required in Part One of the 'Validation checklist for known consignors' as contained in Attachment 6-C and send it to the appropriate authority jointly with the declaration of commitments which shall be signed by the applicant's legal representative or by the person responsible for security at the site.

The AEO authorisation and the relevant assessment of the customs authorities shall be made available by the applicant for further inspection.

The signed declaration shall be retained by the appropriate authority concerned or retained by the EU aviation security validator and made available on request to the appropriate authority concerned;

▼B

(d) if the appropriate authority is satisfied with the information provided under points (a) and (b) or (a) and (c), as applicable, it shall ensure that the necessary details of the consignor are entered into the 'Union database on supply chain security' not later than the next working day. When making the database entry the appropriate authority shall give each approved site a unique alphanumeric identifier in the standard format.

If the appropriate authority is not satisfied with the information provided under points (a) and (b) or (a) and (c), as applicable, then the reasons shall promptly be notified to the entity seeking approval as a known consignor;

(e) a known consignor shall not be considered as approved until its details are listed in the 'Union database on supply chain security'.

6.4.1.3 A known consignor shall designate at least one person at each site who shall be responsible for the application and supervision of the implementation of security controls at that site. This person shall have successfully completed a background check in accordance with point 11.1.

6.4.1.4 A known consignor shall be re-validated at regular intervals not exceeding 5 years. This shall include an on-site verification in order to assess whether the known consignor still complies with the requirements of Regulation (EC) No 300/2008 and its implementing acts.

An inspection at the premises of the known consignor by the appropriate authority in accordance with its national quality control programme may be considered as an on-site verification, provided that it covers all areas specified in the checklist of Attachment 6-C.

▼M12

An examination of the site of the known consignor by the relevant customs authority in accordance with Article 29 of Implementing Regulation (EU) 2015/2447 shall be considered as an on-site verification.

▼M12

6.4.1.5 Where the appropriate authority is no longer satisfied that the known consignor complies with the requirements of Regulation (EC) No 300/2008, it shall withdraw the status of known consignor for the specified site(s).

Immediately after withdrawal, and in all cases within 24 hours of withdrawal, the appropriate authority shall ensure that the known consignor's change of status is indicated in the 'Union database on supply chain security'.

Where the known consignor is no longer a holder of an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447 or where its AEO authorisation is suspended due to non-compliance with point (e) of Article 39 of Regulation (EU) No 952/2013 and Article 28 of Implementing Regulation (EU) 2015/2447, the appropriate authority shall take appropriate action to ensure compliance of the known consignor with the requirements of Regulation (EC) No 300/2008.

The known consignor shall inform the appropriate authority of any changes related to its AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447.

▼B

6.4.1.6 Without prejudice to the right of each Member State to apply more stringent measures in accordance with Article 6 of Regulation (EC) No 300/2008, a known consignor approved in accordance with point 6.4 of this Annex shall be recognised in all Member States.

▼M2

_____

▼M12

6.4.1.7 The appropriate authority shall make available to the customs authority any information related to the status of a known consignor which could be relevant to the holding an AEO authorisation referred to in point (b) of Article 38(2) of Regulation (EU) No 952/2013 and in Article 33 of Implementing Regulation (EU) 2015/2447. That information shall include the information related to new approvals of known consignors, withdrawal of the known consignor status, revalidation and inspections, verification schedules and outcomes of those assessments.

The modalities for that exchange of information shall be established between the appropriate authority and the national customs authorities.

▼B

6.4.2 **Security controls to be applied by a known consignor**

6.4.2.1 A known consignor shall ensure that:

(a) there is a level of security on the site or at the premises sufficient to protect identifiable air cargo and identifiable air mail from unauthorised interference; and

▼M15

(b) all staff implementing security controls and all staff with unsupervised access to identifiable air cargo or identifiable air mail to which the required security controls have been applied are recruited in accordance with the requirements of Chapter 11 and have received security training in accordance with point 11.2.3.9. Persons previously trained in accordance with point 11.2.7 shall have their competences upgraded to those referred to in point 11.2.3.9 by 1 January 2023 at the latest; and

▼B

(c) during production, packing, storage, despatch and/or transportation, as appropriate, identifiable air cargo and identifiable air mail is protected from unauthorised interference or tampering.

When, for whatever reason, these security controls have not been applied to a consignment, or where the consignment has not been originated by the known consignor for its own account, the known consignor shall clearly identify this to the regulated agent so that point 6.3.2.3 can be applied.

6.4.2.2 The known consignor shall accept that consignments to which the appropriate security controls have not been applied are screened in accordance with point 6.2.1.

▼M15

6.5 APPROVED HAULIERS

No provisions in this Regulation.

▼B

6.6 PROTECTION OF CARGO AND MAIL

6.6.1 **Protection of cargo and mail during transportation**

▼M15

6.6.1.1 In order to ensure that consignments to which the required security controls have been applied are protected from unauthorised interference during transportation, all the following requirements shall apply:

(a) the consignments shall be packed or sealed by the regulated agent or known consignor so as to ensure that any tampering would be evident; where this is not possible, alternative protection measures that ensure the integrity of the consignment shall be taken;

(b) the cargo load compartment of the vehicle in which the consignments are to be transported shall be locked or sealed or curtain sided vehicles shall be secured with TIR cords so as to ensure that any tampering would be evident, or the load area of flatbed vehicles shall be kept under observation;

(c) the haulier declaration as contained in Attachment 6-E shall be agreed by the haulier who has entered into the transport agreement with the regulated agent or known consignor, unless the haulier is itself approved as a regulated agent.

The signed declaration shall be retained by the regulated agent or known consignor on whose behalf the transport is carried out. On request, a copy of the signed declaration shall also be made available to the regulated agent or air carrier receiving the consignment or to the appropriate authority concerned.

As an alternative to point (c) of the first paragraph, the haulier may provide evidence to the regulated agent or known consignor for whom it provides transport that it has been certified or approved by an appropriate authority.

This evidence shall include the requirements contained in Attachment 6-E and copies shall be retained by the regulated agent or known consignor concerned. On request, a copy shall also be made available to the regulated agent or air carrier receiving the consignment or to another appropriate authority.

▼B

6.6.1.2 Point 6.6.1.1(b) and (c) shall not apply during airside transportation.

▼M12

6.6.1.3 The haulier shall ensure that staff collecting, carrying, storing and delivering air cargo and mail to which security controls have been applied undergoes at least the following:

(a) a check of the personal integrity, consisting of the verification of the identity and of the curriculum vitae and/or provided references;

(b) general security awareness training, in accordance with point 11.2.7.

6.6.1.4 Any of the haulier's staff granted unsupervised access to cargo and mail while performing any of the functions referred to in point 6.6.1.3, or while implementing any of the security controls set out in this Chapter shall:

(a) have successfully completed a background check;

(b) undergo security training, in accordance with point 11.2.3.9.

6.6.1.5 Where a haulier uses the services of another company to perform one or more of the functions referred to in point 6.6.1.3, such other company shall fulfil the following conditions:

(a) sign a haulier agreement with the haulier;

(b) refrain from subcontracting further;

(c) implement the provisions of points 6.6.1.3 and 6.6.1.4, as applicable.

The subcontracting haulier retains full responsibility for the entire transport on behalf of the agent or consignor.

▼B

6.6.2 **►M2 Protection for cargo and mail during handling, storage, and loading onto an aircraft ◄**

6.6.2.1 Consignments of cargo and mail that are in a critical part shall be considered as protected from unauthorised interference.

▼M2

6.6.2.2 Consignments of cargo and mail in a part other than a critical part of a security restricted area shall be protected from unauthorised interference until they are handed over to another regulated agent or air carrier. Consignments shall be located in the access-controlled parts of a regulated agent's premises or, whenever located outside of such parts, shall be considered as protected from unauthorised interference if:

(a) they are physically protected so as to prevent the introduction of a prohibited article; or

(b) they are not left unattended and access is limited to persons involved in the protection and loading of cargo and mail onto an aircraft.

▼B

6.7 HIGH RISK CARGO AND MAIL (HRCM)

Provisions for high risk cargo and mail are laid down in Commission Implementing Decision C(2015) 8005.

6.8 SECURITY PROCEDURES FOR CARGO AND MAIL BEING CARRIED INTO THE UNION FROM THIRD COUNTRIES

▼B

6.8.1 **Designation of air carriers**

6.8.1.1 Any air carrier carrying cargo or mail from an airport in a third country not listed in Attachments 6-Fi or 6-Fii for transfer, transit or unloading at any airport falling within the scope of Regulation (EC) No 300/2008 shall be designated as an 'Air Cargo or Mail Carrier operating into the Union from a Third Country Airport' (ACC3) by one of the following authorities as appropriate:

(a) by the appropriate authority of the Member State that issued the air carrier's Air Operator's Certificate;

(b) by the appropriate authority of the Member State listed in the Annex to Commission Regulation (EC) No 748/2009 [1], for air carriers that do not hold an Air Operator's Certificate issued by a Member State;

(c) by the appropriate authority of the Member State where the air carrier has its major base of operations in the Union, or any other appropriate authority of the Union by agreement with that appropriate authority, for air carriers not holding an Air Operator's Certificate issued by a Member State and not listed in the Annex to Regulation (EC) No 748/2009.

6.8.1.2 The designation of an air carrier as ACC3 in respect of its cargo and mail operations from an airport for which ACC3 designation is required (hereafter, the 'relevant cargo operations') shall be based on:

(a) the nomination of a person with overall responsibility on the air carrier's behalf for the implementation of cargo or mail security provisions in respect of the relevant cargo operation; and

(b) an EU aviation security validation report confirming the implementation of security measures.

6.8.1.3 The appropriate authority shall allocate to the designated ACC3 a unique alphanumeric identifier in the standard format identifying the air carrier and the third country airport for which the air carrier has been designated to carry cargo or mail into the Union.

6.8.1.4 The designation shall be valid from the date the appropriate authority has entered the ACC3's details into the Union database on supply chain security, for a maximum period of five years.

6.8.1.5 An ACC3 listed on the Union database on supply chain security shall be recognised in all Member States for all operations from the third country airport into the Union.

▼M7

6.8.1.6 Following the notification by the United Kingdom of Great Britain and Northern Ireland of its intention to withdraw from the European Union pursuing Article 50 of the TEU, the ACC3 designations issued by this Member State are subject to the following provisions:

(a) The responsibility for the current designations is transferred to the appropriate authority of the Member State listed in the Annex to Commission Regulation (EC) No 748/2009, as amended for the purposes of the withdrawal of the United Kingdom from the Union.

[1] Commission Regulation (EC) No 748/2009 of 5 August 2009 on the list of aircraft operators which performed an aviation activity listed in Annex I to Directive 2003/87/EC on or after 1 January 2006 specifying the administering Member State for each aircraft operator (OJ L 219, 22.8.2009, p. 1).

▼M7

(b) The responsibility for ACC3 designations of air carriers not listed in the Annex to Commission Regulation (EC) No 748/2009, as amended, is transferred to the appropriate authority as identified in point 6.8.1.1 (c).

(c) The appropriate authority of the Member State as described in points (a) and (b) may agree with its counterpart in another Member State, for the latter to accept responsibility for the ACC3 designation of a given air carrier. In doing so, the concerned Member States shall promptly inform the Commission.

(d) The Commission will inform the appropriate authority of the United Kingdom about the Member States taking over the responsibility of its ACC3 designations.

(e) The appropriate authority of the United Kingdom shall make available to the appropriate authority of the receiving Member State, copy of the necessary documentation on which basis it had designated the air carriers listed in point (a) as ACC3. This shall include, at least, the complete validation report, the security programme and if applicable, the roadmap that was agreed with the relevant air carrier.

(f) Provided the obligations in point (e) are satisfied, the transfer of responsibility for ACC3 designations shall occur on the day of withdrawal of the United Kingdom from the European Union.

(g) ACC3 designations of air carriers operating exclusively to the United Kingdom shall be discontinued.

(h) ACC3 designations transferred shall remain valid until their expiry and the receiving Member State takes over the responsibilities and obligations described in this Regulation.

(i) The Commission will facilitate the administrative transition including the listing of the ACC3 details into the Union database on supply chain security.

▼M11

6.8.1.7 ►M12 During the period from 1 April 2020 to 30 June 2021, the appropriate authority may derogate from the process established in point 6.8.2 and temporarily designate an air carrier as ACC3, in the case where an EU aviation security validation could not take place for objective reasons which are related to the pandemic crisis caused by the COVID-19 and are beyond the responsibility of the air carrier. The designation shall be subject to the following conditions: ◄

(a) the air carrier holds an active ACC3 status at the relevant third country location, or has held an ACC3 status, provided it has not expired before 1 February 2020;

(b) the air carrier applies for the new status to the appropriate authority as identified in point 6.8.1.1 or holding the responsibility for the designation due to expire, confirming the existence of objective reasons beyond the responsibility of the air carrier that impede or delay the fulfilment of the requirements of point 6.8.2;

(c) the air carrier submits its security programme that is relevant and complete in respect of all points set out in Attachment 6-G, or confirms that the current programme is still up to date;

(d) the air carrier submits a signed declaration where it confirms the commitment to continue the full and effective implementation of security requirements for which it had obtained the current or expired ACC3 status;

▼M11

(e) the designation of an air carrier as ACC3 under this point is granted for a period not exceeding six months from the date of the current or previous expiry, as appropriate;

(f) the application, the air carrier security programme and the declaration of commitment are submitted either in writing or in electronic format.

6.8.1.8 Where applicable, the appropriate authority may agree with the relevant air carrier the postponement of the annual EU aviation security validations referred to in point 6.8.2.2 (2) (d), by adding them to the number of airports to be validated during the next year of the air carrier's roadmap.

6.8.1.9 Within the temporary designation period referred to in point 6.8.1.7, the appropriate authority shall perform at the Member State's airport or airports of arrival from the ACC3 location, at least three compliance monitoring activities in respect of the security controls applied by the ACC3 and the RA3 and KC3 parts of its supply chain. In the absence of direct flights operated by the ACC3 into the designating Member State, the performance of compliance monitoring activities shall be coordinated with another Member State where the ACC3 operates into.

▼B

6.8.2 **EU aviation security validation for ACC3**

6.8.2.1 The EU aviation security validation in respect of an air carrier's relevant cargo operations shall consist of:

(a) an examination of the air carrier's security programme ensuring its relevance and completeness in respect of all points set out in Attachment 6-G; and

(b) verification of the implementation of aviation security measures in respect of the relevant cargo operations by using the checklist set out in Attachment 6-C3.

6.8.2.2 The EU aviation security validation's verification of the implementation shall be on-site, to one of the following degrees:

(1) At the airport from which the air carrier has relevant cargo operations before ACC3 designation can be granted for that airport.

If the EU aviation security validation thereupon establishes the non-implementation of one or more of the objectives listed in the checklist set out in Attachment 6-C3, the appropriate authority shall not designate the air carrier as ACC3 for the relevant cargo operations without proof of the implementation of measures by the air carrier rectifying the deficiency identified.

(2) At a representative number of airports with relevant cargo operations of an air carrier before ACC3 designation is granted for all airports with relevant cargo operations of that air carrier. The following conditions apply:

(a) this option is requested by an air carrier which operates several relevant air cargo operations; and

(b) the appropriate authority has verified that the air carrier applies an internal security quality assurance programme that is equivalent to EU aviation security validation; and

▼B

(c) the representative number shall be at least 3 or 5 %, whichever is the higher, and all airports situated in a high risk origin; and

(d) the appropriate authority has agreed to a roadmap that ensures EU aviation security validations for every year of the designation at additional airports for which ACC3 designation will be granted or until all airports are validated. Those validations shall each year be at least equal in number to those required in (c). The roadmap shall state the reasons underpinning the choice of additional airports; and

(e) all ACC3 designations shall end on the same day; and

(f) where one of the EU aviation security validations agreed under the roadmap establishes the non-implementation of one or more of the objectives listed in the checklist set out in Attachment 6-C3, the designating appropriate authority shall require proof of the implementation of measures rectifying the deficiency identified at that airport, and, depending on the seriousness of the deficiency, request:

— EU aviation security validation of all airports for which ACC3 designation is required in accordance with point 6.8.2.2.1 within a deadline set by the appropriate authority, or

— twice the number of the EU aviation security validations established under (d) per each of the remaining years of ACC3 designations.

▼M2

6.8.2.3 The appropriate authority may accept the EU aviation security validation report of a third country entity, or of another ACC3, for ACC3 designation in cases where that entity or ACC3 carries out the entire cargo operation, including loading into the hold of the aircraft, on behalf of the applicant ACC3 and the EU aviation security validation report covers all these activities.

6.8.2.4 The EU aviation security validation shall be recorded in a validation report consisting at least of the declaration of commitments as set out in Attachment 6-H1, the checklist set out in Attachment 6-C3 and a declaration by the EU aviation security validator as set out in Attachment 11-A. The EU aviation security validator shall submit the validation report to the appropriate authority and provide the validated air carrier with a copy.

———————

▼B

6.8.3 **Security controls for cargo and mail arriving from a third country**

▼M2

6.8.3.1 The ACC3 shall ensure that all cargo and mail carried for transfer, transit or unloading at a Union airport is screened, unless:

▼M2

(a) the required security controls have been applied to the consignment by an EU aviation security validated regulated agent (RA3) and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or

(b) the required security controls have been applied to the consignment by an EU aviation security validated known consignor (KC3) and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or

▼M15

_____

▼M2

(d) the consignment is exempted from screening in accordance with point (d) of point 6.1.1 and protected from unauthorised interference from the time that it became identifiable air cargo or identifiable air mail and until loading.

▼M15

_____

▼B

6.8.3.2 Cargo and mail carried into the Union shall be screened by one of the means and methods listed in point 6.2.1 to a standard sufficient to reasonably ensure that it contains no prohibited articles.

6.8.3.3 The ACC3 shall ensure in respect of:

(a) transfer and transit cargo or mail that screening in accordance with point 6.8.3.2 or security controls have been applied by itself or by an EU aviation security validated entity at the point of origin or elsewhere in the supply chain and such consignments have been protected from unauthorised interference from the time that those security controls were applied and until loading; and

(b) high risk cargo and mail that screening in accordance with point 6.7 has been applied by itself or by an EU aviation security validated entity at the point of origin or elsewhere in the supply chain, that such consignments have been labelled SHR and have been protected from unauthorised interference from the time that those security controls were applied and until loading.

▼M2

6.8.3.4 When tendering consignments to which it has applied the required security controls to another ACC3 or RA3, the ACC3, RA3, or KC3 shall indicate in the accompanying documentation the unique alpha-numeric identifier received from the designating appropriate authority.

6.8.3.5 When accepting any consignments, an ACC3 or RA3 shall establish whether the air carrier or the entity from which it receives the consignments is another ACC3, RA3, or KC3 by the following means of:

(a) verifying whether or not the unique alphanumeric identifier of the entity delivering the consignments is indicated on the accompanying documentation; and

(b) confirming that the air carrier or entity delivering the consignment is listed as active in the Union database on supply chain security for the specified airport or site, as appropriate.

▼M2

If there is no indication on the accompanying documentation of the identifier, or if the air carrier or entity delivering the consignments is not listed as active in the Union database on supply chain security, it shall be deemed that no security controls have previously been applied, and the consignments shall be screened by the ACC3 or by another EU aviation security validated RA3 before being loaded onto the aircraft.

▼M12

6.8.3.6 After the security controls referred to in points 6.8.3.1 to 6.8.3.5 have been implemented, the ACC3 or the EU aviation security validated regulated agent (RA3) responsible for the application of the security controls, shall ensure that the accompanying documentation, in the form of an air waybill, an equivalent postal documentation or in a separate declaration, provided in an electronic format or in writing, includes at least the following information:

(a) the unique alphanumeric identifier of the ACC3;

(b) the security status of the consignment referred to in point (d) of point 6.3.2.6 and issued by the ACC3 or by the EU aviation security validated regulated agent (RA3), as appropriate;

(c) the unique identifier of the consignment, such as the number of the house or master air waybill, where applicable;

(d) the content of the consignment, or indication of consolidation where applicable;

(e) the reasons for issuing the security status, including the means or method of screening used or the grounds for exempting the consignment from screening, using the standards adopted in the ICAO Consignment Security Declaration scheme.

In the case of consolidations, the ACC3 or the EU aviation security validated regulated agent (RA3) who has performed the consolidation shall retain the information set out in points (a) to (e) of the first paragraph for each individual consignment at least until the estimated time of arrival of the consignments at the first airport in the Union or for 24 hours, whichever period is longer.

6.8.3.7 Any air carrier arriving from a third country listed in Attachment 6-F shall ensure compliance with the applicable points laid down in point 6.8.3.6 in respect of cargo and mail transported on board. The accompanying documentation regarding such consignments shall at least comply with the ICAO Consignment Security Declaration scheme or with an alternative scheme providing the required information in an equivalent manner.

▼M5

6.8.3.8 Transit or transfer consignments arriving from a third country listed in Attachment 6-I whose accompanying documentation does not comply with point 6.8.3.6 shall be treated in accordance with Chapter 6.7 before the subsequent flight.

▼M12

6.8.3.9 Transit or transfer consignments arriving from a third country not referred to in point 6.8.3.8 the accompanying documentation of which does not comply with point 6.8.3.6, shall be treated in accordance with point 6.2 before the subsequent flight.

▼M15

6.8.3.10 Security controls for cargo and mail arriving from a third country shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

▼M2

6.8.4 **Designation of regulated agents and known consignors**

6.8.4.1 Third country entities being, or intending to be, part of the supply chain of an air carrier holding the status of ACC3, may be designated as

▼M2

either ‘third country regulated agent’ (RA3) or ‘third country known consignor’ (KC3).

6.8.4.2 To obtain designation, the entity shall address the request to:

(a) the appropriate authority of the Member State responsible for the ACC3 designation of an air carrier at the third country airport where the applicant handles EU bound cargo; or

(b) where there is no ACC3 designated air carrier in that country, the appropriate authority of the Member State responsible for the approval of the EU aviation security validator performing, or having performed, the validation.

The appropriate authority receiving the request shall start the designation process, or agree with the appropriate authority of another Member State on its delegation, taking into account political or aviation cooperation, or both.

6.8.4.3 Before designation, the eligibility to obtain RA3 or KC3 status in accordance with point 6.8.4.1 shall be confirmed.

6.8.4.4 The designation of an entity as RA3 or KC3 in respect of its cargo and mail operations (‘relevant cargo operations’) shall be based on the following:

(a) the nomination of a person with overall responsibility on the entity's behalf for the implementation of cargo or mail security provisions in respect of the relevant cargo operation; and

(b) an EU aviation security validation report confirming the implementation of security measures.

6.8.4.5 The appropriate authority shall allocate to the designated RA3 or KC3 a unique alphanumeric identifier in the standard format identifying the entity and the third country for which it has been designated to implement security provisions in respect of cargo or mail bound for the Union.

6.8.4.6 The designation shall be valid from the date the appropriate authority has entered the entity's details into the Union database on supply chain security, for a maximum period of three years.

6.8.4.7 An entity listed as RA3 or KC3 on the Union database on supply chain security shall be recognised in all Member States for operations conducted in respect of cargo or mail transported from the third country airport into the Union by an ACC3.

6.8.4.8 Designations of RA3 and KC3 issued before 1 June 2017 shall expire five years after their designation or on 31 March 2020, whichever date comes earlier.

6.8.4.9 Upon request by the appropriate authority of their approval, EU aviation security validators shall make available the details contained in Part 1 of the checklist set out in Attachment 6-C2 or Attachment 6-C4, as appropriate, for each entity they have designated, in order to establish a consolidated list of entities designated by EU aviation security validators.

▼M7

6.8.4.10 Following the notification by the United Kingdom of Great Britain and Northern Ireland of its intention to withdraw from the European Union pursuing Article 50 of the TEU, designations of RA3 and KC3 issued by this Member State are subject to the following provisions:

▼M7

(a) The responsibility for RA3 or KC3 designation of an entity consisting of a branch or a subsidiary company of an airline operator, or of an air carrier itself, is transferred to the appropriate authority of the Member State identified in point 6.8.1.1 of this Regulation;

(b) The responsibility for RA3 or KC3 designation of an entity not directly linked to an air carrier is transferred to the appropriate authority of the Member State identified in point 6.8.1.1 as holding the responsibility for the national or major air carrier of the third country where the RA3 or KC3 operates.

(c) The responsibility for RA3 or KC3 designation of an entity not falling under points (a) or (b), is transferred to the appropriate authority of the Member State identified in point 6.8.1.1 as holding the responsibility for one of the Union air carriers operating from the airport where the RA3 or KC3 operates, or the closest airport to the site of this entity.

(d) The appropriate authority of the Member State as described in points (a) to (c) may agree with its counterpart in another Member State, for the latter to accept responsibility for the RA3 or KC3 designation of a given entity or airline operator. In doing so, the concerned Member States shall promptly inform the Commission.

(e) The Commission will inform the appropriate authority of the United Kingdom about the Member States taking over the responsibility of its RA3 and KC3 designations.

(f) The appropriate authority of the United Kingdom shall make available to the appropriate authority of the receiving Member State, copy of the necessary documentation on which basis it had designated an entity or an airline operator as RA3 or KC3. This shall include, at least, the complete validation report and the security programme of the relevant entity or airline operator.

(g) Provided the obligations in point (f) are satisfied, the transfer of responsibility for RA3 and KC3 designations shall occur on the day of withdrawal of the United Kingdom from the European Union.

(h) RA3 and KC3 designations transferred shall remain valid until their expiry and the receiving Member State takes over the responsibilities and obligations described in this Regulation.

(i) The Commission will facilitate the administrative transition including the listing of the RA3 and KC3 details into the Union database on supply chain security.

▼M11

6.8.4.11 ►M12 During the period from 1 April 2020 to 30 June 2021, the appropriate authority may derogate from the process established in point 6.8.5 and temporarily designate a third country entity as RA3 or KC3, in the case where an EU aviation security validation could not take place for objective reasons which are related to the pandemic crisis caused by the COVID-19 and are beyond the responsibility of the entity. The designation shall be subject to the following conditions: ◄

▼M11

(a) the entity holds an active RA3 or KC3 status, or has held a RA3 or KC3 status, provided it has not expired before 1 February 2020;

(b) the entity applies for the new status to the appropriate authority currently holding the responsibility for its designation that is due to expire or has expired, confirming the existence of objective reasons beyond the responsibility of the entity that impede or delay the fulfilment of the requirements of point 6.8.5;

(c) the entity submits its security programme that is relevant and complete in respect of the operations performed, or confirms that the current programme is still up to date;

(d) the entity submits a signed declaration where it confirms the commitment to continue the full and effective implementation of security requirements for which it had obtained the current or expired RA3 or KC3 status;

(e) the designation of an entity as RA3 or KC3 under this point is granted for a period not exceeding six months from the date of the current or previous expiry, as applicable;

(f) the application, the entity's security programme and the declaration of commitment are submitted either in writing or in electronic format.

6.8.4.12 Entities referred to in point 6.8.4.8 whose RA3 or KC3 status expired in the period from 1 February 2020 to 31 March 2020, that because of the objective reasons referred to in point 6.8.4.11 could not undergo the process of EU aviation security validation established in point 6.8.5 and subsequent designation by an appropriate authority as set out in point 6.8.4, may apply for a temporary designation granted by the Commission, subject to the following conditions:

(a) the entity applies for the RA3 or KC3 status to the Commission, confirming the existence of objective reasons beyond its responsibility that impede or delay the fulfilment of the requirements of point 6.8.5;

(b) the entity submits a signed declaration where it confirms both the commitment to continue the full and effective implementation of security requirements for which it had obtained the expired RA3 or KC3 status, and that its security programme is still up to date;

(c) the application and the declaration of commitment are submitted either in writing or in electronic format;

▼M12

(d) the designation is granted for a period not exceeding six months and may be subject to extension within the derogation period as set out in point 6.8.4.11.

▼M2

6.8.5 **Validation of regulated agents and known consignors**

6.8.5.1 In order to be designated as EU aviation security validated regulated agent or known consignor, third country entities shall be validated according to one of the following two options:

▼M2

(a) the ACC3's security programme shall set out details of security controls implemented on its behalf by third country entities from which it accepts cargo or mail directly for carriage into the Union. The EU aviation security validation of the ACC3 shall validate the security controls applied by those entities; or

(b) the third country entities shall submit the relevant cargo handling activities to an EU aviation security validation at intervals not exceeding three years. The EU aviation security validation shall consist of the following:

(i) an examination of the entity's security programme ensuring its relevance and completeness in respect of the operations performed; and

(ii) on-site verification of the implementation of aviation security measures in respect of the relevant cargo operations.

The validation report shall consist of, for third country regulated agents, the declaration of commitments as set out in Attachment 6-H2 and the checklist set out in Attachment 6-C2, and for third country known consignors, the declaration of commitments as set out in Attachment 6-H3 and the checklist set out in Attachment 6-C4. The validation report shall also include a declaration by the EU aviation security validator, as set out in Attachment 11-A.

6.8.5.2 Once the EU aviation security validation according to point (b) of point 6.8.5.1 has been completed, the EU aviation security validator shall submit the validation report to the appropriate authority and provide the validated entity with a copy.

6.8.5.3 A compliance monitoring activity conducted by the appropriate authority of a Member State or by the Commission may be considered as an EU aviation security validation, provided that it covers all areas specified in the checklist set out in Attachment 6-C2 or 6-C4, as appropriate.

6.8.5.4 The ACC3 shall maintain a database giving at least the following information for each regulated agent or known consignor that has been subject to EU aviation security validation in accordance with point 6.8.5.1, from which it directly accepts cargo or mail for carriage into the Union:

(a) the company details, including the bona fide business address; and

(b) the nature of the business, excluding business sensitive information; and

(c) contact details, including those of the person(s) responsible for security; and

(d) the company registration number, if applicable; and

(e) where available, the validation report; and

(f) the unique alphanumeric identifier attributed in the Union database on supply chain security.

▼M15

_____

▼M2

The database shall be available for inspection of the ACC3.

Other EU aviation security validated entities may maintain such a database.

▼M12

_____

▼M2

6.8.6 **Non-compliance and discontinuation of ACC3, RA3 and KC3 designation**

6.8.6.1 *Non-Compliance*

▼**M12**

1. Where the Commission or an appropriate authority identifies or receives written information about a serious deficiency relating to the operations of an ACC3, an RA3 or a KC3, which is deemed to have a significant impact on the overall level of aviation security in the Union, it shall:

   (a) inform the air carrier or entity concerned promptly, request comments and appropriate measures in respect to the serious deficiency;

   (b) promptly inform the other Member States and the Commission.

   The serious deficiency referred to in the first paragraph may be identified during either of the following activities:

   (1) during compliance monitoring activities;

   (2) during the examination of documentation including the EU aviation security validation report of other operators which are part of the supply chain of the ACC3, RA3 or KC3;

   (3) upon receipt of factual written information from other authorities and/or operators in respect of the activities of the concerned ACC3, RA3 or KC3, in form of documented evidence clearly indicating security breaches.

▼**M2**

2. Where the ACC3, the RA3 or the KC3 has not rectified the serious deficiency within a specific time-frame, or in case the ACC3, the RA3 or the KC3 does not react to the request set out in point (a) of point 6.8.6.1, the authority, or the Commission shall:

   (a) deactivate the status as ACC3, RA3 or KC3 of the operator or entity in the Union database on supply chain security; or

   (b) request the appropriate authority responsible for the designation to deactivate the status as ACC3, RA3 or KC3 of the operator or entity in the Union database on supply chain security.

   In the situation referred to in the first paragraph, the authority, or the Commission, shall promptly inform the other Member States and the Commission.

3. An air carrier or entity whose status, respectively as an ACC3, RA3 or KC3, has been deactivated in accordance with point 6.8.6.1.2 shall not be reinstated or included in the Union database on supply chain security until an EU aviation security re-designation in accordance with 6.8.1 or 6.8.4 has taken place.

4. If an air carrier or an entity is no longer a holder of the ACC3, RA3 or KC3 status, the appropriate authorities shall undertake appropriate action to satisfy themselves that other ACC3s, RA3s and KC3s under their responsibility, operating in the supply chain of the air carrier or entity that has lost the status, still comply with the requirements of Regulation (EC) No 300/2008.

6.8.6.2 *Discontinuation*

1. The appropriate authority that designated the ACC3, the RA3 or the KC3, is responsible for removing the details thereof from the ‘Union database on supply chain security’:

   (a) at the request of or in agreement with the air carrier or the entity; or

   (b) where the ACC3, the RA3 or the KC3 does not pursue relevant cargo operations and does not react to a request for comments or otherwise obstructs the assessment of risk to aviation.

▼M2

2. If an air carrier or an entity is no longer a holder of the ACC3, RA3 or KC3 status, the appropriate authorities shall undertake appropriate action to satisfy themselves that other ACC3s, RA3s and KC3s under their responsibility, operating in the supply chain of the air carrier or entity that has been discontinued, still comply with the requirements of Regulation (EC) No 300/2008.

▼M12

6.8.7 **Pre-Loading Advance Cargo Information (PLACI)**

6.8.7.1 Pursuant to Article 186 of Implementing Regulation (EU) 2015/2447, the PLACI shall be carried out before departure from a third country, upon receipt by the customs authority of the first point of entry, of the minimum dataset of the entry summary declaration referred to in Article 106(2) and (2a) of Commission Delegated Regulation (EU) 2015/2446 ([1]).

6.8.7.2 In the course of the PLACI and where there are reasonable grounds for the customs office of first entry to suspect that a consignment entering the customs territory of the Union by air could pose a serious threat to civil aviation, that consignment shall be treated as high risk cargo or mail (HRCM) in accordance with point 6.7. ►M16 An air carrier shall not load for carriage into the Union such consignment, unless the required measures as set out in points 6.8.7.3 and 6.8.7.4, as applicable, have been implemented satisfactorily. ◄

6.8.7.3 The air carrier, operator, entity or person in a third country other than those listed in Attachment 6-F and Iceland, shall, upon receipt of a notification from the customs office of first entry requiring a consignment to be treated as high risk cargo or mail (HRCM) in accordance with point 6.8.7.2:

(a) implement in respect of the specific consignment, the security controls listed in points 6.7.3 and 6.7.4 of the Annex to Implementing Decision C(2015) 8005, in case of an ACC3 or an RA3 approved for the performance of such security controls;

(b) ensure that an ACC3 or an RA3 approved for the performance of such security controls complies with the provisions laid down in point (a). Information to the customs office of first entry shall be provided in case the consignment is to be tendered or it has been tendered to another operator, entity or authority for the application of the security controls. Such other operator, entity or authority shall ensure the implementation of the security controls referred to in point (a) and confirm to the air carrier, operator, entity or person from which the consignment was received, both the implementation of such security controls and the results thereof;

(c) confirm to the customs office of first entry both the implementation of the security controls referred to in point (a) and the results thereof.

Points (a) and (b) of the first paragraph shall not apply in case the requested security controls have been previously implemented. However, should there be specific threat information that has only become available after the implementation of the previous security controls, the air carrier, operator, entity or person may be requested to repeat the security controls by using specific means and methods, and provide confirmation as set out in point (c) of the first paragraph. The air carrier, operator, entity or person may be made aware of any element and information necessary in order to effectively meet the security objective.

([1]) Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code (OJ L 343, 29.12.2015, p. 1).

▼**M12**

6.8.7.4 Air carriers, operators, entities or persons in a third country listed in Attachment 6-F or in Iceland, that receive a notification from the customs office of first entry requiring a consignment to be treated as high risk cargo or mail (HRCM) in accordance with point 6.8.7.2, shall:

(a) implement, in respect of the specific consignment, at least the security controls established by ICAO Annex 17 for High Risk Cargo or Mail ([1]);

(b) ensure that the requirements of point (a) are fulfilled by an operator, entity or authority approved by the relevant appropriate authority in the third country for the performance of such security controls. Information to the customs office of first entry shall be provided in case the consignment is to be tendered or it has been tendered to another operator, entity or authority for the application of the security controls. Such other operator, entity or authority shall ensure the implementation of the security controls referred to in point (a) and confirm to the air carrier, operator, entity or person from which the consignment was received, both the implementation of such security controls and the results thereof;

(c) confirm to the customs office of first entry both the implementation of the security controls referred to in point (a) and the results thereof.

Points (a) and (b) of the first paragraph shall not apply in case the requested security controls have been previously implemented. However, should there be specific threat information that has only become available after the implementation of the previous security controls, the air carrier, operator, entity or person may be requested to repeat the security controls by using specific means and methods, and provide confirmation as set out in point (c) of the first paragraph. The air carrier, operator, entity or person may be made aware of any element and information necessary in order to effectively meet the security objective.

6.8.7.5 In the course of the PLACI and where there are reasonable grounds for the customs office of first entry to suspect that a consignment entering the customs territory of the Union by air poses a serious threat to security, leading it to issue a do not load notification, that consignment shall not be loaded on board of an aircraft, or off-loaded, as applicable.

6.8.7.6 The air carrier, operator, entity or person in a third country that receives a notification from the customs office of first entry requiring a consignment not to be loaded on board of an aircraft in accordance with point 6.8.7.5, shall:

(a) ensure that the consignment in its possession is not loaded on board an aircraft, or it is immediately off-loaded in case the consignment is already on board the aircraft;

(b) provide confirmation that it has fulfilled the request to the customs office of first entry in the customs territory of the Union;

(c) cooperate with the relevant authorities of the Member State of the customs office of first entry;

(d) inform the appropriate authority for civil aviation security of the State where the air carrier, operator, entity or person receiving the notification is located and of the third country where the consignment is currently located, if different.

6.8.7.7 Should the consignment be already with another air carrier, operator or entity along the supply chain, the air carrier, operator, entity or person receiving the do not load notification laid down in point 6.8.7.5 shall immediately inform such other air carrier, operator, entity or person that it shall:

([1]) Air carriers, operators and entities in Iceland shall apply points 6.7.3 and 6.7.4 of the Annex to Implementing Decision C(2015) 8005.

▼**M12**

(a) ensure compliance with the provisions of points (a), (c) and (d) of point 6.8.7.6;

(b) confirm the application of point (b) of point 6.8.7.6 to the air carrier, operator, entity or person that received the notification laid down in point 6.8.7.5.

6.8.7.8 Should the aircraft be already airborne with a consignment on board for which the customs office of first entry had notified, pursuant to point 6.8.7.5, that a consignment must not be loaded, the air carrier, operator, entity or person receiving the notification shall immediately inform:

(a) the relevant authorities of the Member State referred to in point (c) of point 6.8.7.6 for the purpose of informing and liaising with the relevant authorities of the Member State of first overflight in the Union;

(b) the appropriate authority for civil aviation security of the third country where the air carrier, operator, entity or person receiving the notification is located and of the third country from which the flight has departed, if different.

6.8.7.9 Following the notification received from the customs office of first entry that has issued a notification as laid down in point 6.8.7.5, the appropriate authority of the same Member State shall, as applicable, implement or ensure the implementation thereof, or cooperate in any subsequent actions, including the coordination with the authorities of the third country of departure and where applicable in the country or countries of transit and/or transfer, the relevant security contingency protocols in accordance with the Member State's national civil aviation security programme and the international standards and recommended practices regulating crisis management and response to acts of unlawful interference.

6.8.7.10 The air carrier, operator, entity or person in a third country that receives a notification issued by the customs authority of a third country implementing a Pre-Loading Advance Cargo Information scheme in adherence to the principles set out by the World Customs Organisation's SAFE Framework of Standards, shall ensure the implementation of the requirements laid down in points 6.8.7.3 and 6.8.7.4 and in points 6.8.7.6, 6.8.7.7, 6.8.7.8.

This point applies only in respect of consignments of cargo or mail fulfilling any of the criteria below:

(a) they are carried for transit or transfer at a Union airport before reaching the final destination at an airport based in the third country of the notifying customs authority;

(b) they are carried for transit or transfer at a Union airport before having another transit or transfer at an airport based in the third country of the notifying customs authority.

For the purposes of the requirements set out in points 6.8.7.6(c) and 6.8.7.8(a), the air carrier, operator, entity or person receiving the notification in a third country, shall immediately inform the relevant authorities of the Member State of first landing in the Union.

Should the aircraft be already airborne, the information shall be provided to the relevant authorities of the Member State of first overflight in the Union that shall ensure the implementation of the actions referred to in point 6.8.7.9, in coordination with the relevant authorities of the Member State of first landing in the Union.

The relevant authorities of both the Member State of first overflight in the Union and of the Member State of first landing in the Union shall inform the respective customs authority.

▼B

ATTACHMENT 6-A

DECLARATION OF COMMITMENTS — REGULATED AGENT

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council [1] on common rules in the field of civil aviation security and its implementing acts,

I declare that,

— to the best of my knowledge, the information contained in the company's security programme is true and accurate,

— the practices and procedures set out in this security programme will be implemented and maintained at all sites covered by the programme,

— this security programme will be adjusted and adapted to comply with all future relevant changes to Union legislation, unless [name of company] informs [name of appropriate authority] that it no longer wishes to trade as a regulated agent,

— [name of company] will inform [name of appropriate authority] in writing of:

▼M15

(a) minor planned changes to its security programme, such as company name, company address, person responsible for security or contact details, change of person requiring access to the 'Union database on supply chain security', promptly and at least within 7 working days before the planned change; and

▼B

(b) major planned changes, such as new screening procedures, major building works which might affect its compliance with relevant Union legislation or change of site/address, at least 15 working days prior to their commencement/the planned change,

— in order to ensure compliance with relevant Union legislation, [name of company] will cooperate fully with all inspections, as required, and provide access to all documents, as requested by inspectors,

— [name of company] will inform [name of appropriate authority] of any serious security breaches and of any suspicious circumstances which may be relevant to air cargo/air mail security, in particular any attempt to conceal prohibited articles in consignments,

— [name of company] will ensure that all relevant staff receive training in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998 and are aware of their security responsibilities under the company's security programme; and

— [name of company] will inform [name of appropriate authority] if:

(a) it ceases trading;

(b) it no longer deals with air cargo/air mail; or

(c) it can no longer meet the requirements of the relevant Union legislation.

[1] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

▼B

I shall accept full responsibility for this declaration.

Name:

Position in company:

Date:

Signature:

ATTACHMENT 6-B

GUIDANCE FOR KNOWN CONSIGNORS

This guidance will help you to assess your existing security arrangements against the required criteria for known consignors as described in Regulation (EC) No 300/2008 of the European Parliament and of the Council ([1]) and its implementing acts. This should enable you to ensure that you meet the requirements before arranging an official on-site validation visit.

It is important that the validator is able to talk to the right people during the validation visit (e.g. person responsible for security and person responsible for recruitment of staff). An EU checklist will be used to record the validator's assessments. Once the validation checklist is completed, the information contained in the checklist will be handled as classified information.

Please note that questions on the EU checklist are of two types: (1) those where a negative response will automatically mean that you cannot be accepted as a known consignor and (2) those which will be used to build up a general picture of your security provisions to allow the validator to reach an overall conclusion. The areas where a 'fail' will automatically be recorded are indicated by the requirements indicated in bold type below. If there is a 'fail' on the requirements indicated in bold **type**, the reasons will be given to you and advice on adjustments needed to pass.

If you are a holder of an AEO certificate referred to in point (b) or (c) of Article 14a(1) of Commission Regulation (EEC) No 2454/93 ([2]) (so called AEOF and AEOS certificates) and if the site for which you are requesting the known consignor status has been successfully examined by customs authorities at a date not earlier than 3 years before the date of requesting the known consignor status, you are required to fill out and have signed by a legal representative of your company Part 1 concerning the organisation and responsibilities as well as the declaration of commitments of the 'Validation checklist for known consignors' as contained in attachment 6-C.

Introduction

The cargo must be originated by your company on the site to be inspected. This covers manufacture on the site and pick and pack operations where the items are not identifiable as air cargo until they are selected to meet an order. (See also Note.)

You will have **to determine where a consignment of cargo/mail becomes identifiable as air cargo/air mail** and demonstrate that you have the relevant measures in place to protect it from unauthorised interference or tampering. This will include details concerning the production, packing, storage and/or despatch.

([1]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

([2]) Commission Regulation (EEC) No 2454/93 of 2 July 1993 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code (OJ L 253, 11.10.1993, p. 1).

▼B

Organisation and responsibilities

You will be required to provide details about your organisation (name, VAT or Chamber of Commerce number or Corporate registration number if applicable, AEO certificate number and the date of the last examination of this site by customs authorities, if applicable), address of the site to be validated and main address of organisation (if different from the site to be validated). The date of the previous validation visit and last unique alphanumeric identifier (if applicable) are required, as well as of the nature of the business, the approximate number of employees on site, name and title of the person responsible for air cargo/air mail security and contact details.

Staff recruitment procedure

You will be required to provide details of your recruitment procedures for all staff (permanent, temporary or agency staff, drivers) with access to identifiable air cargo/air mail. The recruitment procedure shall include **a pre-employment check or a background check** in accordance with point 11.1 of the Annex to Implementing Regulation (EU) 2015/1998. The on-site validation visit will involve an interview with the person responsible for the recruitment of staff. He/she will need to present evidence (e.g. blank forms) to substantiate the company procedures. This recruitment procedure shall apply to staff recruited after 29 April 2010.

Staff security training procedure

You will need to demonstrate that **all staff** (permanent, temporary or agency staff, drivers) **with access to air cargo/air mail have received the appropriate training on security awareness matters**. This training shall take place in accordance with point 11.2.7 of the Annex to Implementing Regulation (EU) 2015/1998. Individual training records should be kept on file. **In addition, you will be required to show that all relevant staff implementing security controls have received training or recurrent training in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998**.

Physical security

You will be required to demonstrate how your site is protected (e.g. a physical fence or barrier) and that relevant access control procedures are in place. Where applicable, you will be required to provide details of any possible alarm- and/or CCTV system. **It is essential that access to the area where air cargo/air mail is processed or stored, is controlled**. All doors, windows and other points of access to air cargo/air mail need to be secured or subject to access control.

Production (where applicable)

You will need to demonstrate that access to the production area is controlled and the production process supervised. If the product can be identified as air cargo/air mail in the course of production then you will have to show **that measures are taken to protect air cargo/air mail from unauthorised interference or tampering at this stage**.

Packing (where applicable)

You will need to demonstrate that access to the packing area is controlled and the packing process supervised. If the product can be identified as air cargo/air mail in the course of packing then you will have to show **that measures are taken to protect air cargo/air mail from unauthorised interference or tampering at this stage**.

▼B

You will be required to provide details of your packing process and show that all finished goods are checked prior to packing.

You will need to describe the finished outer packing and demonstrate that it is robust. You also have to demonstrate how the finished outer packing is made tamper evident, for example by the use of numbered seals, security tape, special stamps or cardboard boxes fixed by a tape. You also need to show that you hold those under secure conditions when not in use and control their issue.

Storage (where applicable)

You will need to demonstrate that access to the storage area is controlled. If the product can be identified as air cargo/air mail while being stored then you will have to show **that measures are taken to protect air cargo/air mail from unauthorised interference or tampering at this stage**.

Finally, **you will have to demonstrate that finished and packed air cargo/air mail is checked before despatch**.

Despatch (where applicable)

You will need to demonstrate that access to the despatch area is controlled. If the product can be identified as air cargo/air mail in the course of despatch then you will have to show **that measures are taken to protect air cargo/air mail from unauthorised interference or tampering at this stage**.

Transportation

You will have to provide details concerning the method of transportation of cargo/mail to the regulated agent.

If you use your own transport, you will have to demonstrate that your drivers have been trained to the required level. **If a contractor is used by your company, you will have to ensure that a) the air cargo/air mail is sealed or packed by you so as to ensure that any tampering would be evident and b) the haulier declaration as contained in Attachment 6-E of the Annex to Implementing Regulation (EU) 2015/1998 has been signed by the haulier**.

If you are responsible for the transportation of air cargo/air mail, you will have to show that the means of transport **are securable**, either through the use of seals, if practicable, or any other method. Where numbered seals are used, you will have to demonstrate that access to the seals is controlled and numbers are recorded; if other methods are used you will have to show how cargo/mail is made tamper evident and/or kept secure. In addition you will need to show that there are measures in place to verify the identity of the drivers of vehicles collecting your air cargo/air mail. You will also need to show that you ensure that cargo/mail is secure when it leaves the premises. **You will have to demonstrate that air cargo/air mail is protected from unauthorised interference during transportation**.

You will not have to provide evidence about driver training or a copy of the haulier declaration where a regulated agent has made the transport arrangements for collecting air cargo/air mail from your premises.

Consignor's responsibilities

You will need to declare that you will accept unannounced inspections by the appropriate authority's inspectors for the purpose of monitoring these standards.

▼B

You will also need to declare to provide [name of appropriate authority] with the relevant details promptly but at least within 10 working days if:

(a) the overall responsibility for security is assigned to anyone other than the person named

(b) there are any other changes to premises or procedures likely to significantly impact on security

(c) your company ceases trading, no longer deals with air cargo/air mail or can no longer meet the requirements of the relevant EU legislation.

Finally, you will need to declare to maintain standards of security until the subsequent on-site validation visit and/or inspection.

You will then be required to accept full responsibility for the declaration and to sign the validation document.

NOTES:

Explosive and incendiary devices

Assembled explosive and incendiary devices may be carried in consignments of cargo if the requirements of all safety rules are met in full.

Consignments from other sources

A known consignor may pass consignments which it has not itself originated to a regulated agent, provided that:

(a) they are separated from consignments which it has originated; and

(b) the origin is clearly indicated on the consignment or on accompanying documentation.

All such consignments must be screened before they are loaded on to an aircraft.

ATTACHMENT 6-C

VALIDATION CHECKLIST FOR KNOWN CONSIGNORS

Completion notes:

When completing this form please note that:

— Items marked '(*)' are required data and MUST be completed.

— If the answer to any question in **bold type** is **NO**, the validation **MUST** be assessed as a **FAIL**. This does not apply where the questions do not apply.

— The overall assessment can only be assessed as a **PASS** after the consignor has signed the declaration of commitments on the last page.

— The original declaration of commitments must be retained by or made available to the appropriate authority until the validation expires. A copy of the declaration should also be given to the consignor.

▼B

PART 1

Organisation and responsibilities

1.1	Date of validation (*)	
	dd/mm/yyyy	
1.2	Date of previous validation and Unique Identifier where applicable	
	dd/mm/yyyy	
	UNI	
1.3	Name of organisation to be validated (*)	
	Name VAT/Chamber of Commerce number/Corporate registration number (if applicable)	
1.4	Information on AEOF or AEOS certificate, where applicable	
	AEO certificate number	
	Date when customs authorities have last examined this site	
1.5	Address of site to be validated (*)	
	Number/Unit/Building	
	Street	
	Town	
	Postcode	
	Country	
1.6	Main address of organisation (if different from site to be validated, provided that it is in the same country)	
	Number/Unit/Building	
	Street	
	Town	
	Postcode	
	Country	
1.7	Nature of Business(es) — types of cargo processed	

▼B

1.8 Is the applicant responsible for:	
(a) Production (b) Packing (c) Storage (d) Dispatch (e) Other, please specify	
1.9 Approximate number of employees on site	
1.10 Name and title of person responsible for air cargo/air mail security (*)	
Name	
Job title	
1.11 Contact telephone number	
Tel. no.	
1.12 E-mail address (*)	
E-mail	

PART 2

Identifiable air cargo/air mail

Aim: To establish the point (or: place) where cargo/mail becomes identifiable as air cargo/air mail.

2.1 By inspection of the production, packing, storage, selection, despatch and any other relevant areas, ascertain where and how a consignment of air cargo/air mail becomes identifiable as such.
Describe:

NB: **Detailed information should be given on the protection of identifiable air cargo/air mail from unauthorised interference or tampering in Parts 5 to 8.**

PART 3

Staff recruitment and training

Aim: To ensure that all staff (permanent, temporary, agency staff, drivers) with access to identifiable air cargo/air mail have been subject to an appropriate pre-employment check and/or background check as well as trained in accordance with point 11.2.7 of the Annex to Implementing Regulation (EU) 2015/1998. In addition, to ensure that all staff implementing security controls in respect of supplies are trained in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998.

Whether or not 3.1 and 3.2 are questions in **bold type** *(and thus where a NO answer must be assessed as a fail) depends on the applicable national rules of the State where the site is located. However, at least one of these two questions*

▼B

shall be in **bold type**, *whereby it should also be allowed that where a background has been carried out, then a pre-employment check is no longer required. The person responsible for implementing security controls shall always have a background check.*

3.1 **Is there a recruitment procedure for all staff with access to identifiable air cargo/air mail which includes a pre-employment check in accordance with point 11.1.4 of the Annex to Implementing Regulation (EU) 2015/1998?** This applies to staff recruited after 29 April 2010.	
YES or NO	
If YES, which type	
3.2 **Does this recruitment procedure also include a background check, including a check on criminal records, in accordance with point 11.1.3 of the Annex to Implementing Regulation (EU) 2015/1998?** This applies to staff recruited after 29 April 2010.	
YES or NO	
If YES, which type	
3.3 **Does the appointment process for the named person responsible for the application and supervision of the implementation of security controls at the site include a requirement for a background check, including a check on criminal records in accordance with point 11.1.3 of the Annex to Implementing Regulation (EU) 2015/1998?**	
YES or NO	
If YES, describe	

▼M15

3.4 **Do staff with unsupervised access to identifiable air cargo/air mail and staff implementing security controls receive security training in accordance with point 11.2.3.9 before being given unsupervised access to identifiable air cargo/air mail?**	

▼B

YES or NO	
If YES, describe	
3.5 **Do staff (as referred to above) receive refresher training in accordance with the frequency established for this training?**	
YES or NO	
3.6 **Assessment — Are the measures sufficient to ensure that all staff with access to identifiable air cargo/air mail and staff implementing security controls have been properly recruited and trained in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998?**	
YES or NO	
If NO, specify reasons	

▼B

PART 4

Physical security

Aim: To establish if there is a level of (physical) security on the site or at the premises sufficient to protect identifiable air cargo/air mail from unauthorised interference.

4.1 Is the site protected by a physical fence or barrier?	
YES or NO	
4.2 Are all the access points to the site subject to access control?	
YES or NO	
4.3 If YES, are the access points…?	
Staffed	
Manual	
Automatic	
Electronic	
Other, specify	
4.4 Is the building of sound construction?	
YES or NO	
4.5 Does the building have an effective alarm system?	
YES or NO	
4.6 Does the building have an effective CCTV system?	
YES or NO	
4.7 If yes, are the images of the CCTV recorded?	
YES or NO	
4.8 Are all doors, windows and other points of access to identifiable air cargo/air mail secure or subject to access control?	
YES or NO	
4.9 If no, specify reasons	
4.10 **Assessment: Are the measures taken by the organisation sufficient to prevent unauthorised access to those parts of the site and premises where identifiable air cargo/air mail is processed or stored?**	
YES or NO	
If NO, specify reasons	

▼B

PART 5

Production

Aim: To protect identifiable air cargo/air mail from unauthorised interference or tampering.

Answer these questions where the product could be identified as air cargo/air mail in the course of the production process.

5.1 Is access controlled to the production area?	
YES or NO	
5.2 If YES, how?	
5.3 Is the production process supervised?	
YES or NO	
5.4 If YES, how?	
5.5 Are controls in place to prevent tampering at the stage of production?	
YES or NO	
If YES, describe	
5.6 **Assessment: Are measures taken by the organisation sufficient to protect identifiable air cargo/air mail from unauthorised interference or tampering during production?**	
YES or NO	
If NO, specify reasons	

PART 6

Packing

Aim: To protect identifiable air cargo/air mail from unauthorised interference or tampering.

Answer these questions where the product could be identified as air cargo/air mail in the course of the packing process.

6.1 Is the packing process supervised?	
YES or NO	
6.2 If YES, how?	
6.3 Please describe the finished outer packaging:	
(a) Is the finished outer packaging robust?	
YES or NO Describe:	

▼B

(b) Is the finished outer packaging tamper evident?	
YES or NO	
Describe:	
6.4 (a) Are numbered seals, security tape, special stamps or cardboard boxes fixed by a tape used to make air cargo/air mail tamper evident?	
YES or NO	
If YES:	
6.4 (b) Are the seals, security tape or special stamps held under secure conditions when not in use?	
YES or NO	
Describe:	
6.4 (c) Is the issue of numbered seals, security tape, and/or stamps controlled?	
YES or NO	
Describe:	
6.5 If the answer to 6.4 (a) is YES, how is this controlled?	
6.6 **Assessment: Are the packing procedures sufficient to protect identifiable air cargo/air mail from unauthorised interference and/or tampering?**	
YES or NO	
If NO, specify reasons	

PART 7

Storage

Aim: To protect identifiable air cargo/air mail from unauthorised interference or tampering.

Answer these questions where the product could be identified as air cargo/air mail in the course of the storage process.

7.1 Is the finished and packed air cargo/air mail stored securely and checked for tampering?	
YES or NO	
7.2 **Assessment: Are the storage procedures sufficient to protect identifiable air cargo/air mail from unauthorised interference and/or tampering?**	
YES or NO	
If NO, specify reasons	

▼B

PART 8

Despatch

Aim: To protect identifiable air cargo/air mail from unauthorised interference or tampering.

Answer these questions where the product could be identified as air cargo/air mail in the course of the despatch process.

8.1 Is access controlled to the despatch area?	
YES or NO	
8.2 If YES, how?	
8.3 Who has access to the despatch area?	
Employees?	
YES or NO	
Drivers?	
YES or NO	
Visitors?	
YES or NO	
Contractors?	
YES or NO	
8.4 **Assessment: Is the protection sufficient to protect the air cargo/air mail from unauthorised interference or tampering in the despatch area?**	
YES or NO	
If NO, specify reasons	

PART 8A

Consignments from other sources

Aim: to establish the procedures for dealing with unsecured consignments.

Answer these questions only if consignments for carriage by air are being accepted from other companies.

8A.1 **Does the company accept consignments of cargo intended for carriage by air from any other companies?**	
YES OR NO	
8A.2 If YES, how are these kept separate from the company's own cargo and how are they identified to the regulated agent/haulier?	

▼B

PART 9

Transportation

Aim: To protect identifiable air cargo/air mail from unauthorised interference or tampering.

9.1 How is the air cargo/air mail conveyed to the regulated agent?	
(a) By, or on behalf of, the regulated agent?	
YES or NO	
(b) Consignor's own transport?	
YES or NO	
(c) Contractor used by the consignor?	
YES or NO	
9.2 **Where a contractor is used by the consignor:** — **is the air cargo/air mail being sealed or packed before transportation so as to ensure that any tampering would be evident? and** — **has the haulier declaration been signed by the haulier?**	
YES or NO	
Only answer the following questions where 9.1(b) or 9.1(c) applies 9.3 Is the cargo compartment of the transport vehicle securable?	
YES or NO	
If YES, specify how…	
9.4 (a) Where the cargo compartment of the transport vehicle is securable, are numbered seals used?	
YES or NO	
(b) Where numbered seals are used, is access to the seals controlled and the numbers recorded on issue?	
YES or NO	
If YES, specify how…	
9.5 Where the cargo compartment of the transport vehicle is not securable, is the air cargo/air mail tamper evident?	
YES or NO	

▼B

9.6 If YES, describe tamper evidence employed.	
9.7 If NO, how is it kept secure?	
9.8 **Assessment: Are the measures sufficient to protect air cargo/air mail from unauthorised interference during transportation?**	
YES or NO	
If NO, specify reasons	

DECLARATION OF COMMITMENTS

I declare that:

— **I will accept unannounced inspections by the appropriate authority's inspectors for the purpose of monitoring these standards. If the inspector discovers any serious lapses in security, this could lead to the withdrawal of my status as known consignor.**

— **I will provide [name of appropriate authority] with the relevant details promptly but at least within 10 working days if:**

  — **the overall responsibility for security is assigned to anyone other than the person named at point 1.10;**

  — **there are any other changes to premises or procedures likely to significantly impact on security; and**

  — **the company ceases trading, no longer deals with air cargo/air mail or can no longer meet the requirements of the relevant Union legislation.**

— **I will maintain standards of security until the subsequent on-site validation visit and/or inspection.**

— **I shall accept full responsibility for this declaration.**

Signed	
Position in company	

Assessment (and notification)

Pass/Fail	
Where the overall assessment is a fail, list below the areas where the consignor fails to achieve the required standard of security or has a specific vulnerability. Also advice on the adjustments needed to achieve the required standard and thus to pass.	
Signed	
(Name of validator)	

▼M2

ATTACHMENT 6-C2

VALIDATION CHECKLIST FOR THIRD COUNTRY EU AVIATION SECURITY VALIDATED REGULATED AGENTS

Third country entities have the option to become part of an ACC3's (*Air cargo or mail carrier operating into the Union from a third country airport*) secure supply chain by seeking designation as a third country EU aviation security validated regulated agent (RA3). An RA3 is a cargo handling entity located in a third country that is validated and approved as such on the basis of an EU aviation security validation.

An RA3 shall ensure that security controls including screening where applicable have been applied to consignments bound for the Union and the consignments have been protected from unauthorised interference from the time that those security controls were applied and until the consignments are loaded onto an aircraft or are otherwise handed over to an ACC3 or other RA3.

The prerequisites for carrying air cargo or air mail into the Union [1] or Iceland, Norway and Switzerland are provided for in Implementing Regulation (EU) 2015/1998.

The checklist is the instrument to be used by the EU aviation security validator for assessing the level of security applied to EU or EEA bound air cargo or air mail [2] by or under the responsibility of the entity seeking designation as a RA3. The checklist is to be used only in the cases specified in point (b) of point 6.8.5.1 of the Annex to Implementing Regulation (EU) 2015/1998. In cases specified in point (a) of point 6.8.5.1 of that Annex, the EU aviation security validator shall use the ACC3 checklist.

A validation report shall be delivered to the designating appropriate authority and to the validated entity within a maximum of one month after the on-site verification. Integral parts of the validation report shall be at least:

— the completed checklist signed by the EU aviation security validator and where applicable commented by the validated entity; and

— the declaration of commitments (Attachment 6-H2 to Implementing Regulation (EU) 2015/1998) signed by the validated entity; and

— an independence declaration (Attachment 11-A to Implementing Regulation (EU) 2015/1998) in respect of the entity validated signed by the EU aviation security validator.

Page numbering, the date of the EU aviation security validation and initialling on each page by the validator and the validated entity shall be the proof of the validation report's integrity.

The RA3 shall be able to use the report in its business relations with any ACC3 and where applicable, with any RA3.

---

[1] The Union Member States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

[2] EU or EEA bound air cargo or air mail or aircraft in this validation checklist is equivalent to the Union and Iceland, Norway and Switzerland bound air cargo or air mail or aircraft.

▼M2

By default the validation report shall be in English.

Part 5 — Screening and Part 6 — High risk cargo or mail (HRCM) shall be assessed against the requirements of Chapters 6.7 and 6.8 of the Annex to Implementing Regulation (EU) 2015/1998. For those parts that cannot be assessed against the requirements of Implementing Regulation (EU) 2015/1998, baseline standards are the Standards and Recommended Practices (SARPs) of Annex 17 to the Convention on International Civil Aviation and the guidance material contained in the ICAO Aviation Security Manual (Doc 8973-Restricted).

Completion notes:

— All applicable and relevant parts of the checklist must be completed, in accordance with the business model and operations of the entity being validated. Where no information is available, this must be explained.

— After each part, the EU aviation security validator shall conclude if and to what extent the objectives of this part are met.

PART 1

Identification of the entity validated and the validator

1.1. Date(s) of validation	
Use exact date format, such as from 01.10.2012 to 02.10.2012	
dd/mm/yyyy	
1.2. Date of previous validation where applicable	
dd/mm/yyyy	
Previous RA3 registration number, where available	
AEO certificate or C-TPAT status or other certifications, where available	
1.3. Aviation security validator information	
Name	
Company/Organisation/Authority	
Unique alphanumeric identifier (UAI)	
Email address	
Telephone number — including international codes	

▼**M2**

1.4. Name of entity	
Name	
Company number (for example, commercial register identification number, if applicable)	
Number/Unit/Building	
Street	
Town	
Postcode	
State (where relevant)	
Country	
P.O. Box address, if applicable	
1.5. Main address of organisation (if different from site to be validated)	
Number/Unit/Building	
Street	
Town	
Postcode	
State (where relevant)	
Country	
P.O. Box address, if applicable	
1.6. Nature of business — More than one business type may be applicable	
(a) air cargo only (b) air and other modes of transport (c) freight forwarder with cargo premises (d) freight forwarder without cargo premises (e) handling agent (f) others	
1.7. Does the applicant …?	
(a) receive cargo from another 3rd country regulated agent	

▼M2

(b) receive cargo from 3rd country known consignors	
(c) receive cargo from 3rd country account consignors	
(d) receive exempted cargo	
(e) screen cargo	
(f) store cargo	
(g) other, please specify	
1.8. Approximate number of employees on site	
Number	
1.9. Name and title of person responsible for third country air cargo or air mail security	
Name	
Job title	
Email address	
Telephone number — including international codes	

PART 2

Organisation and responsibilities of the third country EU aviation security validated regulated agent

Objective: No air cargo or air mail shall be carried to the EU or EEA without being subject to security controls. Cargo and mail delivered by an RA3 to an ACC3 or another RA3 may only be accepted as secure cargo or mail if such security controls are applied by the RA3. Details of such controls are provided in the following Parts of this checklist.

The RA3 shall have procedures in place to ensure that appropriate security controls are applied to all EU or EEA bound air cargo and air mail and that secure cargo or mail is protected until being transferred to an ACC3 or another RA3. Security controls shall consist of one of the following:

(a) physical screening which shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the consignment;

(b) other security controls, part of a supply chain security process, that reasonably ensure that no prohibited articles are concealed in the consignment and which have been applied by another RA3, KC3 or AC3 designated by the RA3.

Reference: point 6.8.3 of the Annex to Implementing Regulation (EU) 2015/1998.

▼M2

2.1. Has the entity established a security programme?	
YES or NO	
If NO go directly to point 2.5.	
2.2. Entity security programme	
Date — use exact format dd/mm/yyyy	
Version	
Is the security programme submitted and/or approved by the appropriate authority of the state of the entity? If YES please describe the process.	
2.3. Does the security programme sufficiently cover the elements mentioned in parts 3 to 9 of the checklist?	
YES or NO	
If NO, describe why detailing the reasons	
2.4. Is the security programme conclusive, robust and complete?	
YES or NO	
If NO, specify the reasons	
2.5. Has the entity established a process to ensure that air cargo or air mail is submitted to appropriate security controls before being transferred to an ACC3 or another RA3?	
YES or NO	
If YES, describe the process	
2.6. Has the entity a management system (such as instruments, instructions) in place to ensure that the required security controls are implemented?	
YES or NO	
If YES, describe the management system and explain if it is approved, checked or provided by the appropriate authority or another entity.	
If NO, explain how the entity ensures that security controls are applied in the required manner.	

▼M2

2.7. Conclusions and general comments on the reliance, conclusiveness and robustness of the process.	
Comments from the entity	
Comments from the EU aviation security validator	

PART 3

Staff recruitment and training

Objective: To ensure the required security controls are applied, the RA3 shall assign responsible and competent staff to work in the field of securing air cargo or air mail. Staff with access to secured air cargo must possess all the competencies required to perform their duties and shall be appropriately trained.

To fulfil that objective, the RA3 shall have procedures in place to ensure that all staff (such as permanent, temporary, agency staff, drivers) with direct and unescorted access to air cargo or air mail to which security controls are being or have been applied:

(a) have been subject to initial and recurrent pre-employment checks or background checks, which are at least in accordance with the requirements of the local authorities of the RA3 premises validated; and

(b) have completed initial and recurrent security training to be aware of their security responsibilities in accordance with the requirements of the local authorities of the RA3 premises validated.

Note:

— A background check means a check of a person's identity and previous experience, including where legally permissible, any criminal history as part of the assessment of an individual's suitability to implement a security control and/or for unescorted access to a security restricted area (ICAO Annex 17 definition).

— A pre-employment check shall establish the person's identity on the basis of documentary evidence, cover employment, education and any gaps during at least the preceding five years, and require the person to sign a declaration detailing any criminal history in all states of residence during at least the preceding 5 years (Union definition).

Reference: point 6.8.3.1 of the Annex to Implementing Regulation (EU) 2015/1998.

3.1. Is there a procedure ensuring that all staff with direct and unescorted access to secured air cargo/air mail is subject to a pre-employment check that assesses background and competence?	
YES or NO	
If YES, indicate the number of preceding years taken into account for the pre-employment check and state which entity carries it out.	

▼M2

3.2. Does this procedure include?	
☐ background check ☐ pre-employment check ☐ check of criminal records ☐ interviews ☐ other (provide details) Explain the elements, indicate which entity carries this element out and where applicable, indicate the preceding timeframe that is taken into account.	
3.3. Is there a procedure ensuring that the person responsible for the application and supervision of the implementation of security controls at the site is subject to a pre-employment check that assesses background and competence?	
YES or NO	
If YES, indicate the number of preceding years taken into account for the pre-employment check and state which entity carries it out.	
3.4. Does this procedure include?	
☐ background check ☐ pre-employment check ☐ check of criminal records ☐ interviews ☐ other (provide details) Explain the elements, indicate which entity carries this element out and where applicable, indicate the preceding timeframe that is taken into account.	
3.5. Do staff with direct and unescorted access to secured air cargo or air mail receive security training before being given access to secured air cargo or air mail?	
YES or NO	
If YES, describe the elements and duration of the training	
3.6. Do staff that accept, screen or protect air cargo or air mail receive specific job-related training?	
YES or NO	
If YES, describe the elements and durations of training courses.	
3.7. Do staff referred to in points 3.5 and 3.6 receive recurrent training?	
YES or NO	
If YES, specify the elements and the frequency of the recurrent training	

▼M2

3.8. Conclusion: do the measures concerning staff recruitment and training ensure that all staff with access to secured air cargo or air mail have been properly recruited and trained to a standard sufficient to be aware of their security responsibilities?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

PART 4

Acceptance procedures

Objective: The RA3 may receive cargo or mail from another RA3, a KC3, an AC3 or from an unknown consignor. The RA3 shall have appropriate acceptance procedures for cargo and mail in place in order to establish whether a consignment comes from a secure supply chain or not and subsequently which security measures need to be applied to it.

When accepting any consignments, the RA3 shall establish the status of the entity from which it receives the consignments verifying whether or not the unique alphanumeric identifier (UAI) of the entity delivering the consignments is indicated on the accompanying documentation, and confirming that the air carrier or entity delivering the consignment is listed as active in the Union database on supply chain security for the specified airport or site, as appropriate.

If there is no indication of the UAI on the documentation or if the status of the air carrier or entity on the Union database on supply chain security is not active, the RA3 shall treat the consignments as arriving from an unknown source.

Additionally, a RA3 shall maintain a database giving at least the following information for each regulated agent or known consignor that has been subject to EU aviation security validation in accordance with point 6.8.5.1, from which it directly accepts cargo or mail to be delivered to an ACC3 for carriage into the Union:

(a) the company details, including the bona fide business address;

(b) the nature of the business, excluding business sensitive information;

(c) contact details, including those of the person(s) responsible for security;

(d) the company registration number, if applicable;

(e) where available, the validation report;

(f) the unique alphanumeric identifier attributed in the Union database on supply chain security.

Reference: points 6.8.3.1, 6.8.3.5, and 6.8.5.4 of the Annex to Implementing Regulation (EU) 2015/1998.

Note: An RA3 may only accept cargo from an AC3 as secure cargo, if this RA3 has designated this consignor itself as AC3, in accordance with point (c) of point 6.8.3.1 of the Annex to Implementing Regulation (EU) 2015/1998, and accounts for the cargo delivered by this consignor.

▼M2

4.1. When accepting a consignment, does the entity establish whether it comes from another RA3, a KC3, an AC3 or an unknown consignor?	
YES or NO	
If YES, how?	
4.2. Does the entity verify the indication of the UAI on the documentation accompanying consignments received from another ACC3, RA3 or KC3 and confirms the active status of the ACC3, RA3 or KC3 on the Union database on supply chain security?	
YES or NO	
4.3. Does the entity have a procedure to ensure that in case the documentation does not contain the UAI or the entity from which the cargo is received has no active status on the Union database on supply chain security, the consignment is treated as shipment coming from an unknown source?	
YES or NO	
4.4. Does the entity designate consignors as AC3?	
YES or NO	
If YES, describe the procedure and the safeguards required by the entity from the consignor.	
4.5. When accepting a consignment, does the entity establish whether its destination is an EU or EEA airport?	
YES or NO — explain	
4.6. If YES — does the entity submit all air cargo or air mail to the same security controls when the destination is an EU or EEA airport?	
YES or NO	
If YES, describe the procedure	
4.7. When accepting a consignment, does the entity establish whether it is to be regarded as high risk cargo and mail (HRCM) (see definition in Part 6), including for consignments that are delivered by other modes of transport than by air?	
YES or NO	
If YES, how? Describe the procedure	
4.8. When accepting a secured consignment, does the validated entity establish whether it has been protected from unauthorised interference or tampering?	
YES or NO	
If YES, describe by which means (for example, using seals, locks, inspection)	

▼M2

4.9. Is the person making the delivery required to present an official identification document containing a photo?	
YES or NO	
4.10. Is there a process in place to identify consignments that require screening?	
YES or NO	
If YES, how?	
4.11. Conclusion: Are the acceptance procedures sufficient to establish that air cargo or air mail to an EU or EEA airport destination comes from a secure supply chain or needs to be subject to screening?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from EU aviation security validator	

PART 5

Screening

Objective: Where the RA3 accepts cargo and mail which does not come from a secure supply chain, the RA3 needs to subject these consignments to appropriate screening before it may be delivered to an ACC3 as secure cargo. The RA3 shall have procedures in place to ensure that EU or EEA bound air cargo and air mail for transfer, transit or unloading at a Union airport is screened by the means or methods referred to in Union legislation to a standard sufficient to reasonably ensure that it contains no prohibited articles.

Where screening of air cargo or air mail is performed by or on behalf of the appropriate authority in the third country, the RA3 shall declare this fact and specify the way adequate screening is ensured.

Reference: point 6.8.3 of the Annex to Implementing Regulation (EU) 2015/1998.

▼M2

5.1. Is screening applied on behalf of the entity by another entity?	
YES or NO	
If YES, Specify the nature of these entities and provide details: — private screening company; — government regulated company; — government screening facility or body; — other Specify the nature of the agreement or contract between the validated entity and the entity that applies the screening on its behalf.	
5.2. Is the entity able to request the appropriate security controls in case the screening is carried out by one of the above entities?	
YES or NO	
If NO, provide details	
5.3. By which instruments and instructions (such as oversight, monitoring, and quality control) does the entity ensure that security controls are applied in the required manner by such service providers?	
5.4. What methods of screening are used for air cargo and mail?	
Specify, including details of equipment used for screening air cargo and air mail (such as manufacturer, type, software version, standard, serial number) for all the methods deployed.	
5.5. Is the equipment or method (such as explosive detection dogs) used included in the most recent EU, European Civil Aviation Conference (ECAC) or the Transportation Security Administration (TSA) of the US compliance list?	
YES or NO	
If YES, provide details	

▼M2

If NO, give details specifying the approval of the equipment and date thereof, as well as any indications that it complies with EU equipment standards.	
5.6. Is the equipment used in accordance with the manufacturers' concept of operations (CONOPS) and is the equipment regularly tested and maintained?	
YES or NO	
If YES, describe the process	
5.7. In case EDDs are deployed, are they subjected to initial and recurrent training, approval and quality control process to a standard equivalent to the EU or TSA requirements?	
YES or NO	
If YES, describe the entire process and the related documentation supporting the assessment	
5.8. In case EDDs are used, is the screening process following a deployment methodology equivalent to EU or TSA standards?	
YES or NO	
If YES, describe the entire process and the related documentation supporting the assessment	
5.9. Is the nature of the consignment taken into consideration during screening?	
YES or NO	
If YES, describe how it is ensured that the screening method selected is employed to a standard sufficient to reasonably ensure that no prohibited articles are concealed in the consignment.	
5.10. Is there a process for the resolution of the alarm generated by the screening equipment? For some equipment, such as x-ray equipment, the alarm is triggered by the operator himself.	
YES or NO	
If YES, describe the process of resolving alarms to reasonably ensure the absence of prohibited articles.	

▼M2

If NO, describe what happens to the consignment	
5.11. Are any consignments exempt from security screening?	
YES or NO	
5.12. Are there any exemptions that do not comply with the Union list?	
YES or NO	
If YES, detail	
5.13. Is access to the screening area controlled to ensure that only authorised and trained staff are granted access?	
YES or NO	
If YES, describe	
5.14. Is an established quality control and/or testing regime in place?	
YES or NO	
If YES, describe	
5.15. Conclusion: Is air cargo or air mail screened by one of the means or methods listed in point 6.2.1 of the Annex to Implementing Regulation (EU) 2015/1998 to a standard sufficient to reasonably ensure that it contains no prohibited articles?	
YES or NO	
If NO, specify reason	
Comments from the entity	
Comments from the EU aviation security validator	

PART 6

High Risk Cargo or Mail

Objective: Consignments which originate from or transfer in locations identified as high risk by the Union or which appear to have been significantly tampered with are to be considered as high risk cargo and mail (HRCM). Such consignments have to be screened in line with specific instructions. The RA3 shall have procedures in place to ensure that EU or EEA bound HRCM is identified and subject to appropriate controls as defined in the Union legislation.

The ACC3 to which the RA3 delivers air cargo or mail for transportation shall be authorised to inform the RA3 about the latest state of relevant information on high risk origins.

▼M2

The RA3 shall apply the same measures, irrespective of whether it receives high risk cargo and mail from an air carrier or through other modes of transportation.

Reference: point 6.7 of the Annex to Implementing Regulation (EU) 2015/1998.

Note: HRCM cleared for carriage into the EU/EEA shall be issued the security status 'SHR', meaning secure for passenger, all-cargo and all-mail aircraft in accordance with high risk requirements.

6.1. Do staff responsible for performing security controls know which air cargo and mail is to be treated as high risk cargo and mail (HRCM)?	
YES or NO	
If YES, describe	
6.2. Does the entity have procedures in place for the identification of HRCM?	
YES or NO	
If YES, describe	
6.3. Is HRCM subject to HRCM screening procedures according to Union legislation?	
YES or NO	
If NO, indicate procedures applied	
6.4. After screening, does the entity issue a security status declaration for SHR in the documentation accompanying the consignment?	
YES or NO	
If YES, describe how security status is issued and in which document	
6.5. Conclusion: Is the process put in place by the entity relevant and sufficient to ensure that all HRCM has been properly treated before loading?	
YES or NO	
If NO, specify reason	
Comments from the entity	
Comments from EU aviation security validator	

▼M2

PART 7

Protection of secured air cargo and mail

Objective: The RA3 shall have procedures in place to ensure EU or EEA bound air cargo and/or air mail is protected from unauthorised interference and/or any tampering from the point where security screening or other security controls are applied or from the point of acceptance after screening or security controls have been applied, until loading or transferring to an ACC3 or another RA3. If previously secured air cargo and mail is not protected afterwards, it may not be loaded or transferred to an ACC3 or another RA3 as secure cargo or mail.

Protection can be provided by different means such as physical (for example barriers, locked rooms), human (for example patrols, trained staff) and technological (for example CCTV, intrusion alarm).

EU or EEA bound secured air cargo or mail should be separated from air cargo or mail which is not secured.

Reference: point 6.8.3.1 of the Annex to Implementing Regulation (EU) 2015/1998.

7.1. Is protection of secured air cargo and air mail applied on behalf of the validated entity by another entity?	
YES or NO	
If YES, Specify the nature of these entities and provide details: — private screening company; — government regulated company; — government screening facility or body; — other	
7.2. Are security controls and protection in place to prevent tampering during the screening process?	
YES or NO	
If YES, describe Specify what kind(s) of protection(s) are put in place: — physical (for example fence, barrier, building of solid construction), — human (for example patrols etc.), — technological (for example CCTV, alarm system). Explain how they are organised.	

▼M2

7.3. Is the secure air cargo/air mail only accessible to authorised persons?	
YES or NO	
If YES, describe Specify how all access points (including doors and windows) to identifiable and secured air cargo or air mail are controlled.	
7.4. Are there procedures in place to ensure EU or EEA bound air cargo or air mail to which security controls have been applied are protected from unauthorised interference from the time it has been secured until its loading or is transferred to an ACC3 or another RA3?	
YES or NO	
If YES, describe how it is protected (for example by physical, human, technological means) Specify also if the building is of solid construction and what kinds of materials are used, if available.	
If NO, specify reasons	
7.5. Conclusion: Is the protection of consignments sufficiently robust to prevent unlawful interference?	
YES or NO	
If NO, specify reason	
Comments from the entity	
Comments from EU aviation security validator	

PART 8

Documentation

Objective: The RA3 shall ensure that the documentation accompanying a consignment to which the RA3 has applied security controls (such as screening, protection), contains at least:

(a) the unique alphanumeric identifier received from the designating appropriate authority; and

▼M2

(b) the unique identifier of the consignment, such as the number of the (house or master) air waybill, when applicable; and

(c) the content of the consignment; and

(d) the security status, indicated as follows:

— ‘SPX’, which means secure for passenger, all-cargo and all-mail aircraft, or

— ‘SCO’, which means secure for all-cargo and all-mail aircraft only, or

— ‘SHR’, which means secure for passenger, all-cargo and all-mail aircraft in accordance with high risk requirements.

If the security status is issued by the RA3, the entity shall additionally indicate the reasons for issuing it, such as the means or method of screening used or the grounds for exempting the consignment from screening, using the standards adopted in the Consignment Security Declaration scheme.

The documentation accompanying the consignment may either be in the form of an air waybill, equivalent postal documentation or in a separate declaration, and either in an electronic format or in writing.

Reference: point (d) of point 6.3.2.6, points 6.8.3.4, 6.8.3.5 and 6.8.3.6 of the Annex to Implementing Regulation (EU) 2015/1998

8.1. Does the entity ensure that appropriate accompanying documentation is established, and include the information required in point (d) of point 6.3.2.6, points 6.8.3.4, 6.8.3.5 and 6.8.3.6 of the Annex to Implementing Regulation (EU) 2015/1998?	
YES or NO	
If NO, explain	
8.2. In particular, does the entity specify the status of the cargo and how this was achieved?	
YES or NO	
If NO, explain	
8.3. Conclusion: Is the documentation process sufficient to ensure that cargo or mail is provided with proper accompanying documentation which specifies the correct security status and all required information?	
YES or NO	
If NO, specify reason	
Comments from the entity	
Comments from EU aviation security validator	

▼M2

PART 9

Transportation

Objective: Air cargo and air mail must be protected from unauthorised interference or tampering from the time it has been secured until its loading or until it is transferred to an ACC3 or another RA3. This includes protection during transportation to the aircraft, to the ACC3 or to another RA3. If previously secured air cargo and mail is not protected during transportation, it may not be loaded or transferred to an ACC3 or another RA3 as secure cargo.

During transportation to an aircraft, an ACC3 or another RA3, the RA3 is responsible for the protection of the secure consignments. This includes cases where the transportation is undertaken by another entity, such as a freight forwarder, on its behalf. This does not include cases whereby the consignments are transported under the responsibility of an ACC3 or another RA3.

Reference: point 6.8.3 of the Annex to Implementing Regulation (EU) 2015/1998.

9.1. How is the air cargo or air mail conveyed to the ACC3 or to another RA3?	
(a) Validated entity's own transport?	
YES or NO	
(b) Other RA3'sor ACC3's transport?	
YES or NO	
(c) Contractor used by the validated entity?	
YES or NO	
9.2. Is the air cargo or air mail tamper evidently packed?	
YES or NO	
If YES, how	
9.3. Is the vehicle sealed or locked before transportation?	
YES or NO	
If YES, how	
9.4. Where numbered seals are used, is access to the seals controlled and are the numbers recorded?	
YES or NO	
If YES, specify how	
9.5. If applicable, does the respective haulier sign the haulier declaration?	
YES or NO	

▼M2

9.6. Has the person transporting the cargo been subject to specific security controls and awareness training before being authorised to transport secured air cargo or air mail, or both?	
YES or NO	
If YES, please describe what kind of security controls (such as pre-employment check, background check) and what kind of training (such as security awareness training).	
9.7. Conclusion: Are the measures sufficient to protect air cargo or air mail from unauthorised interference during transportation?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from EU aviation security validator	

PART 10

Compliance

Objective: After assessing Parts 1 to 9 of this checklist, the EU aviation security validator has to conclude if its on-site verification confirms the implementation of the security controls in compliance with the objectives listed in this checklist for the EU or EEA bound air cargo or air mail.

Two different scenarios are possible. The EU aviation security validator concludes that the entity:

1. has succeeded in complying with the objectives referred to in this checklist. A validation report shall be delivered to the designating appropriate authority and to the validated entity within a maximum of one month after the on-site verification;

2. has failed in complying with the objectives referred to in this checklist. In that case, the entity is not authorised to deliver secured air cargo or mail for EU or EEA destination to an ACC3 or to another RA3. It shall receive a copy of the completed checklist stating the deficiencies.

10.1. General conclusion: Indicate the case closest to the situation validated	
1 or 2	
Comments from EU aviation security validator	
Comments from the entity	

Name of the validator:

Date:

Signature:

▼M2

ANNEX

List of persons and entities visited and interviewed

Providing the name of the entity, the name and the position of the contact person and the date of the visit or interview.

Name of entity	Name of contact person	Position of contact person	Date of visit or interview

ATTACHMENT 6-C3

VALIDATION CHECKLIST FOR ACC3

ACC3 (*Air cargo or mail carrier operating into the Union from a third country airport*) designation is the prerequisite for carrying air cargo or air mail into the European Union ([1]) (EU) or Iceland, Norway and Switzerland and is required by Implementing Regulation (EU) 2015/1998.

ACC3 designation is in principle required for all flights carrying cargo or mail for transfer, transit or unloading at EU or EEA airports ([2]). The appropriate authorities of the Member States of the European Union, Iceland, Norway and Switzerland are each responsible for the designation of specific air carriers as ACC3. The designation is based on the security programme of an air carrier and on an on-site verification of the implementation in compliance with the objectives referred to in this validation checklist.

The checklist is the instrument to be used by the EU aviation security validator for assessing the level of security applied to EU or EEA bound air cargo or air mail by or under the responsibility of the ACC3 or an air carrier applying for ACC3 designation.

([1]) The Union Member States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

([2]) EU or EEA bound air cargo or air mail or aircraft in this validation checklist is equivalent to EU and Iceland, Norway and Switzerland bound air cargo or air mail or aircraft.

▼M2

A validation report shall be delivered to the designating appropriate authority and to the validated entity within a maximum of one month after the on-site verification. Integral parts of the validation report shall be at least:

— the completed checklist signed by the EU aviation security validator and where applicable commented by the validated entity; and

— the declaration of commitments (Attachment 6-H1 to Implementing Regulation (EU) 2015/1998) signed by the validated entity; and

— an independence declaration (Attachment 11-A to Implementing Regulation (EU) 2015/1998) in respect of the entity validated signed by the EU aviation security validator.

Page numbering, the date of the EU aviation security validation and initialling on each page by the validator and the validated entity shall be the proof of the validation report's integrity. By default the validation report shall be drafted in English.

Part 3 — Security programme of the air carrier, Part 6 — Database, Part 7 — Screening and Part 8 — High risk cargo or mail (HRCM) shall be assessed against the requirements of Chapters 6.7 and 6.8 of the Annex to Implementing Regulation (EU) 2015/1998. For the other parts, baseline standards are the Standards and Recommended Practices (SARPs) of Annex 17 to the Convention on International Civil Aviation and the guidance material contained in the ICAO Aviation Security Manual (Doc 8973-Restricted).

Completion notes:

— All applicable and relevant parts of the checklist must be completed, in accordance with the business model and operations of the entity being validated. Where no information is available, this must be explained.

— After each part, the EU aviation security validator shall conclude if and to what extent the objectives of this part are met.

PART 1

Identification of the entity validated and the validator

1.1. Date(s) of validation	
Use exact date format, such as 01.10.2012 to 02.10.2012	
dd/mm/yyyy	
1.2. Date of previous validation and unique alphanumeric identifier (UAI) of the ACC3 where available	
dd/mm/yyyy	
UAI	

▼M2

1.3. Aviation security validator information	
Name	
Company/Organisation/Authority	
UAI	
Email address	
Telephone number — including international codes	
1.4. Name of air carrier to be validated	
Name	
AOC (Air Operators Certificate) issued in (name of State):	
International Air Transport Association (IATA) code or International Civil Aviation Organisation (ICAO) code if IATA code does not exist for. Specify which code applies.	
State responsible for designating air carrier as ACC3	
1.5. Details of third country airport location to be validated or cargo or mail facilities linked to it	
Name	
IATA or ICAO code for the airport	
Country	
1.6. Nature of air carrier's business — More than one business type may be applicable	
(a) passenger and cargo/mail carrier; (b) cargo and mail only carrier; (c) cargo only carrier; (d) mail only carrier; (e) integrator; (f) charter.	
1.7. Name and title of person responsible for third country air cargo or air mail security	
Name	
Job title	
Email address	

▼M2

Telephone number — including international codes	
1.8. Address of the air carrier's main office at the airport being visited	
Number/Unit/Building/Airport	
Street	
Town	
Postcode	
State (where relevant)	
Country	
1.9. Address of the air carrier's main office, for example the corporate headquarters	
Number/Unit/Building/Airport	
Street	
Town	
Postcode	
State (where relevant)	
Country	

PART 2

Organisation and responsibilities of the ACC3 at the airport

Objective: No air cargo or mail shall be carried to the EU or EEA without being subject to security controls. Details of such controls are provided by the following Parts of this checklist. The ACC3 shall not accept cargo or mail for carriage on an EU-bound aircraft unless the application of screening or other security controls is confirmed and accounted for by an EU aviation security validated regulated agent, an EU aviation security validated known consignor or an account consignor designated by itself or by an EU aviation security validated regulated agent, or such consignments are subject to screening in accordance with the Union legislation.

The ACC3 shall have a process to ensure that appropriate security controls are applied to all EU or EEA bound air cargo and air mail unless it is exempted from screening in accordance with the Union legislation and that cargo or mail is protected thereafter until loading onto aircraft. Security controls shall consist of:

▼M2

— physical screening which shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the consignment, or

— other security controls which are part of a supply chain security process that reasonably ensure that no prohibited articles are concealed in the consignment applied by EU aviation security validated regulated agents or known consignors or by an account consignor designated by itself or by an EU aviation security validated regulated agent.

Reference: point 6.8.3 of the Annex to Implementing Regulation (EU) 2015/1998

2.1. Has the air carrier established a process to ensure that air cargo or air mail is submitted to appropriate security controls prior to being loaded onto an EU or EEA bound aircraft?	
YES or NO	
If YES, describe the process	
2.2. Are the security controls applied by the air carrier or on its behalf by an entity covered under the air carrier's security programme?	
If YES, provide details	
If NO, which entities not covered by the air carrier's security programme apply security controls to air cargo or mail carried by this air carrier into the EU or EEA?	
Specify the nature of these entities and provide details: — private handling company; — government regulated company; — government screening facility or body; — other	
2.3. By which instruments and instructions (such as oversight, monitoring, and quality control) does the air carrier ensure that security controls are applied in the required manner by the above service providers?	
2.4. Is the air carrier able to request the appropriate security controls in case the screening is carried out by entities which are not covered by the air carrier's security programme, such as government facilities?	
YES or NO	
If NO, provide details	

▼M2

2.5. By which instruments and instructions (such as oversight, monitoring, and quality control) does the air carrier ensure that security controls are applied in the required manner by such service providers?	
2.6. Has a regulated agent or known consignor programme for air cargo and mail been put in place in accordance with ICAO standards in the State of the airport at which the validation visit takes place?	
If YES, describe the elements of the programme and how it has been put in place	
2.7. Conclusions and general comments on the reliance, conclusiveness and robustness of the process.	
Comments from the air carrier	
Comments from the EU aviation security validator	

PART 3

Security programme of the air carrier

Objective: The ACC3 shall ensure that its security programme includes all the aviation security measures relevant and sufficient for air cargo and mail to be transported into the Union.

The security programme and associated documentation of the air carrier shall be the basis of security controls applied in compliance with the objective of this checklist. The air carrier may wish to consider passing its documentation to the EU aviation security validator in advance of the site visit to help acquaint him with the details of the locations to be visited.

Reference: point 6.8.2.1 of the Annex and Attachment 6-G to Implementing Regulation (EU) 2015/1998

Note: The following points listed in Attachment 6-G to Implementing Regulation (EU) 2015/1998 shall be appropriately covered:

(a) description of measures for air cargo and mail;

(b) procedures for acceptance;

(c) regulated agent scheme and criteria;

(d) known consignor scheme and criteria;

(e) account consignor scheme and criteria;

(f) standard of screening;

(g) location of screening;

(h) details of screening equipment;

(i) details of operator or service provider;

(j) list of exemptions from security screening;

(k) treatment of high risk cargo and mail.

▼M2

3.1. Air carrier security programme	
Date — use exact date format dd/mm/yyyy	
Version	
Has the programme been submitted to an EU or EEA appropriate authority at an earlier stage? If YES was it for ACC3 designation? Other purposes?	
3.2. Does the security programme cover sufficiently the elements of the list above?	
YES or NO	
If NO, describe why detailing the reasons	
3.3. Are the aviation security measures described by the security programme relevant and sufficient to secure EU or EEA bound air cargo or air mail according to the required standards?	
YES or NO	
If NO, describe why detailing the reasons	
3.4. Conclusion: Is the security programme conclusive, robust and complete?	
YES or NO	
If NO, specify reasons	
Comments from the air carrier	
Comments from the EU aviation security validator	

PART 4

Staff recruitment and training

Objective: The ACC3 shall assign responsible and competent staff to work in the field of securing air cargo or air mail. Staff with access to secured air cargo possess all the competencies required to perform their duties and are appropriately trained.

In order to fulfil that objective, the ACC3 shall have a procedure to ensure that all staff (such as permanent, temporary, agency staff, drivers) with direct and unescorted access to air cargo or air mail to which security controls are being or have been applied:

— have been subject to initial and recurrent pre-employment checks or background checks, which are at least in accordance with the requirements of the local authorities of the airport validated, and

— have completed initial and recurrent security training to be aware of their security responsibilities in accordance with the requirements of the local authorities of the airport validated.

▼**M2**

Reference: point 6.8.3.1 of the Annex to Implementing Regulation (EU) 2015/1998

Note:

— A background check means a check of a person's identity and previous experience, including where legally permissible, any criminal history as part of the assessment of an individual's suitability to implement a security control or for unescorted access to a security restricted area (ICAO Annex 17 definition).

— A pre-employment check shall establish the person's identity on the basis of documentary evidence, cover employment, education and any gaps during at least the preceding five years, and require the person to sign a declaration detailing any criminal history in all states of residence during at least the preceding five years (Union definition).

4.1. Is there a procedure ensuring that all staff with direct and unescorted access to secured air cargo or air mail are subject to pre-employment checks that assesses background and competence?	
YES or NO	
If YES, indicate the number of preceding years taken into account for the pre-employment check and state which entity carries it out.	
4.2. Does this procedure include?	
— background check — pre-employment check — check of criminal records — interviews — other (provide details) Explain the elements, indicate which entity carries this element out and where applicable, indicate the preceding timeframe that is taken into account.	
4.3. Is there a procedure ensuring that the person responsible for the application and supervision of the implementation of security controls at the site is subject to a pre-employment check that assesses background and competence?	
YES or NO	
If YES, indicate the number of preceding years taken into account for the pre-employment check and state which entity carries it out.	
4.4. Does this procedure include?	
— background check — pre-employment check — check of criminal records — interviews — other (provide details) Explain the elements, indicate which entity carries this element out and where applicable, indicate the preceding timeframe that is taken into account.	

▼M2

4.5. Do staff with direct and unescorted access to secured air cargo or air mail receive security training before being given access to secured air cargo or air mail?	
YES or NO	
If YES, describe the elements and duration of the training	
4.6. Do staff that accept, screen or protect air cargo or air mail receive specific job related training?	
YES or NO	
If YES, describe the elements and durations of training courses.	
4.7. Do staff referred to in points 4.5 and 4.6 receive recurrent training?	
YES or NO	
If YES, specify the elements and the frequency of the recurrent training	
4.8. Conclusion: do the measures concerning staff recruitment and training ensure that all staff with access to secured air cargo or air mail have been properly assigned and trained to a standard sufficient to be aware of their security responsibilities?	
YES or NO	
If NO, specify reasons	
Comments from the air carrier	
Comments from the EU aviation security validator	

PART 5

Acceptance procedures

Objective: The ACC3 shall have a procedure in place in order to assess and verify upon acceptance the security status of a consignment in respect of previous controls.

The procedure shall include the following elements:

(a) confirmation that the entity delivering the consignment is listed as active in the Union database on supply chain security for the specified airport or site;

(b) verification that the Union database unique alphanumeric identifier of the entity delivering the consignment is indicated on the accompanying documentation;

▼M2

(c) in case of consignments received from an account consignor, verification that the entity is in listed in the air carrier's database.

If there is no indication on the accompanying documentation of the identifier, or if the air carrier or entity delivering the consignments is not listed as active in the Union database on supply chain security, or in the case of account consignors the entity is not in the air carrier's database, it shall be deemed that no security controls have previously been applied, and the consignments shall be screened by the ACC3 or by another EU aviation security validated RA3 before being loaded onto the aircraft;

(d) verification of whether the consignment is delivered by a person nominated by the EU aviation security validated regulated agent or known consignor as listed in its database or an account consignor of such a regulated agent or designated by the air carrier itself;

(e) the person nominated shall correspond to the person tasked to deliver the air cargo or air mail to the air carrier. The person delivering the consignment to the air carrier shall present an identity card, passport, driving license or other document, which includes his or her photograph and which has been issued or is recognised by the national authority;

(f) where applicable, verification of whether the consignment is presented with all the required security information (air waybill and security status information on paper or by electronic means, description of the consignment and unique identifier thereof, reasons for issuing the security status, means or methods of screening or grounds for exemption from screening) that corresponds to the air cargo and mail consignments being delivered;

(g) verification of whether the consignment is free from any signs of tampering; and

(h) verification of whether the consignment has to be treated as high risk cargo and mail (HRCM).

Reference: point 6.8.3.5, 6.8.3.6, 6.8.3.7, and 6.8.5.4 of the Annex to Implementing Regulation (EU) 2015/1998

5.1. When directly accepting a consignment, does the air carrier establish whether it comes from a regulated agent, a known consignor or an account consignor recognised according to Union air cargo legislation and listed in the Union database on supply chain security and in the database kept by the air carrier?	
YES or NO	
If YES, describe the procedure	
5.2. Does the air carrier verify the indication of the UAI on the documentation accompanying consignments received from another ACC3, RA3 or KC3 and confirms the active status of the ACC3, RA3 or KC3 on the database on supply chain security?	
YES or NO	

▼M2

5.3. Does the entity have a procedure to ensure that in case the documentation does not contain the UAI or the entity from which the cargo is received has no active status on the Union database on supply chain security, the consignment is treated as shipment coming from an unknown source?	
YES or NO	
5.4. Does the air carrier designate consignors as AC3?	
YES or NO	
If YES, describe the procedure and the safeguards required by the air carrier from the consignor.	
5.5. When directly accepting a consignment, does the air carrier establish whether its destination is an EU or EEA airport?	
YES or NO — explain	
5.6. If YES — does the air carrier submit all cargo or mail to the same security controls when the destination is an EU or EEA airport?	
YES or NO	
If YES, describe the procedure	
5.7. When directly accepting a consignment, does the air carrier establish whether it is to be regarded as high risk cargo and mail (HRCM), including for consignments that are delivered by other modes of transport other than air?	
YES or NO	
If YES, how? Describe the procedure	
5.8. When accepting a secured consignment, does the air carrier establish whether it has been protected from unauthorised interference and/or tampering?	
YES or NO	

▼M2

If YES, describe (such as seals, locks).	
5.9. If the air carrier accepts transit air cargo or air mail at this location (cargo or mail that departs on the same aircraft it arrived on), does the air carrier establish on the basis of the given data whether or not further security controls need to be applied?	
YES or NO	
If YES, how is it established?	
If NO, what controls are applied to ensure security of EU or EEA bound cargo and mail?	
5.10. If the air carrier accepts transfer air cargo or air mail at this location (cargo or mail that departs on a different aircraft to the one it arrived on), does the air carrier establish on the basis of the given data whether or not further security controls need to be applied?	
YES or NO	
If YES, how is it established?	
If NO, what controls are applied to ensure security of EU or EEA bound cargo and mail?	
5.11. Is the person delivering secured known air cargo to the air carrier required to present an official identification document containing a photograph?	
YES or NO	
5.12. Conclusion: Are the acceptance procedures sufficient to establish whether air cargo or air mail comes from a secure supply chain or that it needs to be subjected to screening?	
YES or NO	
If NO, specify reasons	
Comments from the air carrier	
Comments from the EU aviation security validator	

PART 6

Database

Objective: Where the ACC3 is not obliged to apply 100 % screening to EU/EEA bound air cargo or air mail, the ACC3 shall ensure the cargo or mail comes from an EU aviation security validated entity designated by the appropriate authority of an EU Member State as third country regulated agent (RA3) or third country known consignor (KC3), or from an account consignor (AC3) designated by itself or by a third country regulated agent.

▼M2

For monitoring the security relevant audit trail the ACC3 shall verify the active status of the RA3 and KC3 on the Union database of supply chain security, and maintain a database giving the following information for each entity or person from which it directly accepts cargo or mail:

— the status of the involved entity (regulated agent or known consignor),

— the company details, including the bona fide business address,

— the nature of the business, excluding business sensitive information,

— contact details, including those of the person(s) responsible for security,

— the unique alphanumeric identifier attributed in the Union database on supply chain security, or in case the entity is an AC3 the company registration number.

When receiving air cargo or mail from a RA3 or KC3 the ACC3 shall check in the Union database whether the entity is listed as active, and for AC3 in the air carrier's database. If the RA3 or KC3 status is not active or the AC3 is not included in the database, the air cargo or air mail delivered by such entity shall be screened before loading.

Reference: point (a) of point 6.8.3.5 and point 6.8.5.4 of the Annex to Implementing Regulation (EU) 2015/1998

6.1. When directly accepting a consignment, does the air carrier establish whether it comes from a regulated agent, a known consignor or an account consignor recognised according to Union air cargo legislation and listed in the Union database on supply chain security and in the database kept by the air carrier?	
YES or NO	
If YES, describe the procedure	
6.2. Does the air carrier maintain a database including, as appropriate, the details referred to above, of:	
— entities designated as third country regulated agent (RA3), — entities designated as third country known consignor (KC3), — entities designated as account consignors by an RA3 or by the air carrier (AC3)?	
YES or NO	
If YES, describe the database	
If NO, explain why	

▼M2

6.3. Does staff accepting air cargo and air mail have easy access to the Union database on supply chain security and to the air carrier's database?	
YES or NO	
If YES, describe the process	
6.4. Is the database updated in a regular manner as to provide reliable data to the staff accepting air cargo and air mail?	
YES or NO	
If NO, explain	
6.5. Conclusion: Does the air carrier maintain a database that ensures full transparency on its relation to entities from which it directly receives (screened or security controlled) cargo or mail for transport into the Union or EEA?	
YES or NO	
If NO, specify reasons	
Comments from the air carrier	
Comments from the EU aviation security validator	

PART 7

Screening

Objective: Where the ACC3 accepts cargo and mail from an entity which is not an EU aviation security validated entity or the cargo received has not been protected from unauthorised interference from the time security controls were applied, the ACC3 shall ensure the air cargo or air mail is screened before being loaded onto an aircraft. The ACC3 shall have a process to ensure that EU or EEA bound air cargo and air mail for transfer, transit or unloading at an Union airport are screened by the means or methods referred to in Union legislation to a standard sufficient reasonably to ensure that it contains no prohibited articles.

Where the ACC3 does not screen air cargo or air mail itself, it shall ensure that the appropriate screening is carried out according to Union requirements. Screening procedures shall include where appropriate the treatment of transfer and transit cargo and mail

▼M2

Where screening of air cargo or mail is performed by or on behalf of the appropriate authority in the third country, the ACC3 receiving such air cargo or air mail from the entity shall declare this fact in its security programme, and specify the way adequate screening is ensured.

Reference: points 6.8.3.1, 6.8.3.2, 6.8.3.3 of the Annex to Implementing Regulation (EU) 2015/1998

7.1. Is screening applied by the air carrier or on its behalf by an entity covered under the air carrier's security programme?	
If YES, provide details. If applicable, provide details of the entity or entities covered under the air carrier's security programme: — name — site specific address — presence of AEO status, if applicable	
If NO, which entities not covered by the air carrier's security programme apply screening to air cargo or mail carried by this air carrier into the EU or EEA? Specify the nature of these entities and provide details — private handling company — government regulated company — government screening facility or body — other	
7.2. Is the entity able to request the appropriate security controls in case the screening is carried out by one of the above entities?	
YES or NO	
If NO, provide details	
7.3. By which instruments and instructions (for example oversight, monitoring, and quality control) does the entity ensure that security controls are applied in the required manner by such service providers?	
7.4. What methods of screening are used for air cargo and air mail?	
Specify, including details of equipment used for screening air cargo and air mail (such as manufacturer, type, software version, standard, serial number) for all the methods deployed	

▼M2

7.5. Is the equipment or method (for example explosive detection dogs) used included in the most recent EU, European Civil Aviation Conference (ECAC) or the Transportation Security Administration (TSA) of the US compliance list?	
YES or NO	
If YES, provide details	
If NO, give details specifying the approval of the equipment and date thereof, as well as any indications that it complies with EU equipment standards	
7.6. Is the equipment used in accordance with the manufacturers' concept of operations (CONOPS) and is the equipment regularly tested and maintained?	
YES or NO	
If YES, describe the process	
7.7. In case EDDs are deployed, are they subjected to initial and recurrent training, approval and quality control process to a standard equivalent to the EU or TSA requirements?	
YES or NO	
If YES, describe the entire process and the related documentation supporting the assessment	
7.8. In case EDDs are used, is the screening process following a deployment methodology equivalent to EU or TSA standards?	
YES or NO	
If YES, describe the entire process and the related documentation supporting the assessment	
7.9. Is the nature of the consignment taken into consideration during screening?	
YES or NO	
If YES, describe how it is ensured that the screening method selected is employed to a standard sufficient to reasonably ensure that no prohibited articles are concealed in the consignment	
7.10. Is there a process for the resolution of the alarm generated by the screening equipment?	
YES or NO	
If YES, describe the process of resolving alarms to reasonably ensure the absence of prohibited articles.	

▼M2

If NO, describe what happens to the consignment.	
7.11. Are any consignments exempt from security screening?	
YES or NO	
7.12. Are there any exemptions that do not comply with the Union list?	
YES or NO	
If YES, detail	
7.13. Is access to the screening area controlled to ensure that only authorised and trained staff is granted access?	
YES or NO	
If YES, describe	
7.14. Is an established quality control or testing regime in place?	
YES or NO	
If YES, describe	
7.15. Conclusion: Is air cargo or air mail screened by one of the means or methods listed in point 6.2.1 of the Annex to Implementing Regulation (EU) 2015/1998 to a standard sufficient to reasonably ensure that it contains no prohibited articles?	
YES or NO	
If NO, specify reason	
Comments from the air carrier	
Comments from the EU aviation security validator	

PART 8

High risk cargo or mail

Objective: Consignments which originate from or transfer in locations identified as high risk by the EU or which appear to have been significantly tampered with are to be considered as high risk cargo and mail (HRCM). Such consignments have to be screened in line with specific instructions. High risk origins and screening instructions are provided by the appropriate EU/EEA authority having designated the ACC3. The ACC3 shall have a procedure to ensure that EU or EEA bound HRCM is identified and subject to appropriate controls as defined in the Union legislation.

▼**M2**

The ACC3 shall remain in contact with the appropriate authority responsible for the EU/EEA airports to which it carries cargo in order to have available the latest state of information on high risk origins.

The ACC3 shall apply the same measures, irrespective of whether it receives high risk cargo and mail from another air carrier or through other modes of transportation.

Reference: points 6.7 and 6.8.3.6 of the Annex to Implementing Regulation (EU) 2015/1998

Note: HRCM cleared for carriage into the EU or EEA shall be issued the security status 'SHR', which means secure for passenger, all-cargo and all-mail aircraft in accordance with high risk requirements.

8.1. Does the air carrier staff responsible for performing security controls know which air cargo and mail is to be treated as high risk cargo and mail (HRCM)?	
YES or NO	
If YES, describe	
8.2. Does the air carrier have procedures in place for the identification of HRCM?	
YES or NO	
If YES, describe	
8.3. Is HRCM subject to HRCM screening procedures according to the EU legislation?	
YES or NO	
If NO, indicate procedures applied	
8.4. After screening, does the air carrier issue a security status declaration for SHR in the documentation accompanying the consignment?	
YES or NO	
If YES, describe how security status is issued and in which document	
8.5. Conclusion: Is the process put in place by the air carrier relevant and sufficient to ensure that all HRCM has been properly treated before loading?	
YES or NO	
If NO, specify reason	
Comments from the air carrier	
Comments from EU aviation security validator	

▼M2

PART 9

Protection

Objective: The ACC3 shall have processes in place to ensure EU or EEA bound air cargo or air mail is protected from unauthorised interference from the point where security screening or other security controls are applied or from the point of acceptance after screening or security controls have been applied, until loading.

Protection can be provided by different means such as physical (for example barriers, locked rooms), human (for example patrols, trained staff) and technological (for example CCTV, intrusion alarm).

EU or EEA bound secured air cargo or mail should be separated from air cargo or mail which is not secured.

Reference: point 6.8.3 of the Annex to Implementing Regulation (EU) 2015/1998

9.1. Is protection of secured air cargo and air mail applied by the air carrier or on its behalf by an entity covered under the air carrier's security programme?	
If YES, provide details	
If NO, which entities not covered by the air carrier's security programme apply protection measures to secured air cargo or mail carried by this air carrier into the EU or EEA? Specify the nature of these entities and provide details: — private handling company — government regulated company — government screening facility or body — other	
9.2. Are security controls and protection in place to prevent tampering during the screening process?	
YES or NO	
If YES, describe	
9.3. Are there processes in place to ensure EU or EEA bound air cargo or air mail to which security controls have been applied are protected from unauthorised interference from the time it has been secured until its loading?	
YES or NO	
If YES, describe how it is protected	
If NO, specify reasons	

▼M2

9.4. Conclusions: Is the protection of consignments sufficiently robust to prevent unlawful interference?	
YES or NO	
If NO specify reason	
Comments from the air carrier	
Comments from EU aviation security validator	

PART 10

Accompanying documentation

Objective: The ACC3 shall ensure that the documentation accompanying a consignment to which the ACC3 has applied security controls (for example screening, protection), contains at least:

(a) the unique alphanumeric identifier received from the designating appropriate authority; and

(b) the unique identifier of the consignment, such as the number of the (house or master) air waybill, when applicable; and

(c) the content of the consignment; and

(d) the security status, indicated as follows:

— ‘SPX’, which means secure for passenger, all-cargo and all-mail aircraft, or

— ‘SCO’, which means secure for all-cargo and all-mail aircraft only, or

— ‘SHR’, which means secure for passenger, all-cargo and all-mail aircraft in accordance with high risk requirements.

In the absence of a third country regulated agent, the security status declaration may be issued by the ACC3 or by the air carrier arriving from a third country exempted from the ACC3 regime.

If the security status is issued by the ACC3, the air carrier shall additionally indicate the reasons for issuing it, such as the means or method of screening used or the grounds for exempting the consignment from screening, using the standards adopted in the consignment security declaration scheme.

In the event that the security status and the accompanying documentation have been established by an upstream RA3 or by another ACC3, the ACC3 shall verify, during the acceptance process, that the above information is contained in the accompanying documentation.

The documentation accompanying the consignment may either be in the form of an air waybill, equivalent postal documentation or in a separate declaration, and either in an electronic format or in writing.

Reference: point (d) of point 6.3.2.6, points 6.8.3.4, 6.8.3.5, 6.8.3.6 and 6.8.3.7 of the Annex to Implementing Regulation (EU) 2015/1998

▼M2

10.1. Does the air carrier ensure that appropriate accompanying documentation is established, and include the information required in point (d) of point 6.3.2.6), points 6.8.3.4, 6.8.3.5 and 6.8.3.6 of the Annex to Implementing Regulation (EU) 2015/1998?	
YES or NO	
If YES, describe the content of the documentation	
If NO, explain why and how the cargo or mail is treated as 'secure' by the air carrier if it is loaded onto an aircraft	
10.2. Does the documentation include the air carrier's ACC3 unique alphanumeric identifier?	
YES or NO	
If NO, explain why	
10.3. Does the documentation specify the security status of the cargo and how this status was achieved?	
YES or NO	
Describe how this is specified	
10.4. Conclusion: Is the documentation process sufficient to ensure that cargo or mail is provided with proper accompanying documentation which specifies the correct security status and all required information?	
YES or NO	
If NO specify reason	
Comments from the air carrier	
Comments from EU aviation security validator	

PART 11

Compliance

Objective: After assessing the ten previous Parts of this checklist, the EU aviation security validator has to conclude if its on-site verification corresponds with the content of the part of the air carrier security programme describing the measures for the EU or EEA bound air cargo or air mail and if the security controls sufficiently implements the objectives listed in this checklist.

Conclusions may comprise one of the following four possible main cases:

▼M2

(1) the air carrier security programme is in compliance with Attachment 6-G to Implementing Regulation (EU) 2015/1998 and the on-site verification confirms compliance with the objective of the checklist; or

(2) the air carrier security programme is in compliance with Attachment 6-G to Implementing Regulation (EU) 2015/1998 but the on-site verification does not confirm compliance with the objective of the checklist; or

(3) the air carrier security programme is not in compliance with Attachment 6-G to Implementing Regulation (EU) 2015/1998 but the on-site verification confirms compliance with the objective of the checklist; or

(4) the air carrier security programme is not in compliance with Attachment 6-G to Implementing Regulation (EU) 2015/1998 and the on-site verification does not confirm compliance with the objective of the checklist.

11.1. General conclusion: Indicate the case closest to the situation validated	
1, 2, 3 or 4	
Comments from EU aviation security validator	
Comments from the air carrier	

Name of the validator:

Date:

Signature:

▼M2

ANNEX

List of persons and entities visited and interviewed

Providing the name of the entity, the name and the position of the contact person and the date of the visit or interview.

Name of entity	Name of contact person	Position of contact person	Date of visit or interview

ATTACHMENT 6-C4

VALIDATION CHECKLIST FOR THIRD COUNTRY EU AVIATION SECURITY VALIDATED KNOWN CONSIGNOR

Third country entities have the option to become part of an ACC3's (*Air cargo or mail carrier operating into the Union from a third country airport*) secure supply chain by seeking designation as a third country EU aviation security validated known consignor (KC3). A KC3 is a cargo handling entity located in a third country that is validated and approved as such on the basis of an EU aviation security validation.

A (KC3) shall ensure that security controls have been applied to consignments bound for the Union ([1]) and the consignments have been protected from unauthorised interference from the time that those security controls were applied and until transferring to an ACC3 or a third country EU aviation security validated regulated agent (RA3).

The prerequisites for carrying air cargo or air mail into the Union (EU) or Iceland, Norway and Switzerland are required by Implementing Regulation (EU) 2015/1998.

The checklist is the instrument to be used by the EU aviation security validator for assessing the level of security applied to EU or EEA bound air cargo or air mail ([2]) by or under the responsibility of the entity seeking designation as a KC3. The checklist is to be used only in the cases specified in point (b) of point 6.8.5.1 of the Annex to Implementing Regulation (EU) 2015/1998. In cases specified in point (a) of point 6.8.5.1 of that Annex, the EU aviation security validator shall use the ACC3 checklist.

([1]) The Union Member States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom

([2]) EU or EEA bound air cargo or air mail or aircraft in this validation checklist is equivalent to the Union and Iceland, Norway and Switzerland bound air cargo or air mail or aircraft.

▼M2

A validation report shall be delivered to the designating appropriate authority and to the validated entity within a maximum of one month after the on-site verification. Integral parts of the validation report shall be at least the following:

— the completed checklist signed by the EU aviation security validator and where applicable commented by the validated entity; and

— the declaration of commitments (Attachment 6-H3 to Implementing Regulation (EU) 2015/1998) signed by the validated entity; and

— an independence declaration (Attachment 11-A to Implementing Regulation (EU) 2015/1998) in respect of the entity validated signed by the EU aviation security validator.

Page numbering, the date of the EU aviation security validation and initialling on each page by the validator and the validated entity shall be the proof of the validation report's integrity.

The KC3 shall be able to use the report in its business relations with any ACC3 and any RA3.

By default the validation report shall be in English.

For those parts that cannot be assessed against the requirements of Implementing Regulation (EU) 2015/1998, baseline standards are the Standards and Recommended Practices (SARPs) of Annex 17 to the Convention on International Civil Aviation and the guidance material contained in the ICAO Aviation Security Manual (Doc 8973-Restricted).

Completion notes:

(1) All applicable and relevant parts of the checklist must be completed, in accordance with the business model and operations of the entity being validated. Where no information is available, this must be explained.

(2) After each part, the EU aviation security validator shall conclude if and to what extent the objectives of this part are met.

PART 1

Organisation and responsibilities

1.1. Date(s) of validation	
Use exact date format, such as from 01.10.2012 to 02.10.2012	
dd/mm/yyyy	
1.2. Date of previous validation where applicable.	
dd/mm/yyyy	

▼M2

Previous KC3 registration number, where available	
AEO certificate or C-TPAT status or other certifications, where available	
1.3. Aviation security validator information	
Name	
Company/Organisation/Authority	
Unique alphanumeric identifier (UAI)	
Email address	
Telephone number — including international codes	
1.4. Name of entity	
Name	
Company number (for example commercial register identification number, if applicable)	
Number/Unit/Building	
Street	
Town	
Postcode	
State (where relevant)	
Country	
P.O. Box address, if applicable	
1.5. Main address of organisation (if different from site to be validated)	
Number/Unit/Building	

▼M2

Street	
Town	
Postcode	
State (where relevant)	
Country	
P.O. Box address, if applicable	
1.6. Nature of business — Types of cargo processed	
What is the nature of business(es) — type of cargo processed in the applicant's premises?	
1.7. Is the applicant responsible for…?	
(a) production (b) packing (c) storage (d) despatch (e) other, please specify	
1.8. Approximate number of employees on site	
Number	
1.9. Name and title of person responsible for third country air cargo or air mail security	
Name	
Job title	
Email address	
Telephone number — including international codes	

PART 2

Organisation and responsibilities of the third country EU aviation security validated known consignor

Objective: No air cargo or air mail shall be carried to the EU or EEA without being subject to security controls. Cargo and mail delivered by a KC3 to an ACC3 or RA3 may only be accepted as secure cargo or mail if such security controls are applied by the KC3. Details of such controls are provided by the following Parts of this checklist.

The KC3 shall have procedures in place to ensure that appropriate security controls are applied to all EU or EEA bound air cargo and air mail and that secure cargo or mail is protected until being transferred to an ACC3 or a RA3. Security controls reasonably ensure that no prohibited articles are concealed in the consignment.

Reference: point 6.8.3 of the Annex to Implementing Regulation (EU) 2015/1998.

▼M2

2.1. Has the entity established a security programme?	
YES or NO	
If NO, go directly to point 2.5	
2.2. Entity security programme information	
Date — use exact format dd/mm/yyyy	
Version	
Is the security programme submitted to or approved by the appropriate authority of the state in which the entity is located? If YES, please describe the process.	
2.3. Does the security programme sufficiently cover the elements mentioned in parts 4 to 11 of the checklist?	
YES or NO	
If NO, describe why, detailing the reasons	
2.4. Is the security programme conclusive, robust and complete?	
YES or NO	
If NO, specify the reasons	
2.5. Has the entity established a process to ensure that EU or EEA bound air cargo or air mail is submitted to appropriate security controls before being transferred to an ACC3 or an RA3?	
YES or NO	
If YES, describe the process	
2.6. Has the entity a management system (for example instruments, instructions) in place to ensure that the required security controls are implemented?	
YES or NO	
If YES, describe the management system and explain if it is approved, checked or provided by the appropriate authority or other entity.	
If NO, explain how the entity ensures that security controls are applied in the required manner.	

▼M2

2.7. Conclusions and general comments on the reliance, conclusiveness and robustness of the process.	
Comments from the entity	
Comments from the EU aviation security validator	

PART 3

Identifiable air cargo or air mail

Objective: To establish the point or place where cargo or mail becomes identifiable as air cargo or air mail.

3.1. By inspection of the production, packing, storage, selection, despatch and any other relevant areas, ascertain where and how a consignment of EU or EEA bound air cargo or air mail becomes identifiable as such.	
Describe	
Comments from the entity	
Comments from the EU aviation security validator	

Please note that detailed information should be given on the protection of identifiable air cargo or air mail from unauthorised interference or tampering in Parts 6 to 9.

PART 4

Staff recruitment and training

Objective: In order to ensure that the required security controls are applied, the KC3 shall assign responsible and competent staff to work in the field of securing air cargo or air mail. Staff with access to identifiable air cargo shall possess all the competencies required to perform their duties and be appropriately trained.

In order to fulfil that objective, the KC3 shall have procedures in place to ensure that all staff (such as permanent, temporary, agency staff, drivers) with direct and unescorted access to air cargo or air mail to which security controls are being or have been applied:

(a) have been subject to initial and recurrent pre-employment checks or background checks, which are at least in accordance with the requirements of the local authorities of the KC3 premises validated; and

(b) have completed initial and recurrent security training to be aware of their security responsibilities in accordance with the requirements of the local authorities of the KC3 premises validated.

▼**M2**

Note:

— A background check means a check of a person's identity and previous experience, including where legally permissible, any criminal history as part of the assessment of an individual's suitability to implement a security control or for unescorted access to a security restricted area (ICAO Annex 17 definition).

— A pre-employment check shall establish the person's identity on the basis of documentary evidence, cover employment, education and any gaps during at least the preceding five years, and require the person to sign a declaration detailing any criminal history in all states of residence during at least the preceding 5 years (Union definition).

Reference: point 6.8.3.1 of the Annex to Implementing Regulation (EU) 2015/1998.

4.1. Is there a procedure ensuring that all staff with access to identifiable air cargo or air mail is subject to a pre-employment check that assesses background check and competence?	
YES or NO	
If YES, indicate the number of preceding years taken into account for the pre-employment check and state which entity carries it out.	
4.2. Does this procedure include?	
☐ background check ☐ pre-employment check ☐ check of criminal records ☐ interviews ☐ other (provide details) Explain the elements, indicate which entity carries this element out and where applicable, indicate the preceding timeframe that is taken into account.	
4.3. Is there a procedure ensuring that the person responsible for the application and supervision of the implementation of security controls at the site is subject to a pre-employment check that assesses background and competence?	
YES or NO	
If YES, indicate the number of preceding years taken into account for the pre-employment check and state which entity carries it out.	

▼M2

4.4. Does this procedure include?	
☐ background check ☐ pre-employment check ☐ check of criminal records ☐ interviews ☐ other (provide details) Explain the elements, indicate which entity carries this element out and where applicable, indicate the preceding timeframe that is taken into account.	
4.5. Do staff with access to identifiable air cargo/air mail receive training before being given access to identifiable air cargo or air mail?	
YES or NO	
If YES, describe the elements and duration of the training	
4.6. Do staff referred to in point 4.5 receive recurrent training?	
YES or NO	
If YES, specify the elements and the frequency of the recurrent training	
4.7. Conclusion: do measures concerning staff recruitment and training ensure that all staff with access to identifiable EU or EEA bound air cargo or air mail have been properly recruited and trained to a standard sufficient to be aware of their security responsibilities?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

PART 5

Physical security

Objective: The KC3 shall have procedures in place to ensure identifiable air cargo or air mail bound for the EU or EEA is protected from unauthorised interference or any tampering. If such cargo or mail is not protected, it cannot be forwarded to an ACC3 or RA3 as secure cargo or mail.

▼M2

The entity has to demonstrate how its site or its premises are protected and that relevant access control procedures are in place. It is essential that access to the area where identifiable air cargo or air mail is processed or stored, is controlled. All doors, windows and other points of access to secure EU or EEA bound air cargo or air mail need to be secured or subject to access control.

Physical security can be, but is not limited to:

— physical obstacles such as fencing or barriers,

— technology using alarms and/or CCTV systems,

— human security such as staff dedicated to carry out surveillance activities.

Reference: point 6.8.3.1 of the Annex to Implementing Regulation (EU) 2015/1998.

5.1. Are all access points to identifiable air cargo/air mail subject to access control and is access limited to authorised persons?	
YES or NO	
If YES, how is access controlled? Explain and describe. Multiple answers may be possible. ☐ by security staff ☐ by other staff ☐ manual checking if persons are allowed to enter the area ☐ electronic access control systems ☐ other, specify	
If YES, how is it ensured that a person is authorised to enter the area? Explain and describe. Multiple answers may be possible. — use of a company identification card — use of another type of identification card such as passport or driver's licence — list of authorised persons used by (security) staff — electronic authorisation, e.g. by use of a chip; — distribution of keys or access codes only to authorised personnel — other, specify	

▼M2

5.2. Are all access points to identifiable air cargo or air mail secured? This includes access points which are not permanent in use and points which are normally not used as access points, such as windows.	
YES or NO	
If YES, how are these points secured? Explain and describe. Multiple answers may be possible. — presence of security staff — electronic access control systems which allow access to one person at a time — barriers, for example shutters or locks — CCTV system — intruder detection system	
5.3. Are there additional measures to enhance the security of the premises in general?	
YES or NO	
If YES, explain and describe what they are ☐ fencing or barriers ☐ CCTV system ☐ intruder detection system ☐ surveillance and patrols ☐ other, specify	
5.4. Is the building of solid construction?	
YES or NO	
5.5. Conclusion: Are the measures taken by the entity sufficient to prevent unauthorised access to those parts of the site and premises where identifiable EU or EEA bound air cargo or air mail is processed or stored?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

▼M2

PART 6

Production

Objective: The KC3 shall have procedures in place to ensure identifiable air cargo or air mail bound for the EU or EEA is protected from unauthorised interference or any tampering during the production process. If such cargo or mail is not protected, it cannot be forwarded to an ACC3 or RA3 as secure cargo or mail.

The entity has to demonstrate that access to the production area is controlled and the production process is supervised. If the product becomes identifiable as EU or EEA bound air cargo or air mail in the course of production, the entity has to show that measures are taken to protect air or cargo or air mail from unauthorised interference or tampering from this stage.

Answer these questions where the product can be identified as EU or EEA bound air cargo/air mail in the course of the production process.

6.1. Is access to the production area controlled and limited to authorised persons?	
YES or NO	
If YES, explain how the access is controlled and limited to authorised persons	
6.2. Is the production process supervised?	
YES or NO	
If YES, explain how it is supervised	
6.3. Are controls in place to prevent tampering at the stage of production?	
YES or NO	
If YES, describe	
6.4. Conclusion: Are measures taken by the entity sufficient to protect identifiable EU or EEA bound air cargo or air mail from unauthorised interference or tampering during production?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

PART 7

Packing

Objective: The KC3 shall have procedures in place to ensure identifiable air cargo or air mail bound for the EU or EEA is protected from unauthorised interference or any tampering during the packing process. If such cargo or mail is not protected, it cannot be forwarded to an ACC3 or RA3 as secure cargo or mail.

▼**M2**

The entity has to demonstrate that access to the packing area is controlled and the packing process is supervised. If the product becomes identifiable as EU or EEA bound air cargo or air mail in the course of packing, the entity has to show that measures are taken to protect air cargo/air mail from unauthorised interference or tampering from this stage. All finished goods need to be checked prior to packing.

Answer these questions where the product can be identified as EU or EEA bound air cargo/air mail in the course of the packing process.

7.1. Is access to the packing area controlled and limited to authorised persons?	
YES or NO	
If YES, explain how the access is controlled and limited to authorised persons	
7.2. Is the packing process supervised?	
YES or NO	
If YES, explain how it is supervised	
7.3. Are controls in place to prevent tampering at the stage of packing?	
YES or NO	
If YES, describe	
7.4. Describe the finished outer packaging:	
(a) Is the finished outer packing robust?	
YES or NO	
Describe	
(b) Is the finished outer packaging tamper evident?	
YES or NO	
If YES, describe which process is used to make the packaging tamper evident, for example by use of numbered seals, special stamps or security tape.	
If NO, describe what protection measures that ensure the integrity of the consignments are taken.	
7.5. Conclusion: Are measures taken by the entity sufficient to protect identifiable EU or EEA bound air cargo or air mail from unauthorised interference or tampering during packing?	
YES or NO	

▼M2

If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

PART 8

Storage

Objective: The KC3 shall have procedures in place to ensure identifiable air cargo or air mail bound for the EU or EEA is protected from unauthorised interference or any tampering during storage. If such cargo or mail is not protected, it cannot be forwarded to an ACC3 or RA3 as secure cargo or mail.

The entity has to demonstrate that access to the storage area is controlled. If the product becomes identifiable as EU or EEA bound air cargo or air mail while being stored, the entity has to show that measures are taken to protect air cargo or air mail from unauthorised interference or tampering as from this stage.

Answer these questions where the product can be identified as EU or EEA bound air cargo/air mail in the course of the storage process.

8.1. Is access to the storage area controlled and limited to authorised persons?	
YES or NO	
If YES, explain how the access is controlled and limited to authorised persons	
8.2. Is the finished and packed air cargo or air mail stored securely and checked for tampering?	
YES or NO	
If YES, describe	
If NO, explain how the entity ensures that the finished and packed EU or EEA bound air cargo and air mail is protected against unauthorised interference and any tampering.	
8.3. Conclusion: Are measures taken by the entity sufficient to protect identifiable EU or EEA bound air cargo or air mail from unauthorised interference or tampering during storage?	
YES or NO	
If NO, specify reasons	

▼M2

Comments from the entity	
Comments from the EU aviation security validator	

PART 9

Despatch

Objective: The KC3 shall have procedures in place to ensure identifiable air cargo or air mail bound for the EU or EEA is protected from unauthorised interference or any tampering during the despatch process. If such cargo or mail is not protected, it must not be forwarded to an ACC3 or RA3 as secure cargo or mail.

The entity has to demonstrate that access to the despatch area is controlled. If the product becomes identifiable as EU or EEA bound air cargo or air mail in the course of despatch, the entity has to show that measures are taken to protect air cargo or air mail from unauthorised interference or tampering from this stage.

Answer these questions where the product can be identified as EU/EEA bound air cargo or air mail in the course of the despatch process.

9.1. Is access to the despatch area controlled and limited to authorised persons?	
YES or NO	
If YES, explain how the access is controlled and limited to authorised persons	
9.2. Who has access to the despatch area? Multiple answers may be possible.	
☐ employees of the entity ☐ drivers ☐ visitors ☐ contractors ☐ others, specify	
9.3. Is the despatch process supervised?	
YES or NO	
If YES, explain how it is supervised	
9.4. Are controls in place to prevent tampering in the despatch area?	
YES or NO	
If YES, describe	
9.5. Conclusion: Are measures taken by the entity sufficient to protect identifiable EU or EEA bound air cargo or air mail from unauthorised interference or tampering during the despatch process?	
YES or NO	

▼M2

If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

PART 10

Consignments from other sources

Objective: The KC3 shall have procedures in place to ensure that cargo or mail which it has not originated itself, shall not be forwarded to an ACC3 or an RA3 as secure cargo or mail.

A KC3 may pass consignments which it has not itself originated to a RA3 or an ACC3, provided that following conditions are met:

(a) they are separated from consignments which it has originated; and

(b) the origin is clearly indicated on the consignment or an accompanying documentation.

All such consignments must be screened by an RA3 or ACC3 before they are loaded onto an aircraft.

10.1. Does the entity accept consignments of cargo or mail intended for carriage by air from any other entity?	
YES or NO	
If YES, how are these consignments kept separate from the company's own cargo or mail and how are they identified to the regulated agent or haulier?	
Comments from the entity	
Comments from the EU aviation security validator.	

PART 11

Documentation

Objective: The KC3 shall ensure that the documentation accompanying a consignment to which the KC3 has applied security controls (for example protection), contains at least:

(a) the unique alphanumeric identifier received from the designating appropriate authority; and

(b) the content of the consignment.

The documentation accompanying the consignment may either be in an electronic format or in writing.

Reference: point 6.8.3.4 of the Annex to Implementing Regulation (EU) 2015/1998

▼M2

11.1. Does the entity ensure that appropriate accompanying documentation is established, containing the UAI received from the designating appropriate authority and a description of the consignment?	
YES or NO	
If NO, explain	
11.2. Conclusion: Is the documentation process sufficient to ensure that cargo or mail is provided with proper accompanying documentation?	
YES or NO	
If NO, specify reason	
Comments from the entity	
Comments from EU aviation security validator	

PART 12

Transportation

Objective: The KC3 shall have procedures in place in order to ensure identifiable air cargo or air mail bound for the EU or EEA is protected from unauthorised interference or any tampering during transportation. If such cargo or mail is not protected, it must not be accepted by an ACC3 or RA3 as secure cargo or mail.

During transportation, the KC3 is responsible for the protection of the secure consignments. This includes cases where the transportation is undertaken by another entity, such as a freight forwarder, on its behalf. This does not include cases whereby the consignments are transported under the responsibility of an ACC3 or RA3.

Answer these questions where the product can be identified as EU or EEA bound air cargo or air mail when transported.

12.1. How is the air cargo or air mail conveyed to the ACC3 or RA3?	
(a) Validated entity's own transport?	
YES or NO	
(b) ACC3's or RA3's transport?	
YES or NO	
(c) Contractor used by the validated entity?	
YES or NO	

▼M2

12.2. Is the air cargo or air mail tamper evidently packed?	
YES or NO	
If YES, how	
12.3. Is the vehicle sealed or locked before transportation?	
YES or NO	
If YES, how	
12.4. Where numbered seals are used, is access to the seals controlled and are the numbers recorded?	
YES or NO	
If YES, specify how	
12.5. If applicable, does the respective haulier sign the haulier declaration?	
YES or NO	
12.6. Has the person transporting the cargo been subject to specific security controls and awareness training before being authorised to transport secured air cargo or air mail, or both?	
YES or NO	
If YES, please describe what kind of security controls (for example, pre-employment check, background check) and what kind of training (for example, security awareness training, etc.)	
12.7. Conclusion: Are the measures sufficient to protect air cargo or air mail from unauthorised interference during transportation?	
YES or NO	
If NO, specify reasons	
Comments from the entity	
Comments from the EU aviation security validator	

PART 13

Compliance

Objective: After assessing the twelve previous parts of this checklist, the EU aviation security validator has to conclude whether its on-site verification confirms the implementation of the security controls in compliance with the objectives listed in this checklist for EU or EEA bound air cargo or air mail.

▼**M2**

Two different scenarios are possible. The EU aviation security validator concludes that the entity:

(1) has succeeded in complying with the objectives referred to in this checklist. A validation report shall be delivered to the designating appropriate authority and to the validated entity within a maximum of one month after the on-site verification;

(2) has failed in complying with the objectives referred to in this checklist. In that case, the entity is not authorised to deliver air cargo or mail for EU or EEA destination to an ACC3 or RA3 without it being screened by an authorised party. It shall receive a copy of the completed checklist stating the deficiencies.

The EU aviation security validator has to keep in mind that the assessment is based on an overall objective-based compliance methodology.

12.1. General conclusion: Indicate the scenario closest to the situation validated	
1 or 2	
Comments from EU aviation security validator	
Comments from the entity	

Name of the validator:

Date:

Signature:

▼M2

ANNEX

List of persons and entities visited and interviewed

Providing the name of the entity, the name and the position of the contact person and the date of the visit or interview.

Name of entity	Name of contact person	Position of contact person	Date of visit or interview

▼M15

———————

▼B

ATTACHMENT 6-E

HAULIER DECLARATION

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council ([1]) and its implementing acts,

▼M16

When collecting, carrying, storing and delivering air cargo/mail to which security controls have been applied [on behalf of *name of regulated agent/air carrier applying security controls for cargo or mail/known consignor*], I confirm that the following security procedures will be adhered to:

▼M15

— All staff who performs transport of cargo and mail will have received general security awareness training in accordance with point 11.2.7. Additionally, if such staff is also granted unsupervised access to cargo and mail to which the required security controls have been applied it will have received security training in accordance with point 11.2.3.9;

([1]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

▼B

— The integrity of all staff being recruited with access to this air cargo/mail will be verified. This verification shall include at least a check of the identity (if possible by photographic identity card, driving licence or passport) and a check of the curriculum vitae and/or provided references;

— Load compartments in vehicles will be sealed or locked. Curtain sided vehicles will be secured with TIR cords. The load areas of flatbed trucks will be kept under observation when air cargo is being transported;

— Immediately prior to loading, the load compartment will be searched and the integrity of this search maintained until loading is completed;

— Each driver will carry an identity card, passport, driving licence or other document, containing a photograph of the person, which has been issued or recognised by the national authorities;

— Drivers will not make unscheduled stops between collection and delivery. Where this is unavoidable, the driver will check the security of the load and the integrity of locks and/or seals on his return. If the driver discovers any evidence of interference, he will notify his supervisor and the air cargo/mail will not be delivered without notification at delivery;

— Transport will not be subcontracted to a third party, unless the third party:

▼M16

(a) has a haulier agreement with the regulated agent or known consignor responsible for the transport [same name as above]; or

▼B

(b) is approved or certified by the appropriate authority; or

▼M16

(c) has a haulier agreement with the undersigned haulier requiring that the third party will not subcontract further and implements the security procedures contained in this declaration. The undersigned haulier retains full responsibility for the entire transport on behalf of the regulated agent or known consignor; and

▼B

— No other services (e.g. storage) will be sub-contracted to any other party other than a regulated agent or an entity that has been certified or approved and listed for the provision of these services by the appropriate authority.

▼B

I accept full responsibility for this declaration.

Name:

Position in company:

Name and address of the company:

Date:

Signature:

▼M7

ATTACHMENT 6-F

CARGO AND MAIL

6-Fi

THIRD COUNTRIES, AS WELL AS OTHER COUNTRIES AND TERRITORIES TO WHICH, IN ACCORDANCE WITH ARTICLE 355 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, TITLE VI OF PART THREE OF THAT TREATY DOES NOT APPLY, THAT ARE RECOGNISED AS APPLYING SECURITY STANDARDS EQUIVALENT TO THE COMMON BASIC STANDARDS ON CIVIL AVIATION SECURITY

As regards cargo and mail, the following third countries have been recognised as applying security standards equivalent to the common basic standards on civil aviation security:

Montenegro

▼M13

Republic of Serbia

▼M7

United Kingdom of Great Britain and Northern Ireland

The Commission shall notify without delay the appropriate authorities of the Member States if it has information indicating that security standards applied by the third country or other country or territory concerned with a significant impact on overall levels of aviation security in the Union are no longer equivalent to the common basic standards of the Union.

The appropriate authorities of the Member States shall be notified without delay when the Commission has information about actions, including compensatory measures, confirming that the equivalency of relevant security standards applied by the third country or other country or territory concerned is re-established.

6-Fii

THIRD COUNTRIES, AS WELL AS OTHER COUNTRIES AND TERRITORIES TO WHICH, IN ACCORDANCE WITH ARTICLE 355 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, TITLE VI OF PART THREE OF THAT TREATY DOES NOT APPLY, FOR WHICH ACC3 DESIGNATION IS NOT REQUIRED, ARE LISTED IN COMMISSION IMPLEMENTING DECISION C(2015)8005.

6-Fiii

VALIDATION ACTIVITIES OF THIRD COUNTRIES, AS WELL AS OF OTHER COUNTRIES AND TERRITORIES TO WHICH, IN ACCORDANCE WITH ARTICLE 355 OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, TITLE VI OF PART THREE OF THAT TREATY DOES NOT APPLY, THAT ARE RECOGNISED AS EQUIVALENT TO EU AVIATION SECURITY VALIDATION.

No provisions adopted yet.

▼B

ATTACHMENT 6-G

PROVISIONS RELATING TO THIRD COUNTRY CARGO AND MAIL

The ACC3 security programme shall set out, as applicable and either for each third country airport individually or as a generic document specifying any variations at named third country airports:

(a) description of measures for air cargo and mail;

(b) procedures for acceptance;

(c) regulated agent scheme and criteria;

(d) known consignor scheme and criteria;

(e) account consignor scheme and criteria;

(f) standard of screening;

(g) location of screening;

(h) details of screening equipment;

(i) details of operator or service provider;

(j) list of exemptions from security screening;

(k) treatment of high risk air cargo and mail.

▼M2

ATTACHMENT 6-H1

DECLARATION OF COMMITMENTS — EU AVIATION SECURITY VALIDATED ACC3

On behalf of [name of air carrier] I take note of the following:

This report establishes the level of security applied to EU or EEA bound air cargo operations in respect of the security standards listed in the checklist or referred to therein.

[name of air carrier] can only be designated ‘air cargo or mail carrier operating into the Union from a third country airport’ (ACC3) once an EU aviation security validation report has been submitted to and accepted by the appropriate authority of a Member State of the European Union or Iceland, Norway or Switzerland for that purpose, and the details of the ACC3 have been entered in the Union database on supply chain security.

If a non-compliance in the security measures the report refers to is identified by the appropriate authority of an EU Member State or by the European Commission, this could lead to the withdrawal of [name of air carrier] designation as ACC3 already obtained for this airport which will prevent [name of air carrier] transport air cargo or mail into the EU or EEA area from this airport.

The report is valid for five years and shall therefore expire on … at the latest.

On behalf of [air carrier] I declare that:

▼M2

(1) [name of air carrier] will accept appropriate follow-up action for the purpose of monitoring the standards confirmed by the report.

(2) I will provide the designating appropriate authority with the relevant details promptly but at least within 15 days if:

(a) any changes to [name of air carrier] security programme occur;

(b) the overall responsibility for security is assigned to anyone other than the person named in point 1.7 of Attachment 6-C3 to Implementing Regulation (EU) 2015/1998;

(c) there are any other changes to premises or procedures likely to significantly impact on security;

(d) the air carrier ceases trading, no longer deals with air cargo or mail bound to the Union, or can no longer meet the requirements of the relevant Union legislation that have been validated in this report.

(3) [name of air carrier] will maintain the security level confirmed in this report as compliant with the objective set out in the checklist and, where appropriate, implement and apply any additional security measures required to be designated ACC3 where security standards were identified as insufficient, until the subsequent validation of [name of air carrier] activities.

(4) [name of air carrier] will inform the designating appropriate authority in case it is not able to request, obtain or ensure the application of appropriate security controls in respect of cargo or mail it accepts for carriage into the EU or EEA area, or it cannot exercise effective oversight on its supply chain.

On behalf of [name of air carrier] I accept full responsibility for this declaration.

Name:

Position in company:

Date:

Signature:

ATTACHMENT 6-H2

DECLARATION OF COMMITMENTS — THIRD COUNTRY EU AVIATION SECURITY VALIDATED REGULATED AGENT (RA3)

On behalf of [name of entity] I take note of the following:

This report establishes the level of security applied to EU or EEA bound air cargo operations in respect of the security standards listed in the checklist or referred to therein.

[Name of entity] can only be designated ‘third country EU aviation security validated regulated agent’ (RA3) once an EU aviation security validation report has been submitted to and accepted by the appropriate authority of a Member State of the European Union or Iceland, Norway or Switzerland for that purpose, and the details of the RA3 have been entered in the Union database on supply chain security.

▼M2

If a non-compliance in the security measures the report refers to is identified by the appropriate authority of a Union Member State or by the European Commission, this could lead to the withdrawal of [name of entity] designation as a RA3 already obtained for this premises which will prevent [name of entity] from delivering secured air cargo or mail for EU or EEA destination to an ACC3 or another RA3.

The report is valid for three years and shall therefore expire on … at the latest.

On behalf of [name of entity] I declare that:

(1) [name of entity] will accept appropriate follow-up action for the purpose of monitoring the standards confirmed by the report.

(2) I will provide the designating appropriate authority with the relevant details promptly but at least within 15 days if:

(a) any changes to [name of entity] security programme occur;

(b) the overall responsibility for security is assigned to anyone other than the person named in point 1.9 of Attachment 6-C2 to Implementing Regulation (EU) 2015/1998;

(c) there are any other changes to premises or procedures likely to significantly impact on security;

(d) the company ceases trading, no longer deals with air cargo or mail bound to the European Union, or can no longer meet the requirements of the relevant Union legislation that have been validated in this report.

(3) [name of entity] will maintain the security level confirmed in this report as compliant with the objective set out in the checklist and, where appropriate, implement and apply any additional security measures required to be designated RA3 where security standards were identified as insufficient, until the subsequent validation of [name of entity] activities.

(4) [name of entity] will inform the ACC3s and RA3s to which it delivers secured air cargo and/or air mail if [name of entity] ceases trading, no longer deals with air cargo/air mail or can no longer meet the requirements validated in this report.

On behalf of [name of entity] I accept full responsibility for this declaration.

Name:

Position in company:

Date:

Signature:

ATTACHMENT 6-H3

DECLARATION OF COMMITMENTS — THIRD COUNTRY EU AVIATION SECURITY VALIDATED KNOWN CONSIGNOR (KC3)

On behalf of [name of entity] I take note of the following:

This report establishes the level of security applied to EU or EEA bound air cargo operations in respect of the security standards listed in the checklist or referred to therein.

▼M2

[Name of entity] can only be designated 'third country EU aviation security validated known consignor' (KC3) once an EU aviation security validation report has been submitted to and accepted by the appropriate authority of a Member State of the European Union or Iceland, Norway or Switzerland for that purpose, and the details of the KC3 have been entered in the Union database on supply chain security.

If a non-compliance in the security measures the report refers to is identified by the appropriate authority of a Union Member State or by the European Commission, this could lead to the withdrawal of [name of entity] designation as a KC3 already obtained for this premises which will prevent [name of entity] from delivering secured air cargo or mail for EU or EEA destination to an ACC3 or an RA3.

The report is valid for three years and shall therefore expire on … at the latest.

On behalf of [name of entity] I declare that:

(1) [name of entity] will accept appropriate follow-up action for the purpose of monitoring the standards confirmed by the report;

(2) I will provide the designating appropriate authority with the relevant details promptly but at least within 15 days if:

(a) any changes to [name of entity] security programme occur;

(b) the overall responsibility for security is assigned to anyone other than the person named in point 1.9 of Attachment 6-C4 to Implementing Regulation (EU) 2015/1998;

(c) there are any other changes to premises or procedures likely to significantly impact on security;

(d) the company ceases trading, no longer deals with air cargo/mail bound to the European Union, or can no longer meet the requirements of the relevant Union legislation that have been validated in this report.

(3) [name of entity] will maintain the security level confirmed in this report as compliant with the objective set out in the checklist and, where appropriate, implement and apply any additional security measures required to be designated KC3 where security standards were identified as insufficient, until the subsequent validation of [name of entity] activities.

(4) [name of entity] will inform the ACC3s and RA3s to which it delivers secured air cargo and/or air mail if [name of entity] ceases trading, no longer deals with air cargo/air mail or can no longer meet the requirements validated in this report.

On behalf of [name of entity] I accept full responsibility for this declaration.

Name:

Position in company:

Date:

Signature:

▼B

ATTACHMENT 6-I

Provisions for high risk cargo are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 6-J

Provisions for the use of screening equipment are laid down in Commission Implementing Decision C(2015) 8005.

7. AIR CARRIER MAIL AND AIR CARRIER MATERIALS

7.0 GENERAL PROVISIONS

Unless otherwise stated or unless the implementation of security controls as referred to in Chapters 4, 5 and 6, respectively, are ensured by an authority, airport operator, entity or another air carrier, an air carrier shall ensure the implementation of the measures set out in this Chapter as regards its air carrier mail and air carrier materials.

7.1 AIR CARRIER MAIL AND AIR CARRIER MATERIALS TO BE LOADED ONTO AN AIRCRAFT

7.1.1 Before being loaded into the hold of an aircraft, air carrier mail and air carrier materials shall either be screened and protected in accordance with Chapter 5 or be subjected to security controls and protected in accordance with Chapter 6.

7.1.2 Before being loaded into any part of an aircraft other than the hold, air carrier mail and air carrier materials shall be screened and protected in accordance with the provisions on cabin baggage in Chapter 4.

7.1.3 Air carrier mail and air carrier materials to be loaded onto an aircraft shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

7.2 AIR CARRIER MATERIALS USED FOR PASSENGER AND BAGGAGE PROCESSING

7.2.1 Air carrier materials which are used for the purposes of passenger and baggage processing and which could be used to compromise aviation security shall be protected or kept under surveillance in order to prevent unauthorised access.

Self-check-in and applicable Internet options allowed for use by passengers shall be considered as authorised access to such materials.

7.2.2 Discarded materials which could be used to facilitate unauthorised access or move baggage into the security restricted area or onto aircraft shall be destroyed or invalidated.

7.2.3 Departure control systems and check-in systems shall be managed in such a manner as to prevent unauthorised access.

Self-check-in allowed for use by passengers shall be considered as authorised access to such systems.

▼B

8. IN-FLIGHT SUPPLIES

8.0 GENERAL PROVISIONS

8.0.1 Unless otherwise stated, the authority, airport operator, air carrier or entity responsible in accordance with the national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 shall ensure the implementation of the measures set out in this Chapter.

8.0.2 For the purpose of this Chapter, 'in-flight supplies' means all items intended to be taken on board an aircraft for use, consumption or purchase by passengers or crew during a flight, other than:

(a) cabin baggage; and

(b) items carried by persons other than passengers; and

(c) air carrier mail and air carrier materials.

For the purpose of this Chapter, 'regulated supplier of in-flight supplies' means a supplier whose procedures meet common security rules and standards sufficient to allow delivery of in-flight supplies directly to aircraft.

For the purpose of this Chapter, 'known supplier of in-flight supplies' means a supplier whose procedures meet common security rules and standards sufficient to allow delivery of in-flight supplies to an air carrier or regulated supplier, but not directly to aircraft.

8.0.3 Supplies shall be considered as in-flight supplies from the time that they are identifiable as supplies to be taken on board an aircraft for use, consumption or purchase by passengers or crew during a flight.

8.0.4 The list of prohibited articles in in-flight supplies is the same as the one set out in Attachment 1-A. Prohibited articles shall be handled in accordance with point 1.6.

8.1 SECURITY CONTROLS

8.1.1 **Security controls — general provisions**

8.1.1.1 ►**M15** In-flight supplies shall be screened by or on behalf of an air carrier, a regulated supplier or an airport operator before being taken into a security restricted area, unless: ◄

(a) the required security controls have been applied to the supplies by an air carrier that delivers these to its own aircraft and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery at the aircraft; or

(b) the required security controls have been applied to the supplies by a regulated supplier and the supplies have been protected from unauthorised interference from the time that those controls were applied until arrival at the security restricted area or, where applicable, until delivery to the air carrier or another regulated supplier; or

(c) the required security controls have been applied to the supplies by a known supplier and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery to the air carrier or regulated supplier.

▼B

8.1.1.2 Where there is any reason to believe that in-flight supplies to which security controls have been applied have been tampered with or have not been protected from unauthorised interference from the time that those controls were applied, they shall be screened before being allowed into security restricted areas.

8.1.1.3 The security controls of in-flight supplies shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

8.1.2 **Screening**

8.1.2.1 When screening in-flight supplies, the means or method employed shall take into consideration the nature of the supplies and shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the supplies.

8.1.2.2 The screening of in-flight supplies shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

8.1.2.3 The following means or method of screening, either individually or in combination, shall be applied:

(a) visual check;

(b) hand search;

(c) x-ray equipment;

(d) EDS equipment;

(e) ETD equipment in combination with point (a);

▼M16

(f) explosive detection dogs in combination with point (a);

(g) EVD equipment applied in accordance with the relevant provisions contained in Attachment 6-J and in combination with point (a).

▼B

Where the screener cannot determine whether or not the item contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

8.1.3 **Approval of regulated suppliers**

8.1.3.1 Regulated suppliers shall be approved by the appropriate authority.

The approval as a regulated supplier shall be site specific.

Any entity that ensures the security controls as referred to in point 8.1.5 and delivers in-flight supplies directly to aircraft shall be approved as a regulated supplier. This shall not apply to an air carrier that applies these security controls itself and delivers supplies only to its own aircraft.

8.1.3.2 The following procedure shall apply for the approval of regulated suppliers:

(a) the entity shall seek approval from the appropriate authority of the Member State in which its site is located in order to be granted the status of regulated supplier.

The applicant shall submit a security programme to the appropriate authority concerned. The programme shall describe the methods and procedures which are to be followed by the supplier in order to comply with the requirements of point 8.1.5. The programme shall also describe how compliance with these methods and procedures is to be monitored by the supplier itself.

The applicant shall also submit the ‘Declaration of commitments — regulated supplier of in-flight supplies’ as contained in Attachment 8-A. This declaration shall be signed by the legal representative or by the person responsible for security.

▼M15

The signed declaration shall clearly state the location of the site or sites to which it refers and be retained by the appropriate authority concerned;

▼B

(b) the appropriate authority, or an EU aviation security validator acting on its behalf, shall examine the security programme and then make an on-site verification of the sites specified in order to assess whether the applicant complies with the requirements of point 8.1.5;

▼M2

(c) if the appropriate authority is satisfied with the information provided in accordance with points (a) and (b), it shall ensure that the necessary details of the regulated supplier are entered into the Union database on supply chain security not later than the next working day. When making the database entry the appropriate authority shall give each approved site a unique alphanumeric identifier in the standard format. If the appropriate authority is not satisfied, the reasons shall promptly be notified to the entity seeking approval as a regulated supplier;

(d) a regulated supplier shall not be considered as approved until its details are listed in the Union database on supply chain security.

▼B

8.1.3.3 A regulated supplier shall be re-validated at regular intervals not exceeding 5 years. This shall include an on-site verification in order to assess whether the regulated supplier still complies with the requirements of point 8.1.5.

An inspection at the premises of the regulated supplier by the appropriate authority in accordance with its national quality control programme may be considered as an on-site verification, provided that it covers all the requirements of point 8.1.5.

8.1.3.4 If the appropriate authority is no longer satisfied that the regulated supplier complies with the requirements of point 8.1.5, it shall withdraw the status of regulated supplier for the specified sites.

8.1.3.5 Without prejudice to the right of each Member State to apply more stringent measures in accordance with Article 6 of Regulation (EC) No 300/2008, a regulated supplier approved in accordance with point 8.1.3 shall be recognised in all Member States.

8.1.4 **Designation of known suppliers**

8.1.4.1 Any entity (‘the supplier’) that ensures the security controls as referred to in point 8.1.5 and delivers in-flight supplies, but not directly to aircraft, shall be designated as a known supplier by the operator or the entity to whom it delivers (‘the designating entity’). This shall not apply to a regulated supplier.

8.1.4.2 In order to be designated as a known supplier, the supplier must provide the designating entity with:

▼M15

(a) the ‘Declaration of commitments – known supplier of in-flight supplies’ as contained in Attachment 8-B. This declaration shall clearly state the location of the site or sites to which it refers and be signed by the legal representative; and

▼B

(b) the security programme covering the security controls as referred to in point 8.1.5.

8.1.4.3 All known suppliers must be designated on the basis of validations of:

(a) the relevance and completeness of the security programme in respect of point 8.1.5; and

(b) the implementation of the security programme without deficiencies.

▼B

If the appropriate authority or the designating entity is no longer satisfied that the known supplier complies with the requirements of point 8.1.5, the designating entity shall withdraw the status of known supplier without delay.

8.1.4.4 The appropriate authority shall define in its national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 if the validations of the security programme and its implementation shall be performed by a national auditor, an EU aviation security validator, or a person acting on behalf of the designating entity appointed and trained for that purpose.

Validations must be recorded and if not otherwise stated in this legislation, must take place before designation and repeated every 2 years thereafter.

If the validation is not done on behalf of the designating entity any record thereof must be made available to it.

8.1.4.5 The validation of the implementation of the security programme confirming the absence of deficiencies shall consist of either:

(a) an on-site visit of the supplier every 2 years; or

(b) regular checks upon reception of supplies delivered by that known supplier, starting after the designation, including:

— a verification that the person delivering supplies on behalf of the known supplier was properly trained; and

— a verification that the supplies are properly secured; and

— screening of the supplies in the same way as supplies coming from an unknown supplier.

These checks must be carried out in an unpredictable manner and take place at least either, once every three months or on 20 % of the known supplier's deliveries to the designating entity.

Option (b) may only be used if the appropriate authority defined in its national civil aviation security programme that the validation shall be performed by a person acting on behalf of the designating entity.

8.1.4.6 The methods applied and procedures to be followed during and after designation shall be laid down in the security programme of the designating entity.

8.1.4.7 The designating entity shall keep:

(a) a list of all known suppliers it has designated indicating the expiry date of their designation, and

(b) the signed declaration, a copy of the security programme, and any reports recording its implementation for each known supplier, at least until 6 months after the expiry of its designation.

Upon request, these documents shall be made available to the appropriate authority for compliance monitoring purposes.

8.1.5 **Security controls to be applied by an air carrier, a regulated supplier and a known supplier**

8.1.5.1 An air carrier, a regulated supplier and a known supplier of in-flight supplies shall:

(a) appoint a person responsible for security in the company; and

▼M15

(b) ensure that persons with access to in-flight supplies receive general security awareness training in accordance with point 11.2.7 before being given access to those supplies. In addition, ensure that persons implementing screening of in-flight supplies receive training in accordance with point 11.2.3.3 and persons implementing other security controls in respect of in-flight supplies receive training in accordance with point 11.2.3.10; and

▼B

(c) prevent unauthorised access to its premises and in-flight supplies; and

(d) reasonably ensure that no prohibited articles are concealed in in-flight supplies; and

(e) apply tamper-evident seals to, or physically protect, all vehicles and/or containers that transport in-flight supplies.

Point (e) shall not apply during airside transportation.

8.1.5.2 If a known supplier uses another company that is not a known supplier to the air carrier or regulated supplier for transporting supplies, the known supplier shall ensure that all security controls listed in point 8.1.5.1 are adhered to.

8.1.5.3 The security controls to be applied by an air carrier and a regulated supplier shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

8.2 PROTECTION OF IN-FLIGHT SUPPLIES

Detailed provisions for the protection of in-flight supplies are laid down in Commission Implementing Decision C(2015) 8005.

8.3 ADDITIONAL SECURITY PROVISIONS FOR IN-FLIGHT SUPPLIES OF LAGS AND STEBS

8.3.1 In-flight supplies of STEBs shall be delivered in tamper-evident packaging to an airside area or to a security restricted area.

8.3.2 After first reception on airside or in a security restricted area and until their final sale on the aircraft, LAGs and STEBs shall be protected from unauthorised interference.

8.3.3 Detailed provisions for the additional security provisions for in- flight supplies of LAGs and STEBs are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 8-A

DECLARATION OF COMMITMENTS

REGULATED SUPPLIER OF IN-FLIGHT SUPPLIES

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council [1] and its implementing acts,

I declare that,

— to the best of my knowledge, the information contained in the company's security programme is true and accurate,

— the practices and procedures set out in this security programme will be implemented and maintained at all sites covered by the programme,

[1] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

▼B

— this security programme will be adjusted and adapted to comply with all future relevant changes to Union legislation, unless [name of company] informs [name of appropriate authority] that it no longer wishes to deliver in-flight supplies directly to aircraft (and thus no longer wishes to trade as a regulated supplier),

— [name of company] will inform [name of appropriate authority] in writing of:

(a) minor changes to its security programme, such as company name, person responsible for security or contact details, promptly but at least within 10 working days; and

(b) major planned changes, such as new screening procedures, major building works which might affect its compliance with relevant Union legislation or change of site/address, at least 15 working days prior to their commencement/the planned change,

— in order to ensure compliance with relevant Union legislation, [name of company] will cooperate fully with all inspections, as required, and provide access to all documents, as requested by inspectors,

— [name of company] will inform [name of appropriate authority] of any serious security breaches and of any suspicious circumstances which may be relevant to in-flight supplies, in particular any attempt to conceal prohibited articles in supplies,

— [name of company] will ensure that all relevant staff receive training in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998 and are aware of their security responsibilities under the company's security programme; and

— [name of company] will inform [name of appropriate authority] if:

(a) it ceases trading;

(b) it no longer delivers in-flight supplies directly to aircraft; or

(c) it can no longer meet the requirements of the relevant Union legislation.

I shall accept full responsibility for this declaration.

Name:

Position in company:

Date:

Signature:

ATTACHMENT 8-B

DECLARATION OF COMMITMENTS

KNOWN SUPPLIER OF IN-FLIGHT SUPPLIES

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council [1] and its implementing acts,

I declare that,

— [name of company] will

(a) appoint a person responsible for security in the company; and

[1] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

▼M15

(b) ensure that persons with access to in-flight supplies receive general security awareness training in accordance with point 11.2.7 before being given access to those supplies. In addition, ensure that persons implementing security controls other than screening in respect of in-flight supplies receive training in accordance with point 11.2.3.10; and

▼B

(c) prevent unauthorised access to its premises and in-flight supplies; and

(d) reasonably ensure that no prohibited articles are concealed in in-flight supplies; and

(e) apply tamper-evident seals to, or physically protect, all vehicles and/or containers that transport in-flight supplies (this point will not apply during airside transportation).

When using another company that is not a known supplier to the air carrier or regulated supplier for transporting supplies, [name of company] will ensure that all security controls listed above are adhered to,

— in order to ensure compliance, [name of company] will cooperate fully with all inspections, as required, and provide access to all documents, as requested by inspectors,

— [name of company] will inform [the air carrier or regulated supplier to whom it delivers in-flight supplies] of any serious security breaches and of any suspicious circumstances which may be relevant to in-flight supplies, in particular any attempt to conceal prohibited articles in supplies,

— [name of company] will ensure that all relevant staff receive training in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998 and are aware of their security responsibilities, and

— [name of company] will inform [the air carrier or regulated supplier to whom it delivers in-flight supplies] if:

(a) it ceases trading; or

(b) it can no longer meet the requirements of the relevant Union legislation.

I shall accept full responsibility for this declaration.

Legal representative

Name:

Date:

Signature:

9. **AIRPORT SUPPLIES**

9.0 GENERAL PROVISIONS

9.0.1 Unless otherwise stated or unless the implementation of screening is ensured by an authority or entity, an airport operator shall ensure the implementation of the measures set out in this Chapter.

▼B

9.0.2 For the purpose of this Chapter,

(a) ‘airport supplies’ mean all items intended to be sold, used or made available for any purpose or activity in the security restricted area of airports, other than ‘items carried by persons other than passengers’;

(b) ‘known supplier of airport supplies’ means a supplier whose procedures meet common security rules and standards sufficient to allow delivery of airport supplies to security restricted areas.

9.0.3 Supplies shall be considered as airport supplies from the time that they are identifiable as supplies to be sold, used or made available in security restricted areas of airports.

9.0.4 The list of prohibited articles in airport supplies is the same as the one set out in Attachment 1-A. Prohibited articles shall be handled in accordance with point 1.6.

9.1 SECURITY CONTROLS

9.1.1 **Security controls — general provisions**

9.1.1.1 ►M15 Airport supplies shall be screened by or on behalf of an airport operator or a regulated supplier before being taken into a security restricted area, unless: ◄

(a) the required security controls have been applied to the supplies by an airport operator that delivers these to its own airport and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery to the security restricted area; or

(b) the required security controls have been applied to the supplies by a known supplier or regulated supplier and the supplies have been protected from unauthorised interference from the time that those controls were applied until delivery to the security restricted area.

9.1.1.2 Airport supplies which originate in the security restricted area may be exempted from these security controls.

9.1.1.3 Where there is any reason to believe that airport supplies to which security controls have been applied have been tampered with or have not been protected from unauthorised interference from the time that those controls were applied, they shall be screened before being allowed into security restricted areas.

9.1.2 **Screening**

9.1.2.1 When screening airport supplies, the means or method employed shall take into consideration the nature of the supply and shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the supply.

9.1.2.2 The screening of airport supplies shall also be subject to the additional provisions laid down in Commission Implementing Decision C(2015) 8005.

9.1.2.3 The following means or method of screening, either individually or in combination, shall be applied:

(a) visual check;

(b) hand search;

▼B

(c) x-ray equipment;

(d) EDS equipment;

(e) ETD equipment in combination with point (a);

▼M16

(f) explosive detection dogs in combination with point (a);

(g) EVD equipment applied in accordance with the relevant provisions contained in Attachment 6-J and in combination with point (a).

▼B

Where the screener cannot determine whether or not the item contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

9.1.3 **Designation of known suppliers**

9.1.3.1 Any entity (‘the supplier’) that ensures the security controls as referred to in point 9.1.4 and delivers airport supplies shall be designated as a known supplier by the airport operator.

9.1.3.2 In order to be designated as a known supplier, the supplier must provide the airport operator with:

▼M15

(a) the ‘Declaration of commitments – known supplier of airport supplies’ as contained in Attachment 9-A. This declaration shall clearly state the location of the site or sites to which it refers and be signed by the legal representative; and

▼B

(b) the security programme covering the security controls as referred to in point 9.1.4.

▼M15

9.1.3.3 All known suppliers must be designated on the basis of validations of:

(a) the relevance and completeness of the security programme in respect of point 9.1.4; and

(b) the implementation of the security programme without deficiencies.

As a legal proof of the designation, the appropriate authority may require airport operators to enter the necessary details of the known suppliers they designate into the ‘Union database on supply chain security’ not later than the next working day. When making the database entry, the airport operator shall give each designated site a unique alphanumeric identifier in the standard format.

Access into the security restricted areas of airport supplies may only be granted after having established the status of the supplier. This shall be done by verifying in the ‘Union database on supply chain security’, if applicable, or by using an alternative mechanism delivering the same objective.

If the appropriate authority or the airport operator is no longer satisfied that the known supplier complies with the requirements of point 9.1.4, the airport operator shall withdraw the status of known supplier without delay.

▼B

9.1.3.4 The appropriate authority shall define in its national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 if the validations of the security programme and its implementation shall be performed by a national auditor, an EU aviation security validator, or a person acting on behalf of the airport operator appointed and trained for that purpose.

Validations must be recorded and if not otherwise stated in this legislation, must take place before designation and repeated every 2 years thereafter.

If the validation is not done on behalf of the airport operator any record thereof must be made available to it.

▼B

9.1.3.5 The validation of the implementation of the security programme confirming the absence of deficiencies shall consist of either:

(a) an on-site visit of the supplier every 2 years; or

(b) regular checks upon access to the security restricted area of supplies delivered by that known supplier, starting after the designation, including:

— a verification that the person delivering supplies on behalf of the known supplier was properly trained; and

— a verification that the supplies are properly secured; and

— screening of the supplies in the same way as supplies coming from an unknown supplier.

These checks must be carried out in an unpredictable manner and take place at least either once every three months or on 20 % of the known supplier's deliveries to the airport operator.

Option (b) may only be used if the appropriate authority defined in its national civil aviation security programme that the validation shall be performed by a person acting on behalf of the airport operator.

9.1.3.6 The methods applied and procedures to be followed during and after designation shall be laid down in the security programme of the airport operator.

9.1.3.7 The airport operator shall keep:

(a) a list of all known suppliers it has designated indicating the expiry date of their designation, and

(b) the signed declaration, a copy of the security programme, and any reports recording its implementation for each known supplier, at least until 6 months after the expiry of its designation.

Upon request, these documents shall be made available to the appropriate authority for compliance monitoring purposes.

9.1.4 **Security controls to be applied by a known supplier or airport operator**

9.1.4.1 A known supplier of airport supplies or airport operator delivering airport supplies to the security restricted area shall:

(a) appoint a person responsible for security in the company; and

▼M15

(b) ensure that persons with access to airport supplies receive general security awareness training in accordance with point 11.2.7 before being given access to those supplies. In addition, ensure that persons implementing screening of airport supplies receive training in accordance with point 11.2.3.3 and persons implementing other security controls in respect of airport supplies receive training in accordance with point 11.2.3.10; and

▼B

(c) prevent unauthorised access to its premises and airport supplies; and

(d) reasonably ensure that no prohibited articles are concealed in airport supplies; and

(e) apply tamper-evident seals to, or physically protect, all vehicles and/or containers that transport airport supplies.

Point (e) shall not apply during airside transportation.

▼B

9.1.4.2 If a known supplier uses another company that is not a known supplier to the airport operator for transporting supplies to the airport, the known supplier shall ensure that all security controls listed in this point are adhered to.

9.2 PROTECTION OF AIRPORT SUPPLIES

Detailed provisions for the protection of airport supplies are laid down in Commission Implementing Decision C(2015) 8005.

9.3 ADDITIONAL SECURITY PROVISIONS FOR SUPPLIES OF LAGS AND STEBS

9.3.1 Supplies of STEBs shall be delivered in tamper-evident packaging to an airside area beyond the point where boarding passes are controlled or to a security restricted area.

9.3.2 After first reception on airside or in a security restricted area and until their final sale at the outlet, LAGs and STEBs shall be protected against unauthorised interference.

9.3.3 Detailed provisions for the additional security provisions for supplies of LAGs and STEBs are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 9-A

DECLARATION OF COMMITMENTS

KNOWN SUPPLIER OF AIRPORT SUPPLIES

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council [1] and its implementing acts,

I declare that,

— [name of company] will

(a) appoint a person responsible for security in the company; and

▼M15

(b) ensure that persons with access to airport supplies receive general security awareness training in accordance with point 11.2.7 before being given access to these supplies. In addition, ensure that persons implementing security controls other than screening in respect of airport supplies receive training in accordance with point 11.2.3.10; and

▼B

(c) prevent unauthorised access to its premises and airport supplies; and

(d) reasonably ensure that no prohibited articles are concealed in airport supplies; and

(e) apply tamper-evident seals to, or physically protect, all vehicles and/or containers that transport airport supplies (this point will not apply during airside transportation).

When using another company that is not a known supplier to the airport operator for transporting supplies, [name of company] will ensure that all security controls listed above are adhered to,

— in order to ensure compliance, [name of company] will cooperate fully with all inspections, as required, and provide access to all documents, as requested by inspectors,

[1] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

▼B

— [name of company] will inform [the airport operator] of any serious security breaches and of any suspicious circumstances which may be relevant to airport supplies, in particular any attempt to conceal prohibited articles in supplies,

— [name of company] will ensure that all relevant staff receive training in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998 and are aware of their security responsibilities, and

— [name of company] will inform [the airport operator] if:

(a) it ceases trading; or

(b) it can no longer meet the requirements of the relevant EU legislation.

I shall accept full responsibility for this declaration.

Legal representative

Name:

Date:

Signature:

10. **IN-FLIGHT SECURITY MEASURES**

No provisions in this Regulation.

11. **STAFF RECRUITMENT AND TRAINING**

11.0 GENERAL PROVISIONS

11.0.1 The authority, airport operator, air carrier or entity deploying persons implementing, or responsible for implementing, measures for which it is responsible in accordance with the national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 shall ensure that these persons meet the standards set out in this Chapter.

11.0.2 For the purpose of this Chapter, ‘certification’ means a formal evaluation and confirmation by or on behalf of the appropriate authority indicating that the person has successfully completed the relevant training and that the person possesses the necessary competencies to perform assigned functions to an acceptable level.

11.0.3 For the purposes of this Chapter, a ‘state of residence’ shall be any country in which the person has been resident continuously for 6 months or more and a ‘gap’ in the record of education or employment shall mean any gap of more than 28 days.

11.0.4 For the purposes of this Chapter, ‘competency’ means being able to demonstrate suitable knowledge and skills.

11.0.5 Competencies acquired by persons prior to recruitment may be taken into consideration when assessing any training needs under this Chapter.

11.0.6 Where relevant competencies required by this Regulation that are not specific to aviation security have been acquired through training not delivered by an instructor in line with point 11.5 of this Regulation and/or through courses not specified or approved by the appropriate authority, it may be taken into consideration when assessing any training needs under this Chapter.

11.0.7 Where a person has received training and acquired competencies listed in point 11.2, the training need not be repeated for another function other than for the purposes of recurrent training.

▼M5

11.0.8 For the purposes of this Chapter, ‘radicalisation’ means the phenomenon of socialisation to extremism of people embracing opinions, views and ideas, which could lead to terrorism.

▼M5

11.0.9 For the purposes of this Chapter and without prejudice to the applicable Union and national laws, in determining the reliability of an individual undergoing the process described in points 11.1.3 and 11.1.4, Member States shall consider at least:

(a) the offences referred to in the Annex II to the Directive (EU) 2016/681 of The European Parliament and of the Council ([1]);

and

(b) the terrorist offences referred to in the Directive (EU) 2017/541 of the European Parliament and of the Council ([2]).

The offences listed in point (b) shall be considered as disqualifying crimes.

11.1 RECRUITMENT

▼M15

11.1.1 The following personnel shall have successfully completed an enhanced background check:

(a) persons being recruited to implement, or to be responsible for the implementation of screening, access control or other security controls in a security restricted area;

(b) persons with general responsibility at national or local level for ensuring that a security programme and its implementation meet all legal provisions (security managers);

(c) instructors, as referred to in Chapter 11.5;

(d) EU aviation security validators, as referred to in Chapter 11.6.

Point (b) of the first paragraph shall apply from 1 January 2023. Before that date, such persons shall have completed an enhanced or a standard background check either in accordance with point 1.2.3.1 or as determined by the appropriate authority in accordance with applicable national rules.

▼M8

11.1.2 The following personnel shall have successfully completed an enhanced or a standard background check:

a) Persons being recruited to implement, or to be responsible for the implementation of, screening, access control or other security controls elsewhere than a security restricted area;

b) Persons having unescorted access to air cargo and mail, air carrier mail and air carrier material, in-flight supplies and airport supplies to which the required security controls have been applied;

c) Persons having administrator rights or unsupervised and unlimited access to critical information and communications technology systems and data used for civil aviation security purposes as described in 1.7.1 in accordance with the national aviation security programme, or having been otherwise identified in the risk assessment in accordance with 1.7.3.

([1]) Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

([2]) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

▼M8

Unless otherwise specified in this Regulation, whether an enhanced or a standard background check has to be completed shall be determined by the appropriate authority in accordance with applicable national rules.

▼M5

11.1.3 In accordance with the applicable rules of Union and national law, an enhanced background check shall at least:

(a) establish the person's identity on the basis of documentary evidence;

(b) cover criminal records in all states of residence during at least the preceding 5 years;

(c) cover employment, education and any gaps during at least the preceding 5 years;

(d) cover intelligence and any other relevant information available to the competent national authorities that they consider may be relevant to the suitability of a person to work in a function which requires an enhanced background check.

11.1.4 In accordance with the applicable rules of Union and national law, a standard background check shall:

(a) establish the person's identity on the basis of documentary evidence;

(b) cover criminal records in all states of residence during at least the preceding 5 years;

(c) cover employment, education and any gaps during at least the preceding 5 years.

11.1.5 A standard background check or points (a) to (c) of an enhanced background check shall be completed before the person undergoes initial security training involving access to information which is not publicly available due to its security sensitivity. Where applicable, point (d) of an enhanced background check shall be completed before a person is allowed to implement, or to be responsible for the implementation of, screening, access control or other security controls.

▼M15

An enhanced background check shall be fully completed before the person undergoes the training referred to in points 11.2.3.1 to 11.2.3.5.

▼M5

11.1.6 Enhanced or standard background checks shall be considered as failed if not all the elements specified in points 11.1.3 and 11.1.4 respectively, are completed satisfactorily, or if at any point in time these elements do not provide the necessary level of assurance as to the reliability of the individual.

Member States shall endeavour to establish appropriate and effective mechanisms in order to ensure information sharing at national level and with other States for the purposes of elaboration and evaluation of information relevant to background check.

11.1.7 Background checks shall be subject to the following:

(a) a mechanism for the ongoing review of the elements specified in points 11.1.3 and 11.1.4 through the prompt notification to the competent authority, operator or issuing entity, as applicable, of any occurrence that may affect the reliability of the individual. Modalities for the notification, exchange of information and content thereof between the competent authorities, operators and entities, shall be established and monitored in accordance with the national law; or

▼M5

(b) a repeat at regular intervals not exceeding 12 months for enhanced background checks, or three years for standard background checks.

11.1.8 The recruitment process for all persons being recruited under points 11.1.1 and 11.1.2 shall include at least a written application and an interview stage designed to provide an initial assessment of abilities and aptitudes.

11.1.9 Persons being recruited to implement security controls shall have the mental and physical abilities and aptitudes required to carry out their designated tasks effectively and shall be made aware of the nature of these requirements at the outset of the recruitment process.

These abilities and aptitudes shall be assessed during the recruitment process and before completion of any probationary period.

11.1.10 Recruitment records, including results of any assessment tests, shall be kept for all persons recruited under points 11.1.1 and 11.1.2 for at least the duration of their contract.

11.1.11 In order to address the insider threat, and notwithstanding the respective staff training contents and competences listed in paragraph 11.2, the security programme of operators and entities referred to in Articles 12, 13 and 14 of Regulation (EC) No 300/2008 shall include an appropriate internal policy and related measures enhancing staff awareness and promoting security culture.

11.1.12 Background checks successfully completed before ►M9 31 December 2021 ◄ will remain valid until their expiry or at the latest until ►M9 30 June 2024 ◄, whichever date comes earlier.

▼B

11.2 TRAINING

11.2.1 **General training obligations**

11.2.1.1 Persons shall have successfully completed relevant training before being authorised to implement security controls unsupervised.

11.2.1.2 Training of persons performing tasks as listed in points 11.2.3.1 to 11.2.3.5 and point 11.2.4 shall include theoretical, practical and on-the-job training elements.

11.2.1.3 The content of courses shall be specified or approved by the appropriate authority before:

(a) an instructor delivers any training required under Regulation (EC) No 300/2008 and its implementing acts; or

(b) a computer based training course is used in order to meet the requirements of Regulation (EC) No 300/2008 and its implementing acts.

Computer based training may be used with or without the support of an instructor or coach.

11.2.1.4 Training records shall be kept for all persons trained for at least the duration of their contract.

▼B

11.2.2 **Basic training**

Basic training of persons performing tasks as listed in points 11.2.3.1, 11.2.3.4 and 11.2.3.5 as well as in points 11.2.4, 11.2.5 and 11.5 shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

(b) knowledge of the legal framework for aviation security;

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;

(d) knowledge of access control procedures;

▼M2

(e) knowledge of identification card systems in use;

▼B

(f) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported;

(g) knowledge of reporting procedures;

(h) ability to identify prohibited articles;

(i) ability to respond appropriately to security related incidents;

(j) knowledge of how human behaviour and responses can affect security performance;

▼M5

(k) ability to communicate clearly and confidently; and

(l) knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.

▼B

11.2.3 **Job specific training for persons implementing security controls**

11.2.3.1 Job specific training of persons implementing screening of persons, cabin baggage, items carried and hold baggage shall result in all of the following competencies:

(a) understanding of the configuration of the screening checkpoint and the screening process;

(b) knowledge of how prohibited articles may be concealed;

(c) ability to respond appropriately to the detection of prohibited articles;

(d) knowledge of the capabilities and limitations of security equipment or screening methods used;

▼B

(e) knowledge of emergency response procedures.

In addition, where the designated tasks of the person concerned so require, training shall also result in the following competences:

(f) interpersonal skills, in particular how to deal with cultural differences and with potentially disruptive passengers;

(g) knowledge of hand searching techniques;

(h) ability to carry out hand searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;

(i) knowledge of exemptions from screening and special security procedures;

(j) ability to operate the security equipment used;

(k) ability to correctly interpret images produced by security equipment; and

(l) knowledge of protection requirements for hold baggage.

11.2.3.2 Training of persons implementing screening of cargo and mail shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls in the supply chain;

(d) ability to identify prohibited articles;

(e) ability to respond appropriately to the detection of prohibited articles;

(f) knowledge of the capabilities and limitations of security equipment or screening methods used;

(g) knowledge of how prohibited articles may be concealed;

▼B

(h) knowledge of emergency response procedures;

(i) knowledge of protection requirements for cargo and mail;

In addition, where the designated tasks of the person concerned so require, training shall also result in the following competences:

(j) knowledge of screening requirements for cargo and mail, including exemptions and special security procedures;

(k) knowledge of screening methods appropriate for different types of cargo and mail;

(l) knowledge of hand searching techniques;

(m) ability to carry out hand searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;

(n) ability to operate the security equipment used;

(o) ability to correctly interpret images produced by security equipment;

(p) knowledge of transportation requirements.

11.2.3.3 Training of persons implementing screening of air carrier mail and materials, in-flight supplies and airport supplies shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls in the supply chain;

(d) ability to identify prohibited articles;

(e) ability to respond appropriately to the detection of prohibited articles;

(f) knowledge of how prohibited articles may be concealed;

(g) knowledge of emergency response procedures;

(h) knowledge of the capabilities and limitations of security equipment or screening methods used;

▼B

In addition, where the designated tasks of the person concerned so require, training shall also result in the following competences:

(i) knowledge of hand searching techniques;

(j) ability to carry out hand searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;

(k) ability to operate the security equipment used;

(l) ability to correctly interpret images produced by security equipment;

(m) knowledge of transportation requirements.

11.2.3.4 Specific training of persons performing vehicle examinations shall result in all of the following competencies:

(a) knowledge of the legal requirements for vehicle examinations, including exemptions and special security procedures;

(b) ability to respond appropriately to the detection of prohibited articles;

(c) knowledge of how prohibited articles may be concealed;

(d) knowledge of emergency response procedures;

(e) knowledge of vehicle examination techniques;

(f) ability to carry out vehicle examinations to a standard sufficient to reasonably ensure the detection of concealed prohibited articles.

11.2.3.5 Specific training of persons implementing access control at an airport as well as surveillance and patrols shall result in all of the following competencies:

(a) knowledge of the legal requirements for access control, including exemptions and special security procedures;

(b) knowledge of access control systems used at the airport;

(c) knowledge of authorisations, including identification cards and vehicle passes, providing access to airside areas and ability to identify those authorisations;

(d) knowledge of procedures for patrolling and for challenging persons and of circumstances in which persons should be challenged or reported:

(e) ability to respond appropriately to the detection of prohibited articles;

(f) knowledge of emergency response procedures;

(g) interpersonal skills, in particular how to deal with cultural differences and with potentially disruptive passengers.

11.2.3.6 Training of persons implementing aircraft security searches shall result in all of the following competencies:

▼M5

(a) knowledge of the legal requirements for aircraft security searches and of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(b) knowledge of the configuration of the type(s) of aircraft on which the person is to implement aircraft security searches;

(c) ability to identify prohibited articles;

(d) ability to respond appropriately to the detection of prohibited articles;

(e) knowledge of how prohibited articles may be concealed;

(f) ability to implement aircraft security searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles.

In addition, where the person holds an airport identification card, training shall also result in all of the following competences:

(g) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

(h) knowledge of the legal framework for aviation security;

(i) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;

(j) understanding of the configuration of the screening checkpoint and the screening process;

(k) awareness of access control and relevant screening procedures;

(l) knowledge of airport identification card used at the airport.

11.2.3.7 Training of persons implementing aircraft protection shall result in all of the following competencies:

▼M5

(a) knowledge of how to protect and prevent unauthorised access to aircraft and of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(b) knowledge of procedures for sealing aircraft, if applicable for the person to be trained;

(c) knowledge of identification card systems used at the airport;

(d) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported; and

(e) knowledge of emergency response procedures.

In addition, where the person holds an airport identification card, training shall also result in all of the following competences:

(f) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

(g) knowledge of the legal framework for aviation security;

(h) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;

▼B

(i) understanding of the configuration of the screening checkpoint and the screening process;

(j) awareness of access control and relevant screening procedures.

11.2.3.8 Training of persons implementing baggage reconciliation shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;

(d) ability to respond appropriately to the detection of prohibited articles;

(e) knowledge of emergency response procedures;

(f) knowledge of passenger and baggage reconciliation requirements and techniques;

(g) knowledge of protection requirements for air carrier materials used for passenger and baggage processing.

▼M2

In addition, where the person holds an airport identification card, training shall also result in all of the following competences:

(h) understanding of the configuration of the screening checkpoint and the screening process;

(i) awareness of access control and relevant screening procedures;

(j) knowledge of airport identification cards used at the airport;

(k) knowledge of reporting procedures;

(l) ability to respond appropriately to security related incidents.

▼B

11.2.3.9 ►M15 Training of persons with unsupervised access to identifiable air cargo and mail to which the required security controls have been applied and persons implementing security controls for air cargo and mail other than screening shall result in all of the following competences: ◄

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls in the supply chain;

(d) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported;

▼B

(e) knowledge of reporting procedures;

(f) ability to identify prohibited articles;

(g) ability to respond appropriately to the detection of prohibited articles;

(h) knowledge of how prohibited articles may be concealed;

(i) knowledge of protection requirements for cargo and mail;

(j) knowledge of transportation requirements, if applicable.

▼M2

In addition, where the person holds an airport identification card, training shall also result in all of the following competences:

(k) understanding of the configuration of the screening checkpoint and the screening process;

(l) awareness of access control and relevant screening procedures;

(m) knowledge of identification cards in use;

(n) ability to respond appropriately to security related incidents.

▼B

11.2.3.10 Training of persons implementing security controls for air carrier mail and materials, in-flight supplies and airport supplies other than screening shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;

(d) knowledge of procedures for challenging persons and of circumstances in which persons should be challenged or reported;

(e) knowledge of reporting procedures;

(f) ability to identify prohibited articles;

(g) ability to respond appropriately to the detection of prohibited articles;

(h) knowledge of how prohibited articles may be concealed;

(i) knowledge of protection requirements for air carrier mail and materials, in-flight supplies and airport supplies, as applicable;

(j) knowledge of transportation requirements, if applicable.

▼M2

In addition, where the person holds an airport identification card, training shall also result in all of the following competences:

▼M2

(k) understanding of the configuration of the screening checkpoint and the screening process;

(l) awareness of access control and relevant screening procedures;

(m) knowledge of identification cards in use;

(n) ability to respond appropriately to security related incidents.

▼M15

11.2.3.11 Training of flight and cabin crew members implementing in-flight security measures shall result in all of the following competences:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of flight and cabin crew members;

(d) knowledge of how to protect and prevent unauthorised access to aircraft;

(e) knowledge of procedures for sealing aircraft, if applicable for the person to be trained;

(f) ability to identify prohibited articles;

(g) knowledge of how prohibited articles may be concealed;

(h) ability to implement aircraft security searches to a standard sufficient to reasonably ensure the detection of concealed prohibited articles;

(i) knowledge of the configuration of the type or types of aircraft on which the duties are performed;

(j) ability to protect flight deck during the flight;

(k) knowledge of procedures relevant to carriage of potentially disruptive passengers on board an aircraft, if applicable for the person to be trained;

(l) knowledge of handling persons authorised to carry firearms on board, if applicable for the person to be trained;

(m) knowledge of reporting procedures;

(n) ability to respond appropriately to security related incidents and emergencies on board an aircraft.

▼B

11.2.4 **Specific training for persons directly supervising persons implementing security controls (supervisors)**

Specific training of supervisors shall, in addition to the competencies of the persons to be supervised, result in all of the following competencies:

▼B

(a) knowledge of the relevant legal requirements and how they should be met;

(b) knowledge of supervisory tasks;

(c) knowledge of internal quality control;

(d) ability to respond appropriately to the detection of prohibited articles;

(e) knowledge of emergency response procedures;

(f) ability to provide mentoring and on-the-job training and to motivate other.

In addition, where the designated tasks of the person concerned so require, that training shall also result in all of the following competences:

(g) knowledge of conflict management;

(h) knowledge of the capabilities and limitations of security equipment or screening methods used.

11.2.5 **Specific training for persons with general responsibility at national or local level for ensuring that a security programme and its implementation meet all legal provisions (security managers)**

Specific training of security managers shall result in all of the following competencies:

(a) knowledge of the relevant legal requirements and how they should be met;

(b) knowledge of internal, national, Union and international quality control;

(c) ability to motivate others;

(d) knowledge of the capabilities and limitations of security equipment or screening methods used.

11.2.6 **Training of persons other than passengers requiring unescorted access to security restricted areas**

11.2.6.1 Persons other than passengers requiring unescorted access to security restricted areas and not falling under points 11.2.3 to 11.2.5 and 11.5 shall receive security awareness training before being issued with an authorisation granting unescorted access to security restricted areas.

For objective reasons, the appropriate authority may exempt persons from this training requirement if their access is limited to areas in the terminal accessible to passengers.

▼B

11.2.6.2 Security awareness training shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security, including the obligations and responsibilities of persons implementing security controls;

(d) understanding of the configuration of the screening checkpoint and the screening process;

(e) awareness of access control and relevant screening procedures;

(f) knowledge of airport identification cards used at the airport;

(g) knowledge of reporting procedures;

(h) ability to respond appropriately to security related incidents.

11.2.6.3 Each person undergoing security awareness training shall be required to demonstrate understanding of all subjects referred to in point 11.2.6.2 before being issued with an authorisation granting unescorted access to security restricted areas.

11.2.7 **Training of persons requiring general security awareness**

General security awareness training shall result in all of the following competencies:

(a) knowledge of previous acts of unlawful interference with civil aviation, terrorist acts and current threats;

▼M5

(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;

▼B

(c) knowledge of the objectives and organisation of aviation security in their working environment, including the obligations and responsibilities of persons implementing security controls;

(d) knowledge of reporting procedures;

▼B

(e) ability to respond appropriately to security related incidents.

Each person undergoing general security awareness training shall be required to demonstrate understanding of all subjects referred to in this point before taking up duty.

This training shall not apply to instructors falling under point 11.5.

▼M8

11.2.8 Training of persons with roles and responsibility related to cyber threats

11.2.8.1 Persons implementing the measures as laid down in point 1.7.2 shall have the skills and aptitudes required to carry out their designated tasks effectively. They shall be made aware of relevant cyber risks on a need-to-know basis.

11.2.8.2 Persons having access to data or systems shall receive appropriate and specific job related training commensurate with their role and responsibilities, including being made aware of relevant risks where their job function requires this. The appropriate authority, or the authority or agency as laid down in point 1.7.4 shall specify or approve the content of the course.

▼B

11.3 CERTIFICATION OR APPROVAL

11.3.1 Persons performing tasks as listed in points 11.2.3.1 to 11.2.3.5 shall be subject to:

(a) an initial certification or approval process; and

▼M5

(b) for persons operating x-ray or EDS equipment, recertification at least every 3 years; and

▼B

(c) for all other persons, recertification or reapproval at least every 5 years.

Persons performing tasks as listed in point 11.2.3.3 may be exempted from these requirements if they are only authorised to implement visual checks and/or hand searches.

▼M5

11.3.2 Persons operating x-ray or EDS equipment shall, as part of the initial certification or approval process, pass a standardised image interpretation test.

11.3.3 The recertification or re-approval process for persons operating x-ray or EDS equipment shall include both the standardised image interpretation test and an evaluation of operational performance.

▼B

11.3.4 Failure to undertake or successfully complete recertification or reapproval within a reasonable timescale, not normally exceeding 3 months, shall result in the related security entitlements being withdrawn.

11.3.5 Certification or approval records shall be kept for all persons certified or approved, respectively, for at least the duration of their contract.

▼B

11.4 RECURRENT TRAINING

11.4.1 Persons operating x-ray or EDS equipment shall be subject to recurrent training consisting of image recognition training and testing. This shall take the form of:

(a) classroom and/or computer based training; or

(b) on-the-job TIP training, on condition that a TIP library of at least 6 000 images, as specified below, is employed on the x-ray or EDS equipment used and the person works with this equipment during at least one third of his working hours.

▼M5

_____

▼B

For classroom and/or computer based training, persons shall be subject to image recognition training and testing for at least 6 hours in every 6 month period, using either:

— an image library containing at least 1 000 images of at least 250 different threat articles, including images of component parts of threat articles, with each article captured in a variety of different orientations, and arranged to provide an unpredictable selection of images from the library during the training and testing; or

— the most frequently missed TIP images from the TIP library in use combined with images of recently captured threat articles relevant for the type of screening operation and covering all types of relevant threat articles if only used once for the training of a given screener over a three-year period.

For on-the-job TIP training, the TIP library shall consist of at least 6 000 images of at least 1 500 different threat articles, including images of component parts of threat articles, with each article captured in a variety of different orientations.

▼M5

11.4.2 Evaluation of the performance of individual screeners shall be carried out at the end of every 6 month period. The results of this evaluation:

(a) shall be provided to the person and recorded;

(b) shall be used to identify weaknesses and inform future training and testing adapted to address those weaknesses; and

(c) may be taken into consideration as part of the recertification or re-approval process.

▼B

11.4.3 Persons performing tasks as listed under point 11.2 other than those referred to in point 11.4.1 and 11.4.2 shall undergo recurrent training at a frequency sufficient to ensure that competencies are maintained and acquired in line with security developments.

Recurrent training shall be conducted:

(a) for competencies acquired during initial basic, specific and security awareness training, at least once every 5 years or, in cases where the competencies have not been exercised for more than 6 months, before return to security duties; and

(b) for new or extended competencies, as required to ensure that persons implementing, or responsible for implementing, security controls are promptly made aware of new threats and legal requirements by the time they have to be applied.

▼B

The requirements under (a) shall not apply to competencies acquired during specific training which are no longer required for the person's designated tasks.

11.4.4 Records of recurrent training shall be kept for all persons trained for at least the duration of their contract.

11.5 QUALIFICATION OF INSTRUCTORS

11.5.1 Instructors shall at least fulfil all of the following requirements:

▼M5

(a) the successful completion of an enhanced background check in accordance with point 11.1.3;

▼B

(b) competency in instructional techniques;

(c) knowledge of the work environment in the relevant aviation security field;

(d) competency in the security elements to be taught.

▼M16

Certification shall at least apply to those instructors authorised to give training defined in points 11.2.3.1 to 11.2.3.5 and in points 11.2.4 (unless it concerns the training of supervisors exclusively supervising persons referred to in points 11.2.3.6 to 11.2.3.11) and 11.2.5.

▼M2

Instructors shall be subject to recertification at least every 5 years.

▼B

11.5.2 Instructors shall receive regular training or information on developments in the relevant fields.

11.5.3 The appropriate authority shall maintain or have access to lists of instructors operating in the Member State.

11.5.4 If the appropriate authority is no longer satisfied that training delivered by an instructor is resulting in persons having the relevant competencies, or where the instructor fails the background check, it shall either withdraw approval of the course or ensure that the instructor is suspended or removed from the list of instructors, as appropriate. Where such action is taken, the appropriate authority shall also specify how the instructor may apply to have the suspension lifted, be reinstated on the list of instructors or have the course approval reinstated.

11.5.5 Any competencies acquired by an instructor in order to meet the requirements under this Chapter in one Member State shall be recognised in another Member State.

11.6 EU AVIATION SECURITY VALIDATION

11.6.1 EU aviation security validation is a standardised, documented, impartial and objective process for obtaining and evaluating evidence to determine the level of compliance of the validated entity with requirements set out in Regulation (EC) No 300/2008 and its implementing acts.

11.6.2 **EU aviation security validation**

EU aviation security validation:

(a) may be a requirement for obtaining or maintaining a legal status under Regulation (EC) No 300/2008 and its implementing acts;

▼B

(b) may be performed by an appropriate authority or a validator approved as EU aviation security validator or a validator recognised as equivalent to it, in accordance with this Chapter;

(c) shall assess security measures applied under the responsibility of the validated entity or parts thereof for which the entity seeks validation. At least, it shall consist of:

(1) an evaluation of security relevant documentation, including the validated entity's security programme or equivalent; and

(2) a verification of the implementation of aviation security measures, which shall include an on-site verification of the validated entity's relevant operations, unless otherwise stated;

(d) shall be recognised by all Member States.

11.6.3 **Approval requirements for EU aviation security validators**

11.6.3.1 Member States shall approve EU aviation security validators based on conformity assessment capacity, which shall comprise:

(a) independence from the validated industry, unless otherwise stated; and

(b) appropriate personnel competence in the security area to be validated as well as methods to maintain such competence at the level referred to in 11.6.3.5; and

(c) the functionality and appropriateness of validation processes.

11.6.3.2 Where relevant, the approval shall take account of accreditation certificates in relation to the relevant harmonised standards, namely with EN-ISO/IEC 17020 instead of re-assessing conformity assessment capacity.

11.6.3.3 An EU aviation security validator may be any individual or a legal entity.

11.6.3.4 The national accreditation body established pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council [1] may be empowered to accredit the conformity assessment capacity of legal entities to perform EU aviation security validation, adopt administrative measures in that respect and carry out the surveillance of EU aviation security validation activities.

11.6.3.5 Every individual performing EU aviation security validation shall have appropriate competence and background, and shall meet all of the following requirements:

▼M5

(a) have been subjected to an enhanced background check in accordance with point 11.1.3;

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

▼B

(b) perform EU aviation security validation impartially and objectively, shall understand the meaning of independence and apply methods to avoid situations of conflict of interest in respect of the validated entity;

(c) have sufficient theoretical knowledge and practical experience in the field of quality control as well as respective skills and personal attributes to collect, record and assess findings based on a checklist, in particular regarding:

(1) compliance monitoring principles, procedures and techniques;

(2) factors affecting human performance and supervision;

(3) the role and powers of the validator, including on conflict of interest;

(d) provide proof of appropriate competence based on training and/or a minimum work experience in respect of the following areas:

(1) general aviation security principles of Union and ICAO aviation security standards;

(2) specific standards related to the activity validated and how they are applied to operations;

(3) security technologies and techniques relevant for the validation process;

(e) undergo recurrent training at a frequency sufficient to ensure that existing competencies are maintained and new competencies are acquired to take account of developments in the field of aviation security.

11.6.3.6 The appropriate authority shall either itself provide training for EU aviation security validator or approve and maintain a list of appropriate security training courses. ►M12 The appropriate authority shall provide the validators it approves with the relevant parts of the non-public legislation and national programmes referring to the operations and areas to validate. ◄

11.6.3.7 Member States may limit the approval of an EU aviation security validator to validation activities which are carried out solely on the territory of that Member State on behalf of the appropriate authority of that Member State. In such cases, the requirements of point 11.6.4.2 do not apply.

▼M12

11.6.3.8 The appropriate authority acting as validator may only perform validations in respect of air carriers, operators and entities that are placed under its responsibility or under the responsibility of the appropriate authority of another Member State, where it has been explicitly requested or appointed to do so by that authority.

▼M7

11.6.3.9 As from the date of withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union pursuing Article 50 of the TEU, the following provisions apply in respect of EU aviation security validators approved by this Member State to perform validations in respect of airlines, operators and entities seeking respectively ACC3, RA3 and KC3 designation:

▼M7

(a) they are no longer recognised in the Union;

(b) the EU aviation security validations performed before the date of withdrawal of the United Kingdom from the Union, including the EU validation reports issued before that date remain valid for the purpose of the designation of air carriers, operators and entities they have validated;

11.6.3.10 Individuals and entities indicated in the previous point may seek approval as EU aviation security validator by the appropriate authority of a Member State. The approving Member State shall:

(a) Obtain from the appropriate authority of the United Kingdom the necessary documentation on which basis the individual or legal entity had been approved as EU aviation security validator;

(b) Verify that the applicant fulfils the Union requirements in this Chapter. If the appropriate authority is satisfied, it may approve the individual or the entity as EU aviation security validator for a period not exceeding the approval that was granted by the appropriate authority of the United Kingdom;

(c) Promptly inform the Commission that will ensure the listing of the EU aviation security validator into the Union database on supply chain security.

▼M12

11.6.3.11 The approval of an EU aviation security validator shall be valid for a maximum period of five years.

▼B

11.6.4 **Recognition and discontinuation of EU aviation security validators**

▼M12

11.6.4.1 An EU aviation security validator:

(a) shall not be considered to be approved until its details are listed in the ‘Union database on supply chain security’;

(b) shall be provided with proof of its status by or on behalf of the appropriate authority;

▼M13

(c) may not perform EU aviation security validations if it holds the status of aviation security validator under an equivalent scheme in place in a third country or an international organisation, unless the third country or international organisation grants reciprocal opportunities to EU aviation security validators within its scheme.

▼M12

EU aviation security validators listed in the ‘Union database on supply chain security’ on account of the appropriate authority, may only perform validations of airlines, operators or entities under the responsibility of that appropriate authority.

▼B

11.6.4.2 Approved EU aviation security validators shall be recognised by all Member States.

▼M2

11.6.4.3 When a Member State is no longer satisfied that an EU aviation security validator meets the requirements referred to in points 11.6.3.1 or 11.6.3.5, it shall withdraw the approval and remove the validator from the Union database on supply chain security, or inform the appropriate authority that approved it, sharing the basis for its concern.

▼B

11.6.4.4 Industry associations and entities under their responsibility operating quality assurance programmes may be approved as EU aviation security validators provided equivalent measures of those programmes ensure impartial and objective validation. Recognition shall be done in cooperation of the appropriate authorities of at least two Member States.

11.6.4.5 The Commission may recognise validation activities undertaken by authorities or aviation security validators under the jurisdiction of and recognised by a third country or an international organisation where it can confirm their equivalency to EU aviation security validation. A list thereof shall be kept in Attachment 6-Fiii.

11.6.5 **EU aviation security validation report (‘the validation report’)**

11.6.5.1 The validation report shall record the EU aviation security validation and contain at least:

(a) a completed checklist signed by the EU aviation security validator including, where requested, comments by the validated entity in the necessary detail; and

(b) a declaration of commitments signed by the validated entity; and

(c) an independence declaration in respect of the entity validated signed by the individual performing the EU aviation security validation.

11.6.5.2 The EU aviation security validator shall establish the level of compliance with the objectives contained in the checklist and record these findings in the appropriate part of the checklist.

11.6.5.3 A declaration of commitment shall state the validated entity's commitment to continue operation under the successfully validated operation standards.

11.6.5.4 The validated entity may declare its agreement or disagreement to the validation report's established compliance level. Such a declaration shall become an integral part of the validation report.

11.6.5.5 Page numbering, date of the EU aviation security validation and initialling by the validator and the validated entity on each page shall prove the validation report's integrity. ►M5 Manual initialling on each page may be replaced by an electronic signature of the entire document. ◄

▼M12

11.6.5.6 By default the report shall be in English and delivered to the appropriate authority along with the validated entity, within not more than one month after the on-site verification.

The appropriate authority shall assess the validation report within not more than six weeks after its reception.

▼M12

Where the report concerns an airline, operator or entity undergoing validation for the purposes of an existing designation that expires after the periods referred to in the paragraphs above, the appropriate authority may set a longer period to complete the assessment.

In such case, and unless further information and additional documentary evidence is necessary to successfully conclude the assessment, the appropriate authority shall ensure that the process is completed before the expiry of the validity of status.

Within three months from the date of reception of the report, the validator shall be provided with a written feedback regarding the quality of the report, and where applicable, any recommendations and remarks that the appropriate authority may deem necessary. Where applicable, a copy of such feedback shall be transmitted to the appropriate authority that has approved the validator.

For the purposes of the designation of other airlines, operators or entities as provided for in this Regulation, an appropriate authority may request and shall obtain, within 15 days, from the appropriate authority that has drafted a validation report in its national language or has required the validator performing the validation to do so, a copy of the full validation report in the English language.

▼B

11.7. MUTUAL RECOGNITION OF TRAINING

11.7.1 Any competencies acquired by a person in order to meet the requirements under Regulation (EC) No 300/2008 and its implementing acts in one Member State shall be recognised in another Member State.

▼M2

ATTACHMENT 11-A

INDEPENDENCE DECLARATION — EU AVIATION SECURITY VALIDATOR

(a) I confirm that I have established the level of compliance of the validated entity in an impartial and objective way.

(b) I confirm that I am not, and have not in the preceding two years, been employed by the validated entity.

(c) I confirm that I have no economic or other direct or indirect interest in the outcome of the validation activity, the validated entity or its affiliates.

(d) I confirm that I have, and have had in the preceding 12 months no business relations such as training and consultancy beyond the validation process with the validated entity in areas related to aviation security.

(e) I confirm that the EU aviation security validation report is based on a thorough fact finding evaluation of relevant security documentation, consisting of:

— the validated entities' security programme or equivalent, and

— an on- site verification of the implementation thereof.

(f) I confirm that the EU aviation security validation report is based on an assessment of all security relevant areas on which the validator is required to give an opinion based on the relevant EU checklist.

(g) I confirm that I have applied a methodology that allows for separate EU aviation security validation reports in respect of each entity validated and ensures objectivity and impartiality of the fact finding and evaluation, where several entities are being validated in a joint action.

▼M2

(h) I confirm that I accepted no financial or other benefits, other than a reasonable fee for the validation and a compensation of travel and accommodation costs.

I accept full responsibility for the EU aviation security validation report.

Name of the validated entity:

Name of the EU aviation security validator:

Date:

Signature:

▼B

12. SECURITY EQUIPMENT

▼M10

12.0. GENERAL PROVISION AND APPROVAL OF SECURITY EQUIPMENT

12.0.1. **General provision**

12.0.1.1. The authority, operator or entity using equipment for the implementation of measures for which it is responsible in accordance with the national civil aviation security programme as referred to in Article 10 of Regulation (EC) No 300/2008 shall ensure that the equipment meets the standards set out in this Chapter.

The information contained in this Chapter and classified in accordance with Decision (EU, Euratom) 2015/444 ([1]) shall be made available by the appropriate authority to manufacturers on a need-to-know basis.

12.0.1.2. There shall be routine testing of each piece of security equipment.

12.0.1.3. Equipment manufacturers shall provide a concept of operations and equipment shall be evaluated and used in accordance with it.

12.0.1.4. Where several security equipment are combined, each one has to comply with the defined specifications and meet the standards set out in this Chapter, both used separately and combined as a system.

12.0.1.5. Equipment shall be positioned, installed and maintained in compliance with the requirements of equipment manufacturers.

12.0.2. **Approval of security equipment**

▼M16

12.0.2.1. Subject to point 12.0.5, the following security equipment and software may be installed after 1 October 2020 only if it has been granted an ‘EU Stamp’ marking or an ‘EU Stamp pending’ marking status as referred to in point 12.0.2.5:

(a) walk-through metal detection (WTMD) equipment;

(b) explosive detection systems (EDS) equipment;

(c) explosive trace detection (ETD) equipment;

(d) liquid explosive detection systems (LEDS) equipment;

(e) metal detection equipment (MDE);

([1]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

▼M16

(f) security scanners;

(g) shoe scanner equipment;

(h) explosive vapour detection (EVD) equipment;

(i) automated prohibited items detections (APID) software.

▼M10

12.0.2.2. The Commission shall approve the security equipment listed in 12.0.2.1 and shall grant the ‘EU Stamp’ marking.

▼M12

12.0.2.3. The ‘EU Stamp’ marking shall be granted to security equipment tested by test centres which implement quality control measures in accordance with the Common Evaluation Process of the European Civil Aviation Conference under the responsibility of the appropriate authority.

▼M10

12.0.2.4. The Commission may grant an ‘EU Stamp’ marking to security equipment only after it has received the test reports for the equipment in question or Level 2 reports by the Common Evaluation Process of the European Civil Aviation Conference.

The Commission may request additional information relating to test reports.

12.0.2.5. The Commission may grant an ‘EU Stamp’ marking to security equipment confirmed by the Common Evaluation Process of the European Civil Aviation Conference. Such equipment shall be automatically eligible to the ‘EU Stamp’ marking, and shall receive a temporary ‘EU Stamp pending’ marking status until the final approval.

Security equipment with an ‘EU Stamp pending’ marking status shall be allowed for installation and use.

12.0.3. **‘EU Stamp’ marking and Union database on supply chain security — security equipment**

12.0.3.1. Security equipment listed in point 12.0.2.1 for which ‘EU Stamp’ marking has been granted shall be entered into the ‘Union database on supply chain security — security equipment’.

▼M15

12.0.3.2. The ‘EU Stamp’ marking shall be affixed by manufacturers on security equipment approved by the Commission and visible on one side or on-screen.

▼M10

12.0.3.3. Equipment with ‘EU Stamp’ marking shall be installed with hardware and software versions corresponding to its description in the ‘Union database on supply chain security — security equipment’.

12.0.3.4. Without prejudice to points 12.0.4 and 12.0.5, security equipment with ‘EU Stamp’ marking benefits from mutual recognition and shall be recognised for availability, deployment and use in all Member States.

12.0.3.5. The Commission shall maintain the ‘Union database on supply chain security — security equipment’.

12.0.3.6. An entry in the ‘Union database on supply chain security — security equipment’ shall contain the following information:

(a) a unique alphanumeric identifier;

(b) the manufacturer name;

(c) the designation name;

(d) the detailed configuration with at least:

(i) the hardware version;

(ii) the detection algorithm;

(iii) if necessary, the system software version;

▼M10

(iv) if necessary, the auxiliary hardware version; and

(v) if necessary, the concept of operations version;

(e) the standard obtained;

(f) the status of the equipment, stating one of the following:

(i) ‘EU Stamp’;

(ii) ‘EU Stamp pending’;

(iii) ‘EU Stamp suspended’;

(iv) ‘EU Stamp withdrawn’;

(v) ‘EU Stamp obsolete’;

(g) the date of issuance of the status of the equipment.

12.0.4. **Suspension and withdrawal of ‘EU Stamp’ marking**

12.0.4.1. On request from Member States or on its own initiative, the Commission can suspend the ‘EU Stamp’ marking and the ‘EU Stamp pending’ marking status of security equipment without prior notice when it receives information indicating that the equipment does not meet the standard for which it has been approved. In doing so, the Commission updates the status in the ‘Union database on supply chain security — security equipment’ accordingly.

12.0.4.2. Security equipment whose ‘EU Stamp’ marking or ‘EU Stamp pending’ marking status has been suspended can no longer be deployed and the pieces already installed shall be operated with the addition of compensatory measures, as appropriate.

12.0.4.3. On request from Member States or on its own initiative, the Commission can withdraw the ‘EU Stamp’ marking or the ‘EU Stamp pending’ marking status of security equipment when it is no longer satisfied that the security equipment meets the standard for which it has been approved.

12.0.4.4. Security equipment whose ‘EU Stamp’ marking or ‘EU Stamp pending’ marking status has been withdrawn or has become obsolete can no longer be operated from the date of issuance of the status as recorded in the ‘Union database on supply chain security — security equipment’.

12.0.4.5. The Commission can reinstate the ‘EU Stamp’ marking or ‘EU Stamp pending’ marking status when it receives information that the equipment meets again the standard for which is has been approved.

12.0.5. **More stringent measures on security equipment and national approval**

12.0.5.1. Member States may derogate from the principle of mutual recognition by applying more stringent measures on security equipment. They shall notify the Commission of these measures, their approvals of security equipment and the steps taken to ensure that security equipment they approve meets the standards set out in this Chapter.

12.0.5.2. Member States may derogate from the principle of mutual recognition by applying their own national approval mechanism of security equipment. They shall notify the Commission of this mechanism, their approvals of equipment and the additional steps taken to ensure that security equipment meets the standards set out in this Chapter.

▼M12

12.0.5.3. Security equipment approved at national level on the basis of point 12.0.5.1 or 12.0.5.2 shall not automatically receive the ‘EU Stamp’ marking.

▼B

12.1 WALK-THROUGH METAL DETECTION (WTMD) EQUIPMENT

12.1.1 **General principles**

12.1.1.1 Walk-through metal detection equipment (WTMD) shall be able to detect and to indicate by means of an alarm at least specified metallic items, both individually and in combination.

12.1.1.2 The detection by WTMD shall be independent of the position and orientation of the metallic item.

12.1.1.3 WTMD shall be firmly fixed to a solid base.

12.1.1.4 WTMD shall have a visual indicator to show that the equipment is in operation.

12.1.1.5 The means for adjusting the detection settings of WTMD shall be protected and accessible only to authorised persons.

12.1.1.6 WTMD shall give both a visual alarm and an audible alarm when it detects metallic items as referred to in point 12.1.1.1. Both types of alarm shall be noticeable at a range of 2 metres.

12.1.1.7 The visual alarm shall give an indication of the strength of signal detected by the WTMD.

▼M5

_____

▼B

12.1.2 **Standards for WTMD**

▼M15

12.1.2.1 There shall be four standards for WTMD. Detailed requirements on those standards are laid down in Commission Implementing Decision C(2015) 8005.

▼B

12.1.2.2 All WTMD exclusively used for screening persons other than passengers shall meet at least standard 1.

12.1.2.3 All WTMD used for screening of passengers shall meet standard 2.

▼M15

12.1.2.4 All WTMD installed as of 1 July 2023 shall meet standard 1.1 or standard 2.1.

▼B

12.1.3 **Additional requirements for WTMD**

All WTMD for which a contract to install them was placed as from 5 January 2007 shall be able to:

(a) generate an audible and/or visual signal on a percentage of persons passing through the WTMD who did not cause an alarm as referred to in point 12.1.1.1. It shall be possible to set the percentage; and

(b) count the number of persons screened, excluding any person that passes through the WTMD in the opposite direction; and

(c) count the number of alarms; and

(d) calculate the number of alarms as a percentage of the number of screened persons.

12.1.4 **Additional requirements for WTMD used in combination with shoe metal detection (SMD) equipment**

12.1.4.1 All WTMD equipment used in combination with shoe metal detection (SMD) equipment shall be able to detect and indicate by means of a visual indication at least specified metallic items, both individually and in combination, and this shall correspond to the height at which this item (or items) is located on the person passing through it. This shall be irrespective of the type and number of items and their orientation.

▼B

12.1.4.2 All WTMD equipment used in combination with SMD equipment shall be able to detect and indicate all alarms generated by metallic items on a person in at least two zones. The first zone shall correspond to the lower legs of a person and shall be between the floor and a maximum of 35 cm above the floor. All other zones shall be above the first zone.

12.2 HAND-HELD METAL DETECTION (HHMD) EQUIPMENT

12.2.1 Hand-held metal detection equipment (HHMD) shall be able to detect ferrous and non-ferrous metallic items. Detection and identification of the position of the detected metal shall be indicated by means of an alarm.

12.2.2 The means for adjusting the sensitivity settings of HHMD shall be protected and accessible only to authorised persons.

12.2.3 HHMD shall give an audible alarm when it detects metallic items. The alarm shall be noticeable at a range of 1 metre.

▼M15

_____

▼B

12.2.5 HHMD shall have a visual indicator to show that the equipment is in operation.

12.3 X-RAY EQUIPMENT

X-ray equipment shall comply with the detailed requirements laid down in Commission Implementing Decision C(2015) 8005.

▼M13

12.3.1 All equipment installed from 1 January 2023 at the latest, to be used in the Union for the screening of cargo and mail, as well as air carrier mail and air carrier materials subject to security controls in accordance with Chapter 6, shall be multi-view.

The appropriate authority, for objective reasons, may allow the use of single-view X-ray equipment installed before 1 January 2023 until the following dates:

(a) single-view X-ray equipment installed before 1 January 2016, until 31 December 2025 at the latest;

(b) single-view X-ray equipment installed from 1 January 2016, for a maximum period of 10 years from the date of its installation or at the latest until 31 December 2027, whichever is the earlier.

The appropriate authority shall inform the Commission where it applies the provisions of the second paragraph.

▼B

12.4 EXPLOSIVE DETECTION SYSTEMS (EDS) EQUIPMENT

12.4.1 **General principles**

▼M16

12.4.1.1 Explosive detection systems equipment (EDS) shall be able to detect and to indicate by means of an alarm specified and higher individual quantities of explosive or chemical material contained in baggage or other consignments.

12.4.1.2 The detection shall be independent of the shape, position or orientation of the explosive or chemical material.

▼B

12.4.1.3 EDS shall give an alarm in each of the following circumstances:

▼M16

— when it detects explosive or chemical material, and

— when it detects the presence of an item that prevents explosive or chemical material from being detected, and

▼B

— when the contents of a bag or consignment are too dense to be analysed.

▼M12

12.4.2 **Standards for EDS**

12.4.2.1 All EDS equipment shall fulfil the following requirements:

(a) equipment installed before 1 September 2014 must at least meet standard 2;

(b) equipment installed from 1 September 2014 to 31 August 2022 must at least meet standard 3;

(c) equipment installed from 1 September 2022 to 31 August 2026 must at least meet standard 3.1;

(d) equipment installed from 1 September 2026 must at least meet standard 3.2.

12.4.2.2 Standard 2 shall expire on 1 September 2021.

12.4.2.3 For the purposes of allowing an extension of the use of standard 2 EDS, there shall be four categories of airports:

(a) category I – airport with more than 25 million passengers in 2019;

(b) category II – airport with scheduled services to at least one of the third countries listed in Attachment 5-A of this Regulation, with the exception of the United Kingdom of Great Britain and Northern Ireland;

(c) category III – airport with the highest volume of traffic in 2019 in each Member State where they are not already listed under category I or II;

(d) category IV – other airport.

12.4.2.4 The appropriate authority may allow the use of standard 2 EDS as of 1 September 2021, in accordance with the following table, until:

	Standard 2 EDS equipment installed before 1 January 2011	Standard 2 EDS equipment installed between 1 January 2011 and 1 September 2014
Airports in Category I	1 March 2022	1 March 2023
Airports in Category II or Category III	1 September 2022	1 September 2023
Airports in Category IV	1 March 2023	1 March 2024

▼M13

Additionally, the appropriate authority may allow the use of standard 2 EDS for the screening of cargo and mail as well as air carrier mail and air carrier materials subject to security controls in accordance with Chapter 6, until 1 September 2022 at the latest.

▼M12

12.4.2.5 The appropriate authority shall inform the Commission when it allows the use of standard 2 EDS to continue as of 1 September 2021.

12.4.2.6 All EDS equipment designed to screen cabin baggage shall meet at least standard C1.

12.4.2.7 All EDS equipment designed to screen cabin baggage containing portable computers and other large electrical items shall meet at least standard C2.

▼M12

12.4.2.8 All EDS equipment designed to screen cabin baggage containing portable computers and other large electrical items and LAGS shall meet at least standard C3.

12.4.2.9 All EDS equipment that meets standard C3 shall be considered as equivalent to LEDS equipment that meets standard 2 for the screening of LAGS.

▼B

12.4.3 **Image quality requirements for EDS**

Image quality for EDS shall comply with the detailed requirements laid down in Commission Implementing Decision C(2015) 8005.

12.5 THREAT IMAGE PROJECTION (TIP)

12.5.1 **General principles**

12.5.1.1 Threat image projection (TIP) shall be able to project combined threat images (CTI) or fictional threat images (FTI).

CTI are x-ray images of bags or other consignments containing threat articles.

FTI are x-ray images of threat articles which are projected into x-ray images of bags or other consignments being screened.

Threat articles shall appear within the x-ray image of bags and other consignments in an evenly distributed manner and not in a fixed position.

It shall be possible to set the percentage of CTI and FTI to be projected.

Where CTI are used:

(a) the concept of operation must ensure that the screener cannot see the bags or other consignments that are introduced into the x-ray or EDS equipment and cannot determine that a CTI is or might be projected to him/her; and

(b) the TIP system and library size shall reasonably ensure that a screener is not exposed to the same CTI again within 12 months.

▼M15

_____

▼B

12.5.1.2 TIP shall not impair the performance and normal functioning of x-ray or EDS equipment.

No indication shall be given to the screener that a CTI or FTI is about to be projected or has been projected until a message is presented in accordance with point 12.5.2.2.

12.5.1.3 The means for managing TIP shall be protected and accessible only to authorised persons.

12.5.1.4 There shall be a TIP administrator responsible for the configuration management of the TIP system.

12.5.1.5 The appropriate authority shall regularly monitor the correct implementation of the TIP systems and ensure that the systems are correctly configured, including realistic and relevant projection of CTI and FTI where in use, are in compliance with the requirements and have up-to-date image libraries.

▼B

12.5.2 **Composition of TIP**

12.5.2.1 TIP shall comprise of at least:

(a) a library of CTI or FTI; and

(b) a means for presenting messages and for messages to be cleared; and

(c) a means for recording and presenting the results of the responses of individual screeners.

12.5.2.2 TIP shall present a message to the screener in each of the following circumstances:

(a) where the screener responded and a CTI or FTI was projected;

(b) where the screener did not respond and a CTI or FTI was projected;

(c) where the screener responded and no CTI or FTI was projected;

(d) where an attempt to project a CTI or FTI failed and was visible to the screener.

The message shall be presented so that it does not obscure the image of the bag or consignment to which it refers.

The message shall remain until it has been cleared by the screener. In the case of points (a) and (b) the message shall be presented together with the CTI or FTI.

12.5.2.3 Access to equipment with TIP installed and deployed shall require that the screener uses a unique identifier.

12.5.2.4 TIP shall be able to store the results of the responses of individual screeners for a minimum of 12 months and in a format to allow the provision of reports.

12.5.2.5 The composition of TIP shall also be subject to the additional detailed requirements laid down in Commission Implementing Decision C(2015) 8005.

12.6 EXPLOSIVE TRACE DETECTION (ETD) EQUIPMENT

12.6.1 ►M16 ETD equipment shall be able to collect and analyse trace levels of particles from contaminated surfaces, or the contents of baggage or consignments, and indicate, by means of an alarm, the presence of explosives or chemicals. ◄ For the purpose of screening, it shall meet all of the following requirements:

(a) consumables shall not be used beyond the recommendations of the manufacturer of the consumable or if the performance of the consumable appears to have deteriorated through use;

(b) ETD equipment shall only be used in an environment for which the equipment has been approved for use.

▼M16

There shall be standards for ETD set for particulate sampling. Detailed requirements for these standards are laid down in Commission Implementing Decision C(2015) 8005.

12.6.2 The standard for ETD equipment for the detection of explosives, that uses particulate sampling, shall apply to ETD equipment deployed from 1 September 2014.

The standard for ETD equipment for the detection of chemicals, that uses particulate sampling, shall apply as of 1 July 2024 to ETD equipment deployed from 1 September 2014.

▼M15

———————

▼B

12.7 EQUIPMENT FOR SCREENING LIQUIDS, AEROSOLS AND GELS (LAGs)

12.7.1 **General principles**

12.7.1.1 LEDS equipment shall be able to detect and to indicate by means of an alarm specified and higher individual quantities of threat materials in LAGs.

▼M2

12.7.1.2 The equipment shall be used in a manner that ensures that the container is positioned and orientated so as to ensure that the detection capabilities are utilised in full.

12.7.1.3 The equipment shall give an alarm in each of the following circumstances:

(a) when it detects threat material;

(b) when it detects the presence of an item that prevents threat material from being detected;

(c) when it cannot assess whether the LAG is benign or not;

(d) when the contents of the screened bag are too dense to be analysed.

———————

▼B

12.7.2 **Standards for Liquid Explosive Detection Systems (LEDS) equipment**

12.7.2.1 There shall be three standards for LEDS equipment. Detailed requirements on these standards are laid down in Commission Implementing Decision C(2015) 8005.

▼M2

12.7.2.2 All LEDS equipment shall meet standard 2.

———————

▼M15

———————

▼B

12.8 METHODS OF SCREENING USING NEW TECHNOLOGIES

12.8.1 A Member State may allow a method of screening using new technologies other than those laid down in this Regulation, provided that:

(a) it is being used for the purpose of evaluating a new method of screening; and

(b) it will not negatively affect the overall level of security being attained; and

(c) appropriate information that a trial is being conducted shall be given to those affected, including passengers.

12.8.2 Before its planned introduction the Member State concerned shall inform in writing the Commission and the other Member States of the proposed method of screening it intends to allow, enclosing an assessment indicating how it shall guarantee that the application of the new method will meet the requirement of point 12.8.1(b). The notification shall also contain detailed information on the location(s) where the method of screening is planned to be used and the intended length of the evaluation period.

12.8.3 If the Commission gives the Member State a positive reply, or if no reply is received within three months upon receipt of the written request, the Member State may then allow the introduction of the method of screening using new technologies.

▼B

If the Commission is not satisfied that the proposed method of screening provides sufficient guarantees that the overall level of aviation security will be maintained in the Union, the Commission shall inform the Member State thereof within three months of receipt of the notification referred to in point 12.8.2, explaining its concerns. In such a circumstance the Member State concerned shall not commence with the method of screening until it has satisfied the Commission.

12.8.4 The maximum evaluation period for each method of screening using new technologies shall be eighteen months. This evaluation period may be extended by the Commission by a maximum of a further twelve months on condition that the Member State provides adequate justification for the extension.

12.8.5 At intervals of no more than six months during the evaluation period, the appropriate authority in the Member State concerned shall provide the Commission with a progress report on the evaluation. The Commission shall inform the other Member States of the contents of the progress report. If no progress reports are provided, the Commission may request the Member State to suspend the trial.

12.8.6 If, on the basis of a report, the Commission is not satisfied that the method of screening being trialled is providing sufficient guarantees that the overall level of aviation security is being maintained in the Union, the Commission shall inform the Member State that the trial shall be suspended until such guarantees can be given.

12.8.7 No evaluation period may be longer than thirty months.

12.9 EXPLOSIVE DETECTION DOGS

12.9.1 **General Principles**

12.9.1.1 An explosive detection dog (EDD) shall be able to detect and indicate specified and higher individual quantities of explosive material.

12.9.1.2 The detection shall be independent of the shape, position or orientation of the explosive materials.

12.9.1.3 An EDD shall give an alarm, in the form of a passive response, when it detects explosive materials set in Attachment 12-D of Commission Implementing Decision C(2015) 8005.

12.9.1.4 An EDD and its handler can be used for screening if they both have been approved independently and in combination as a team.

12.9.1.5 An EDD and its handler shall be subject to initial and recurrent training to ensure that required competencies are learned and maintained and, where appropriate, new competencies are learned.

12.9.1.6 In order to be approved, an EDD team, consisting of an EDD and handler(s), shall have successfully passed a training course.

▼M15

12.9.1.7 An EDD team shall be approved by or on behalf of the appropriate authority in accordance with Attachments 12-E and 12-F to Commission Implementing Decision C(2015) 8005. The appropriate authority may allow the deployment and use of EDD teams trained and/or approved by the appropriate authority of another Member State, provided it has formally agreed with the approving authority on the respective roles and responsibilities in ensuring that all the requirements in Chapter 12.9 of this Annex are fulfilled, in accordance with Attachment 12-P to this Annex. In the absence of such agreement, full responsibility for the fulfilment of all requirements in Chapter 12.9 of this Annex remains with the appropriate authority of the Member State where the EDD team is deployed and used.

▼B

12.9.1.8 After approval by the appropriate authority, an EDD team may be used for security screening by use of free running or remote explosive scent tracing method.

12.9.2 **Standards for EDD**

12.9.2.1 The performance requirements for an EDD are laid down in Attachment 12-D of Commission Implementing Decision C(2015) 8005.

12.9.2.2 An EDD team used for the screening of persons, cabin baggage, items carried by persons other than passengers, vehicles, aircraft, in-flight supplies and airport supplies, and security restricted areas of an airport shall meet detection standard 1.

12.9.2.3 An EDD team used for the screening of hold baggage, air carrier mail, air carrier materials, cargo and mail shall meet detection standard 2.

12.9.2.4 An EDD team approved to detect explosive materials using the remote explosive scent tracing method may only be used in screening of cargo, but no other areas included in standard 2.

▼M2

12.9.2.5 An EDD used for the detection of explosive materials shall be fitted with appropriate means to allow for the unique identification of the EDD.

▼B

12.9.2.6 When performing explosive detection duties, an EDD shall always be accompanied by the handler who is approved to work with the EDD.

12.9.2.7 An EDD approved for free running method shall only have one handler. One handler may be approved for leading a maximum of two EDDs.

12.9.2.8 An EDD approved for remote explosive scent tracing method shall be led by a maximum of two handlers per EDD.

12.9.3 **Training requirements**

General training obligations

12.9.3.1 The training of an EDD team shall include theoretical, practical and on-the-job training elements.

▼M15

12.9.3.2 The content of training courses shall be specified or approved by the appropriate authority. The theoretical training of the handler shall include the provisions laid down in Chapter 11.2 for the screening of the specific area or areas where the EDD team is approved.

▼B

12.9.3.3 The training shall be conducted by or on behalf of the appropriate authority using instructors qualified according to point 11.5.

12.9.3.4 Dogs to be trained for explosive detection shall be single purpose dogs.

12.9.3.5 During training, training aids representing explosive materials shall be used.

12.9.3.6 Training shall be provided to any persons handling the training aids so as to prevent contamination.

▼B

Initial training for EDD Teams

12.9.3.7 An EDD team shall be subject to initial training in accordance with the requirements laid down in point 12.9.3 of Commission Implementing Decision C(2015) 8005.

12.9.3.8 Initial training for EDD team shall include practical training in the intended work environment.

Recurrent training for EDD Teams

12.9.3.9 An EDD and the handler shall be subject to recurrent training requirements, both individually and in combination as a team.

12.9.3.10 Recurrent training shall maintain the existing competencies as required by the initial training and those acquired in line with security developments.

12.9.3.11 Recurrent training for an EDD team shall be performed at intervals of at least every 6 weeks. The minimum duration of the re-current training shall be no less than 4 hours in any 6 week period.

12.9.3.12 Point 11 shall not apply in the case where an EDD is subject to recognition training of all materials listed in Attachment 12-D of Commission Implementing Decision C(2015) 8005 on at least a weekly basis.

Training records for EDD Teams

12.9.3.13 The records of both initial and recurrent training shall be kept for both the EDD and its handler for at least the duration of their contract of employment and they shall be made available to the appropriate authority upon request.

Operational Training for EDD Teams

12.9.3.14 When EDD is deployed in the screening duties, the EDD shall be subject to operational training to ensure that it meets the performance set in Attachment 12-D of Commission Implementing Decision C(2015) 8005.

12.9.3.15 Operational training shall be done on a continuous random basis during the deployment period, and shall measure EDD's detection performance by means of approved training aids.

12.9.4 **Approval Procedures**

12.9.4.1 The approval procedure shall ensure that all of the following competencies are measured:

(a) ability of the EDD to meet the detection performance laid down in the Attachment 12-D of Commission Implementing Decision C(2015) 8005;

(b) ability of the EDD to give a passive indication on the presence of explosive materials;

(c) ability of the EDD and its handler(s) to work effectively as a team;

(d) ability of the handler to correctly lead the EDD, interpret and respond appropriately to the EDD's reaction to the presence of an explosive material.

12.9.4.2 The approval procedure shall simulate each of the work areas in which the EDD team shall work.

12.9.4.3 The EDD team shall have successfully completed training in each area for which the approval is sought.

12.9.4.4 The approval procedures shall be carried out in accordance with the Attachments 12-E and 12-F of Commission Implementing Decision C(2015) 8005.

▼B

12.9.4.5 The validity of each approval period shall not be longer than 12 months.

12.9.5 **Quality Control**

12.9.5.1 The EDD team shall be subject to quality control measures set out in the Attachment 12-G of Commission Implementing Decision C(2015) 8005.

12.9.6 **Methodology of Screening**

Further, detailed requirements are contained in Commission Implementing Decision C(2015) 8005.

12.10 METAL DETECTION EQUIPMENT (MDE)

Detailed provisions on the use of MDE are laid down in Commission Implementing Decision C(2015) 8005.

12.11 SECURITY SCANNERS

12.11.1 **General principles**

A security scanner is a system for the screening of persons that is capable of detecting metallic and non-metallic objects, distinct from the human skin, carried on the body or within clothes.

A security scanner with human reviewer may consist of a detection system that creates an image of a person's body for a human reviewer to analyse and establish that no metallic and non-metallic object, distinct from the human skin, is carried on the body of the person screened. When the human reviewer identifies such an object, its location shall be communicated to the screener for further search. In this case, the human reviewer is to be considered as an integral part of the detection system.

A security scanner with automatic threat detection may consist of a detection system that automatically recognises metallic and non-metallic objects, distinct from the human skin, carried on the body of the person screened. When the system identifies such an object, its location shall be indicated on a stick figure to the screener.

For the purpose of screening passengers, a security scanner shall meet all of the following standards:

(a) security scanners shall detect and indicate by means of an alarm at least specified metallic and non-metallic items including explosives both individually and in combination;

(b) detection shall be independent of the position and orientation of the item;

(c) the system shall have a visual indicator to show that the equipment is in operation;

(d) security scanners shall be positioned so as to ensure that their performance is not affected by sources of interference;

(e) the correct functioning of security scanners shall be tested on a daily basis;

(f) the security scanner shall be used in accordance with the concept of operations provided by the manufacturer.

▼B

Security scanners for the screening of passengers shall be deployed and used in compliance with Council Recommendation 1999/519/EC ([1]) and Directive 2013/35/EU of the European Parliament and of the Council ([2]).

12.11.2 **Standards for security scanners**

The performance requirements for security scanners are laid down in Attachment 12-K, which shall be classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL' and be handled in accordance with Decision (EU, Euratom) 2015/444.

Security scanners shall meet the standard defined in Attachment 12-K from the entry into force of this Regulation.

12.11.2.1 All security scanners shall meet standard 1.

Standard 1 shall expire on 1 January 2022.

12.11.2.2 Standard 2 shall apply to security scanners installed as of 1 January 2019.

▼M5

12.11.2.3 Standard 2.1 shall apply to security scanners installed from 1 January 2021.

12.12 SHOE SCANNER EQUIPMENT

12.12.1 **General principles**

12.12.1.1 Shoe metal detection (SMD) equipment shall be able to detect and to indicate by means of an alarm at least specified metallic items, both individually and in combination.

12.12.1.2 Shoe explosive detection (SED) equipment shall be able to detect and indicate by means of an alarm at least specified explosives items.

12.12.1.3 The detection by SMD and SED shall be independent of the position and orientation of the metallic or explosive items.

12.12.1.4 SMD and SED shall be placed on a solid base.

12.12.1.5 SMD and SED shall have a visual indicator to show that the equipment is in operation.

12.12.1.6 The means for adjusting the detection settings of SMD and SED shall be protected and accessible only to authorised persons.

12.12.1.7 SMD shall give at least a visual alarm and an audible alarm when it detects metallic items as refers to in point 12.12.1.1. Both types of alarm shall be noticeable at a range of 1 m.

12.12.1.8 SED shall give at least a visual alarm and an audible alarm when it detects explosive items as refers to in point 12.12.1.2. Both types of alarm shall be noticeable at a range of 1 m.

([1]) Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (OJ L 199, 30.7.1999, p. 59).

([2]) Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC (OJ L 179, 29.6.2013, p. 1).

▼M5

12.12.2 **Standards for SMD**

12.12.2.1 There shall be two standards for SMD. Detailed requirements on these standards are laid down in Commission Implementing Decision C(2015) 8005.

12.12.2.2 All SMD exclusively used for screening persons other than passengers shall meet at least standard 1.

12.12.2.3 All SMD used for screening of passengers shall meet standard 2.

12.12.2.4 All SMD shall be able to resolve alarms generated on a WTMD, in the area between the surface supporting the shoe and at least 35 cm above.

12.12.3 **Standard for SED**

12.12.3.1 Detailed requirements on this standard are laid down in Commission Implementing Decision C(2015) 8005.

▼M16

12.13 AUTOMATED PROHIBITED ITEMS DETECTION (APID) SOFTWARE

12.13.1 **General principles**

12.13.1.1 Automated Prohibited Items Detection (APID) software shall be able to detect and to indicate by means of an alarm prohibited items contained in baggage or other consignments.

12.13.2 **Standards for APID software**

12.13.2.1 There shall be three standards for APID software. Detailed requirements on these standards are laid down in Commission Implementing Decision C(2015) 8005.

12.14 EXPLOSIVE VAPOUR DETECTION (EVD) EQUIPMENT

12.14.1 **General principles**

12.14.1.1 Explosives Vapour Detection (EVD) equipment shall be able to collect samples of air and analyse the collected sample for vapour, aerosols and/or airborne particles indicating the presence of explosives and explosive related materials.

If trace levels of explosives or explosive related materials are found in the sample, the EVD equipment shall indicate an alarm.

12.14.1.2 For the purpose of screening with EVD equipment, the following requirements shall apply:

(a) EVD equipment shall only be used in an environment and for the purpose for which it has been approved, i.e. screening of:

— Passengers and persons other than passengers (EVD-PX);

— Cabin baggage (EVD-CB);

— Hold baggage (EVD-HB);

— Air cargo and mail, air carrier mail and air carrier materials, in-flight supplies and airport supplies (EVD-CS);

(b) consumables shall not be used beyond the recommendations of their manufacturer or if the performance of the consumable appears to have deteriorated through use.

▼M16

12.14.2 **Standards for EVD**

12.14.2.1 All EVD equipment used for the screening of hold baggage, air cargo and mail, air carrier mail and air carrier materials loaded in the aircraft hold, in-flight supplies as well as airport supplies shall meet at least standard 1.

12.14.2.2 All EVD equipment used for the screening of passengers and persons other than passengers as well as cabin baggage shall meet at least standard 3.

12.14.2.3 Detailed requirements on these standards are laid down in Commission Implementing Decision C(2015) 8005.

▼B

ATTACHMENT 12-A

Detailed provisions for performance requirements for WTMD and SMD are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-B

Detailed provisions for performance requirements for EDS are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-C

Detailed provisions for performance requirements for equipment for the screening of liquids, aerosols and gels (LAGS) are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-D

Detailed provisions for performance requirements for an EDD are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-E

Detailed provisions for approval procedures of an EDD are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-F

Detailed provisions for approval test areas and test conditions for an EDD are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-G

Detailed provisions for quality control requirements for an EDD are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-H

Detailed provisions for ‘Free Running EDD — Standards for deployment methodology’ are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-I

Detailed provisions for ‘Remote Explosive Scent Tracing EDD — Standards for deployment methodology’ are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-J

Detailed provisions for performance requirements for MDE are laid down in Commission Implementing Decision C(2015) 8005.

▼B

ATTACHMENT 12-K

Detailed provisions for performance requirements for security scanners are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-L

Detailed provisions for performance requirements for Explosive Trace Detection (ETD) are laid down in Commission Implementing Decision C(2015) 8005.

▼M16

ATTACHMENT 12-M

Detailed provisions for performance requirements for APID are laid down in Commission Implementing Decision C(2015) 8005.

▼M10

ATTACHMENT 12-N

Detailed provisions for performance requirements for SED are laid down in Commission Implementing Decision C(2015) 8005.

ATTACHMENT 12-O

Detailed provisions for performance requirements for EVD are laid down in Commission Implementing Decision C(2015) 8005.

▼M15

ATTACHMENT 12-P

LETTER OF UNDERSTANDING BETWEEN APPROPRIATE AUTHORITIES SUPPORTING THE DEPLOYMENT OF EDD TEAMS

This letter of understanding is established between the following parties:

The appropriate authority receiving support for the deployment of EDD teams:

.....

The appropriate authority or authorities providing support for the deployment of EDD teams:

.....

For the identification of the following roles [1] to ensure that the deployment of EDD teams meets EU requirements:

Appropriate authority in charge of specifying or approving the content of training courses:

.....

Appropriate authority in charge of approving EDD teams:

.....

Appropriate authority in charge of the external quality control:

.....

For the following period of validity:

Date:

Signatures:

[1] Should there be a need, this letter of understanding may be supplemented with additional details and amended as needed in order to specify the roles of the appropriate authorities, and to determine its scope of application.