COMMISSION IMPLEMENTING REGULATION (EU) 2015/1998

of 5 November 2015

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

(Text with EEA relevance)

Introductory Text

Article 1 The detailed measures for the implementation of the basic...
Article 2 Regulation (EU) No 185/2010 is repealed. References to the repealed...
Article 3 This Regulation shall enter into force on the day following...

ANNEX

1. AIRPORT SECURITY
- 1.1 AIRPORT PLANNING REQUIREMENTS
  - 1.1.1 Boundaries
  - 1.1.2 Security restricted areas
  - 1.1.3 Critical parts of security restricted areas
- 1.2 ACCESS CONTROL
  - 1.2.1 Access to airside
  - 1.2.2 Access to security restricted areas
  - 1.2.3 Requirements for Gibraltar crew identification cards and airport identification cards
  - 1.2.4 Supplementary requirements for Gibraltar crew identification cards
  - 1.2.5 Supplementary requirements for airport identification cards
  - 1.2.6 Requirements for vehicle passes
  - 1.2.7 Escorted access
  - 1.2.8 *Omitted*
- 1.3 SCREENING OF PERSONS OTHER THAN PASSENGERS AND ITEMS CARRIED
  - 1.3.1 Screening of persons other than passengers and items carried
  - 1.3.2 Exemptions and special screening procedures
- 1.4 EXAMINATION OF VEHICLES
  - 1.4.1 Vehicles entering critical parts
  - 1.4.2 Vehicles entering security restricted areas other than critical parts
  - 1.4.3 Methods of examination
  - 1.4.4 Exemptions and special examination procedures
- 1.5 SURVEILLANCE, PATROLS AND OTHER PHYSICAL CONTROLS
- 1.6 PROHIBITED ARTICLES

2. DEMARCATED AREAS OF AIRPORTS

3. AIRCRAFT SECURITY
- 3.1 AIRCRAFT SECURITY SEARCH

3.1.1 When to perform an aircraft security search
3.1.2 *Omitted*
3.1.3 Information on the aircraft security search
3.2 PROTECTION OF AIRCRAFT
3.2.1 Protection of aircraft — General
3.2.2 Additional protection of aircraft with closed external doors in a part other than a critical part
4. PASSENGERS AND CABIN BAGGAGE
4.1 SCREENING OF PASSENGERS AND CABIN BAGGAGE
4.1.1 Screening of passengers
4.1.2 Screening of cabin baggage
4.1.3 Screening of liquids, aerosols and gels (LAGs)
4.2 *Omitted*
4.3 POTENTIALLY DISRUPTIVE PASSENGERS
4.4 PROHIBITED ARTICLES
5. HOLD BAGGAGE
5.1 SCREENING OF HOLD BAGGAGE
5.2 PROTECTION OF HOLD BAGGAGE
5.3 BAGGAGE RECONCILIATION
5.3.1 Identification of hold baggage
5.3.2 Factors beyond the passenger's control
5.3.3 Appropriate security controls for unaccompanied hold baggage
5.4 PROHIBITED ARTICLES
6. **CARGO AND MAIL**
6.1 SECURITY CONTROLS — GENERAL PROVISIONS
6.2 SCREENING
6.2.1 Screening
6.2.2 *Omitted*
6.3 REGULATED AGENTS
6.3.1 Approval of regulated agents
6.3.2 Security controls to be applied by a regulated agent
6.4 KNOWN CONSIGNORS
6.4.1 Approval of known consignors
6.4.2 Security controls to be applied by a known consignor
6.5 *Omitted*
6.6 PROTECTION OF CARGO AND MAIL
6.6.1 Protection of cargo and mail during transportation
6.6.2 Protection for cargo and mail during handling, storage, and loading onto an aircraft
6.7 *Omitted*
6.8 SECURITY PROCEDURES FOR CARGO AND MAIL BEING CARRIED INTO GIBRALTAR FROM OTHER COUNTRIES
6.8.1 Designation of air carriers
6.8.2 *Omitted*

6.8.3 Security controls for cargo and mail arriving from another country
6.8.4 Designation of regulated agents and known consignors
6.8.5 *Omitted*
6.8.6 Non-compliance and discontinuation of GIBRALTAR-ACC3, RA3 and KC3 designation
7. AIR CARRIER MAIL AND AIR CARRIER MATERIALS
7.1 AIR CARRIER MAIL AND AIR CARRIER MATERIALS TO BE LOADED ONTO AN AIRCRAFT
7.2 AIR CARRIER MATERIALS USED FOR PASSENGER AND BAGGAGE PROCESSING
8. IN-FLIGHT SUPPLIES
8.1 SECURITY CONTROLS
8.1.1 Security controls — general provisions
8.1.2 Screening
8.1.3 Approval of regulated suppliers
8.1.4 Designation of known suppliers
8.1.5 Security controls to be applied by an air carrier, a regulated supplier and a known supplier
8.2 *Omitted*
8.3 ADDITIONAL SECURITY PROVISIONS FOR IN-FLIGHT SUPPLIES OF LAGS AND STEBS
9. AIRPORT SUPPLIES
9.1 SECURITY CONTROLS
9.1.1 Security controls — general provisions
9.1.2 Screening
9.1.3 Designation of known suppliers
9.1.4 Security controls to be applied by a known supplier or airport operator
9.2 *Omitted*
9.3 ADDITIONAL SECURITY PROVISIONS FOR SUPPLIES OF LAGS AND STEBS
10. IN-FLIGHT SECURITY MEASURES
11. STAFF RECRUITMENT AND TRAINING
11.1 RECRUITMENT
11.2 TRAINING
11.2.1 General training obligations
11.2.2 Basic training
11.2.3 Job specific training for persons implementing security controls
11.2.4 Specific training for persons directly supervising persons implementing security controls (supervisors)
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)

11.2.6 Training of persons other than passengers requiring unescorted access to security restricted areas
11.2.7 Training of persons requiring general security awareness
11.3 CERTIFICATION OR APPROVAL
11.4 RECURRENT TRAINING
11.5 QUALIFICATION OF INSTRUCTORS
11.6 AVIATION SECURITY VALIDATION
11.6.2 Aviation security validation
11.6.3 Approval requirements for aviation security validators
11.6.4 Recognition and discontinuation of aviation security validators
11.6.5 Aviation security validation report (‘the validation report’)
11.7 *Omitted*
12. SECURITY EQUIPMENT
12.0 GENERAL PROVISION AND APPROVAL OF SECURITY EQUIPMENT
12.0.1 General provision
12.0.2 Approval of security equipment
12.0.3 ‘ EU Stamp ’ marking and Union database on supply chain security — security equipment
12.0.4 Suspension and withdrawal of ‘ EU Stamp ’ marking
12.0.5 More stringent measures on security equipment and national approval
12.1 WALK-THROUGH METAL DETECTION (WTMD) EQUIPMENT
12.1.1 General principles
12.1.2 Standards for WTMD
12.1.3 Additional requirements for WTMD
12.1.4 Additional requirements for WTMD used in combination with shoe metal detection (SMD) equipment
12.2 HAND-HELD METAL DETECTION (HHMD) EQUIPMENT
12.3 *Omitted*
12.4 EXPLOSIVE DETECTION SYSTEMS (EDS) EQUIPMENT
12.4.1 General principles
12.4.2 Standards for EDS
12.4.3 *Omitted*
12.5 THREAT IMAGE PROJECTION (TIP)
12.5.1 General principles
12.5.2 Composition of TIP
12.6 EXPLOSIVE TRACE DETECTION (ETD) EQUIPMENT
12.7 EQUIPMENT FOR SCREENING LIQUIDS, AEROSOLS AND GELS (LAGs)
12.7.1 General principles
12.7.2 Standards for Liquid Explosive Detection Systems (LEDS) equipment
12.7.3 Approval of equipment for the screening of LAGs

12.8 METHODS OF SCREENING USING NEW TECHNOLOGIES
12.9 EXPLOSIVE DETECTION DOGS
12.9.1 General Principles
12.9.2 Standards for EDD
12.9.3 Training requirements
12.9.4 Approval Procedures
12.9.5 Quality Control
12.9.6 *Omitted*
12.10 *Omitted*
12.11 SECURITY SCANNERS
12.11.1 General principles
12.11.2 *Omitted*
12.12 SHOE SCANNER EQUIPMENT
12.12.1 General principles
12.12.2 Standards for SMD
12.12.3 *Omitted*
12.13 AUTO CLEAR SOFTWARE (ACS)
12.13.1 General principles
12.13.2 *Omitted*
12.14 EXPLOSIVE VAPOUR DETECTION (EVD) EQUIPMENT
12.14.1 Standards for EVD

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1998

of 5 November 2015

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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, and in particular Article 4(3) thereof,

Whereas:

(1) In accordance with Article 4(3) of Regulation (EC) No 300/2008, the Commission should adopt detailed measures for the implementation of common basic standards referred to in Article 4(1) and of general measures supplementing common basic standards referred to in Article 4(2) of that Regulation.

(2) If they contain sensitive security information, those measures should be treated in accordance with Commission Decision (EU, Euratom) 2015/444, as provided for by point (a) of Article 18 of Regulation (EC) No 300/2008. Those measures should therefore be adopted separately, by means of a Commission Implementing Decision addressed to the Member States, and should not be published.

(3) Commission Regulation (EU) No 185/2010, which lays down the measures referred to in Article 4(3) of Regulation (EC) No 300/2008, was amended 20 times since its entry into force. In order to ensure

clarity and legal certainty, it should therefore be repealed and replaced by a new act, consolidating the initial act and all amendments thereto. That new act should also be clarified and updated where appropriate, in light of the practical experiences gained and the relevant technological developments.

(4) These measures should be reviewed regularly to ensure they are commensurate with the evolution of the threat.

(5) The measures provided for in this Regulation are in accordance with the opinion of the Committee on Civil Aviation Security set up by Article 19(1) of Regulation (EC) No 300/2008,

HAS ADOPTED THIS REGULATION:

Article 1

The detailed measures for the implementation of the 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 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.

Done at Brussels, 5 November 2015.

ANNEX.

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.

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, 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.

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.

1.1 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.

1.1.1.2 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.

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

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.

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.

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 any airport other than an airport designated by the appropriate authority;

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 point (b) is 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

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.

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.

1.2.3 Requirements for Gibraltar crew identification cards and airport identification cards

1.2.3.1 A crew identification card of a crew member employed by a Gibraltar air carrier and an airport identification card may only be issued to a person who has an operational need and has successfully completed a 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 a background check shall be immediately withdrawn.

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 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 to the issuing entity:

(a) upon request of the issuing entity; or

(b) upon termination of employment; or

(c) upon change of employer; or

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

(e) upon expiry of the card; or

(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.

1.2.4 Supplementary requirements for Gibraltar crew identification cards

1.2.4.1 A crew identification card of a crew member employed by a Gibraltar 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.

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

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. Electronic vehicle passes shall also be electronically readable airside.

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).

1.2.8 ***Omitted***

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;

(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.

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.

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.

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) explosive detection dogs;

(e) explosive trace detection (ETD) equipment.

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

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.

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.

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.

1.3.2 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.

1.4 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.

1.4.2 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.

1.4.3 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.

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.

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.

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.

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.

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.

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.

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;

(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 *Omitted*

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.

3.0.6 *Omitted*

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.

3.1 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 *Omitted*

3.1.1.3 An aircraft arriving into a critical part from any airport other than an airport designated by the appropriate authority 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.

3.1.2 *Omitted*

3.1.3 Information on the aircraft security search

The following information on the aircraft security search 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; and

(b) origin of the previous flight.

Where an aircraft security search was performed, the information shall also include:

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

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

Recording of the information as above, may be held in electronic format.

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

(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.

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 *Omitted*

4.0.3 *Omitted*

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;

(c) ‘liquid explosive detection systems (LEDS) equipment’ is a piece of equipment capable of detecting threat materials.

4.1 SCREENING OF PASSENGERS AND CABIN BAGGAGE

4.1.1 Screening of passengers

4.1.1.1 Before screening, coats and jackets shall be taken off and shall be screened as cabin baggage. The screener may request the passenger to undertake further divesting as appropriate.

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;

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

(g) shoe metal detection (SMD) equipment;

(h) shoe explosive detection (SED) equipment.

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.

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.

4.1.1.8 *Omitted*

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

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. 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.

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

(e) 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.

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.

4.1.2.5 Where x-ray or EDS equipment is used, each image shall be viewed by the screener or analysed by auto clear software (ACS).

4.1.2.6 Where x-ray or EDS equipment is used, all alarms 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.

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.

4.1.3 Screening of liquids, aerosols and gels (LAGs)

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.

4.1.3.2 . . . . . .

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.

4.2 ***Omitted***

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.

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-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;

(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 *Omitted*

5.0.3 *Omitted*

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.

5.1 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.

5.1.6 *Omitted*

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.

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

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.

5.3.3 **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.

5.3.3.2 Hold baggage that becomes unaccompanied baggage due to factors other than those designated by the appropriate authority shall be removed from the aircraft and rescreened before loading it again.

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.

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.

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,
- 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.

6.1 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

(c) *Omitted*

(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.

6.1.3 A person with unescorted access to identifiable air cargo or identifiable air mail to which the required security controls have been applied shall have successfully completed either a background check or a pre-employment check in accordance with point 11.1.

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 *Omitted*

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;

(g) metal detection equipment (MDE).

6.2.1.6 If agreed by the appropriate authority, 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 *Omitted*

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 in which the sites included in the application are located.

(b)

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 signed declaration shall be retained by the appropriate authority concerned;

(c)

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 Regulation (EC) No 300/2008 and its implementing acts.

Except for the requirements laid down in point 6.2, an examination of the site of the applicant by the relevant customs authority in accordance with Article 14n of Commission Regulation (EEC) No

2454/93 ([3]) shall be considered as an on-site verification if it took place not earlier than 3 years before the date on which the applicant seeks approval as a regulated agent. The AEO certificate and the relevant assessment of the customs authorities shall be made available by the applicant for further inspection.

(d) 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 '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;

(e) a regulated agent shall not be considered as approved until its details are listed in the '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.

6.3.1.5 If the appropriate authority is no longer satisfied that the regulated agent complies with the requirements of Regulation (EC) No 300/2008 and its implementing acts, it shall withdraw the status of regulated agent for the specified site(s).

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

6.3.1.6 *Omitted*

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.

6.3.1.8 *Omitted*

6.3.2 Security controls to be applied by a regulated agent

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 .

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.

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

(a) screened in accordance with point 6.2; or

(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.

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 have been applied, the regulated agent shall ensure the protection of cargo and mail in accordance with point 6.6.

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 small consignments or consolidations of such consignments designated by the appropriate authority;

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

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

- ‘SCO’, meaning secure for all-cargo and all-mail aircraft only, or

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

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

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

(ii) *Omitted*

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

(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);

- visual check (VCK);

- metal detection equipment (CMD);

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

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

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

(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.

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.

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 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.

6.3.2.9 A regulated agent shall ensure that all staff implementing security controls are recruited and trained in accordance with the requirements of Chapter 11 and all staff with access to identifiable air cargo or identifiable air mail to which the required security controls have been applied have been recruited and subject to security awareness training in accordance with the requirements of Chapter 11.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:

(a)
the applicant shall seek approval from the appropriate authority.

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)
he appropriate authority, or 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 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.

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

(c)
Omitted

(d)
if the appropriate authority is satisfied with the information provided under points (a) and (b) Union, 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), 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 ‘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.

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

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

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

(b) all staff implementing security controls are recruited and trained in accordance with the requirements of Chapter 11 and all staff with access to identifiable air cargo or identifiable air mail to which the required security controls have been applied have been recruited and subject to security awareness training in accordance with the requirements of Chapter 11; and

(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.

6.5 *Omitted*

6.6 PROTECTION OF CARGO AND MAIL

6.6.1 Protection of cargo and mail during transportation

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:

(a) the consignments shall be packed or sealed by the regulated agentor 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; and

(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; and

(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), 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.

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

6.6.2 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.

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.

6.7 ***Omitted***

6.8 SECURITY PROCEDURES FOR CARGO AND MAIL BEING CARRIED INTO GIBRALTAR FROM OTHER COUNTRIES

6.8.1 Designation of air carriers

6.8.1.1 Any air carrier carrying cargo or mail from an airport in another country 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 Gibraltar from Another Country Airport’ (GIBRALTAR-ACC3) by the appropriate authority.

This requirement does not apply in respect of a country or territory designated by the appropriate authority.

6.8.1.2 The designation of an air carrier as GIBRALTAR-ACC3 in respect of its cargo and mail operations from an airport for which GIBRALTAR-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 assessment by the appropriate authority of relevant evidence (which for the purpose of this Regulation may include a validation report) confirming the implementation of security measures.

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

6.8.1.4 The designation shall be valid from the date the appropriate authority has entered the GIBRALTAR-ACC3's details into the database on supply chain security, for a period of five years, unless the appropriate authority determines that the designation shall cease to be valid on an earlier date or determines that the designation remains valid for a further period not exceeding three months.

6.8.1.5 A GIBRALTAR-ACC3 listed on the database on supply chain security shall be recognised by the appropriate authority for all operations from an airport in another country into Gibraltar.

6.8.1.7 During the period from 1 April to 31 December 2020 , 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;

(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.

6.8.2 ***Omitted***

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

(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.

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.

6.8.3 Security controls for cargo and mail arriving from another country

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

(a) the required security controls have been applied to the consignment by an 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 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

(c) *Omitted*

(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.

6.8.3.2 Cargo and mail carried into Gibraltar 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 GIBRALTAR-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 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 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.

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

6.8.3.5 When accepting any consignments, an GIBRALTAR-ACC3 or RA3 shall establish whether the air carrier or the entity from which it receives the consignments is another GIBRALTAR-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 database on supply chain security for the specified airport or site, as appropriate.

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 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 GIBRALTAR-ACC3 or by another aviation security validated RA3 before being loaded onto the aircraft.

6.8.3.6 After the security controls referred to in points 6.8.3.1 to 6.8.3.5 have been applied, the GIBRALTAR-ACC3 or the aviation security validated regulated agent (RA3) operating on its behalf shall ensure that the accompanying documentation, either in the form of an air waybill, equivalent postal documentation or in a separate declaration and either in an electronic format or in writing, indicate at least:

(a) the unique alphanumeric identifier of the GIBRALTAR-ACC3; and

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

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

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

(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 Consignment Security Declaration scheme.

In the case of consolidations, the GIBRALTAR-ACC3 or the aviation security validated regulated agent (RA3) who has performed the consolidation retains the information required above for each individual consignment at least until the estimated time of arrival of the consignments at the first airport in Gibraltar or for 24 hours, whichever is the longer.

6.8.3.7 *Omitted*

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.

6.8.3.9 Transit or transfer consignments arriving from a third country not listed in Attachment 6-I whose accompanying documentation does not comply with point 6.8.3.6 shall be treated in accordance with Chapter 6.2 before the subsequent flight. Accompanying documentation of consignments arriving from a third country listed in Attachment 6-F shall at least comply with the ICAO Consignment Security Declaration scheme.

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

6.8.4.1 Entities from another country being, or intending to be, part of the supply chain of an air carrier holding the status of GIBRALTAR-ACC3, may be designated as either ‘regulated agent for another country’ (RA3) or ‘known consignor from another country’ (KC3).

6.8.4.2 To obtain designation, the entity shall address the request to the appropriate authority.

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 assessment by the appropriate authority of relevant evidence (which for the purpose of this Regulation may include a 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 other country for which it has been designated to implement security provisions in respect of cargo or mail bound for Gibraltar.

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

6.8.4.7 *Omitted*

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 *Omitted*

6.8.4.11 During the period from 1 April to 31 December 2020 , 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:

(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;

(d) 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 previous expiry.

6.8.5 *Omitted*

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

6.8.6.1 *Non-Compliance*

1. If the appropriate authority identifies a serious deficiency relating to the operations of an GIBRALTAR-ACC3, an RA3 or a KC3, which is deemed to have a significant impact on the overall level of aviation security in Gibraltar, it shall:

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

2. Where the GIBRALTAR-ACC3, the RA3 or the KC3 has not rectified the serious deficiency within a specific time-frame, or in case the GIBRALTAR-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 shall:

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

3. An air carrier or entity whose status, respectively as an GIBRALTAR-ACC3, RA3 or KC3, has been deactivated in accordance with point 6.8.6.1.2 shall not be reinstated or included in the database on supply chain security until an 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 GIBRALTAR-ACC3, RA3 or KC3 status, the appropriate authority shall undertake appropriate action to satisfy itself that other GIBRALTAR-ACC3s, RA3s and KC3s under its 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 GIBRALTAR-ACC3, the RA3 or the KC3, is responsible for removing the details thereof from the ‘database on supply chain security’:

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

(b) where the GIBRALTAR-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.

2. If an air carrier or an entity is no longer a holder of the GIBRALTAR-ACC3, RA3 or KC3 status, the appropriate authority shall undertake appropriate action to satisfy itselfthat other GIBRALTAR-ACC3s, RA3s and KC3s under its 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.]

ATTACHMENT 6-A

DECLARATION OF COMMITMENTS — REGULATED AGENT

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council ([5]) on 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 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:

(a) minor changes to its security programme, such as company name, person responsible for security or contact details, change of person requiring access to the ‘database on supply chain security’, promptly

and 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 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 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 legislation.

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 ([6]) 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 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.

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.

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,), 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**.

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.

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 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.

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 *Omitted*	
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	

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 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	

3.4 **Do staff with access to identifiable air cargo/air mail receive security awareness training in accordance with point 11.2.7 of the Annex to Implementing Regulation (EU) 2015/1998 before being given access to identifiable air cargo/air mail? Do staff implementing security controls in respect of supplies receive training in accordance with Chapter 11 of the Annex to Implementing Regulation (EU) 2015/1998?**

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	

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	

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	
5.4If 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) 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	

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?	

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

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 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)

ATTACHMENT 6-E

HAULIER DECLARATION

In accordance with Regulation (EC) No 300/2008 of the European Parliament and of the Council ([3]) and its implementing acts,

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:

- All staff who transport this air cargo/mail will have received general security awareness training in accordance with point 11.2.7 of the Annex to Implementing Regulation (EU) 2015/1998;
- 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:

(a) has a haulier agreement with the regulated agent or known consignor responsible for the transport [same name as above]; or

(b) is approved or certified by the appropriate authority; or

(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

- 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.

I accept full responsibility for this declaration.

Name:

Position in company:

Name and address of the company:

Date:

Signature:

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 *Omitted*

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.

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 In-flight supplies shall be screened 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.

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.

8.1.2 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 *Omitted*

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);

(f) explosive detection dogs in combination with point (a).

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 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.

The signed declaration shall be retained by the appropriate authority concerned;

(b) the appropriate authority, or an 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;

(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 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 database on supply chain security.

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.

8.1.4 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:

(a) the 'Declaration of commitments — known supplier of in-flight supplies' as contained in Attachment 8-B. This declaration shall be signed by the legal representative; and

(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.

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 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

(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 these supplies; and

(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.

8.2 *Omitted*

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.

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 ([4]) 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 Gibraltar 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 Gibraltar 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 Gibraltar 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 ([5]) and its implementing acts,

I declare that,

- [name of company] will

(a) appoint a person responsible for security in the company; and

(b) ensure that persons with access to in-flight supplies receive general security awareness training in accordance with point 11.2.7 of the Annex to Implementing Regulation (EU) 2015/1998 before being given access to these supplies. In addition, ensure that persons implementing screening of in-flight supplies receive training according to 11.2.3.3 of the Annex to Implementing Regulation (EU) 2015/1998 and persons implementing other security controls in respect of in-flight supplies receive training according to 11.2.3.10 of the Annex to Implementing Regulation (EU) 2015/1998; and

(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 Gibraltar 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.

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 Airport supplies shall be screened before being allowed into security restricted areas, 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 *Omitted*

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;

(c) x-ray equipment;

(d) EDS equipment;

(e) ETD equipment in combination with point (a);

(f) explosive detection dogs in combination with point (a).

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:

(a) the ‘Declaration of commitments — known supplier of airport supplies’ as contained in Attachment 9-A. This declaration shall be signed by the legal representative; and

(b) the security programme covering the security controls as referred to in point 9.1.4.

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.

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.

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 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.

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

(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; and

(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.

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 *Omitted*

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.

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 ([6]) and its implementing acts,

I declare that,

- [name of company] will

(a) appoint a person responsible for security in the company; and

(b) ensure that persons with access to airport supplies receive general security awareness training in accordance with point 11.2.7 of the Annex to Implementing Regulation (EU) 2015/1998 before being given access to these supplies. In addition, ensure that persons implementing screening of airport supplies receive training according to point 11.2.3.3 of the Annex to Implementing Regulation (EU) 2015/1998 and persons implementing other security controls in respect of airport supplies receive training according to point 11.2.3.10 of the Annex to Implementing Regulation (EU) 2015/1998; and

(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,
- [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.

11.1 RECRUITMENT

11.1.1 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 shall have successfully completed a background check.

11.1.2 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 shall have successfully completed a background check.

Persons having completed a pre-employment check shall undergo a background check by 30 June 2021 at the latest.

11.1.3 In accordance with the applicable rules of national law, a background check shall at least:

(a) establish the person's identity on the basis of documentary evidence; and

(b) cover criminal records in all states of residence during at least the preceding 5 years; and

(c) cover employment, education and any gaps during at least the preceding 5 years.

11.1.4 In accordance with the applicable rules of national law, a pre-employment check shall:

(a) establish the person's identity on the basis of documentary evidence; and

(b) cover employment, education and any gaps during at least the preceding 5 years; and

(c) require the person to sign a declaration detailing any criminal history in all states of residence during at least the preceding 5 years.

11.1.5 Background or pre-employment checks shall be completed before the person undergoes any security training involving access to information which is not publicly available. Background checks shall be repeated at regular intervals not exceeding five years.

11.1.6 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.

11.1.7 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.

11.1.8 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.

11.2 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.

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;

(e) knowledge of identification card systems in use;

(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;

(k) ability to communicate clearly and confidently.

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;

(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;

(b) awareness of the relevant legal requirements;

(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;

(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 follov

(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;

(b) awareness of the relevant legal requirements;

(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;

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:

(a) knowledge of the legal requirements for aircraft security searches;

(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:

(a) knowledge of how to protect and prevent unauthorised access to aircraft;

(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;

(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;

(b) awareness of the relevant legal requirements;

(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.

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.

11.2.3.9 Training of persons implementing security controls for cargo and mail 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;

(b) awareness of the relevant legal requirements;

(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;

(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.

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.

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;

(b) awareness of the relevant legal requirements;

(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.

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.

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:

(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 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.

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;

(b) awareness of the relevant legal requirements;

(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;

(b) awareness of the relevant legal requirements;

(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;

(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.

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

(b) for persons operating x-ray or EDS equipment, recertification at least every 3 years; and

(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.

11.3.2 Persons operating x-ray or EDS equipment, 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.

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.

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.

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.

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:

shall be provided to the person and recorded;

shall be used to identify weaknesses and inform future training and testing adapted to address those weaknesses; and

may be taken into consideration as part of the recertification or re-approval process.

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.

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:

(a) the successful completion of a background check in accordance with points 11.1.3 and 11.1.5;

(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.

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 11.2.3.10) and 11.2.5.

Instructors shall be subject to recertification at least every 5 years.

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 Gibraltar.

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.

11.6 AVIATION SECURITY VALIDATION

11.6.1 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 Aviation security validation

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) may be performed by an appropriate authority or a validator approved as 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;

11.6.3 Approval requirements for aviation security validators

11.6.3.1 The appropriate authority shall approve 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 *Omitted*

11.6.3.3 An aviation security validator may be any individual or a legal entity.

11.6.3.4 *Omitted*

11.6.3.5 Every individual performing aviation security validation shall have appropriate competence and background, and shall meet all of the following requirements:

(a) have been subject to a background check in accordance with 11.1.3 that shall be recurrent at least every five years;

(b) perform 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 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 aviation security validator or approve and maintain a list of appropriate security training courses.

11.6.3.7 *Omitted*

11.6.3.8 The approval of an aviation security validator shall expire after a maximum period of five years.

11.6.4 Recognition and discontinuation of aviation security validators

11.6.4.1 An aviation security validator shall not be considered as approved until its details are recorded by the appropriate authority. Every aviation security validator shall be provided with proof of its status by or on behalf of the appropriate authority.

11.6.4.2 *Omitted*

11.6.4.3 When the appropriate authority 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.

11.6.4.4 Industry associations and entities under their responsibility operating quality assurance programmes may be approved as aviation security validators provided equivalent measures of those programmes ensure impartial and objective validation.

11.6.5 Aviation security validation report (‘the validation report’)

11.6.5.1 A validation report, where required, shall record the aviation security validation and contain at least:

(a) a completed checklist signed by the 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 aviation security validation.

11.6.5.2 The 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 aviation security validation and initialling by the validator and the validated entity on each page shall prove the validation report's integrity. Manual initialling on each page may be replaced by an electronic signature of the entire document.

11.6.5.6 By default the report shall be in English and delivered to the appropriate authority, where applicable, along with the validated entity within a maximum of one month after the on-site verification.

11.7 *Omitted*

ATTACHMENT 11-A

INDEPENDENCE DECLARATION — 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 aviation security validation report is based on a thorough fact finding evaluation of relevant s

- the validated entities' security programme or equivalent, and

- an on- site verification of the implementation thereof.

(f) I confirm that the 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 checklist.

(g) I confirm that I have applied a methodology that allows for separate 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.

(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 aviation security validation report.

Name of the validated entity:

Name of the aviation security validator:

Date:

Signature:

12. SECURITY EQUIPMENT

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

12.0.2.1. Without prejudice to point 12.0.5, the following security equipment 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 provided for in points 12.0.2.5 and 12.0.2.6:

(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);
(f) security scanners;
(g) shoe scanner equipment; and
(h) explosive vapour detection (EVD) equipment.

12.0.2.2. The Commission shall approve the security equipment listed in 12.0.2.1 and shall grant the ‘ EU Stamp ’ marking.

12.0.2.3. The ‘ EU Stamp ’ marking may be granted only to security equipment tested by test centres for which an appropriate authority has the responsibility for quality control measures in accordance with the Common Evaluation Process of the European Civil Aviation Conference.

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 ’ .

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.

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;
    (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.

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 receive the ‘ EU Stamp ’ marking.]

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.

12.1.2 Standards for WTMD

12.1.2.1 There shall be two standards for WTMD.

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.

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.

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.

12.2.4 The performance of HHMD shall not be affected by sources of interference.

12.2.5 HHMD shall have a visual indicator to show that the equipment is in operation.

12.3 *Omitted*

12.4 EXPLOSIVE DETECTION SYSTEMS (EDS) EQUIPMENT

12.4.1 General principles

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 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 material.

12.4.1.3 EDS shall give an alarm in each of the following circumstances:

- when it detects explosive material, and
- when it detects the presence of an item that prevents explosive material from being detected, and
- when the contents of a bag or consignment are too dense to be analysed.

12.4.2 Standards for EDS

12.4.2.1 All EDS installed before 1 September 2014 shall at least meet standard 2.

12.4.2.2 Standard 2 shall expire on 1 September 2021 .

12.4.2.3 The appropriate authority may permit standard 2 EDS installed between 1 January 2011 and 1 September 2014 to continue to be used until 1 September 2022 at the latest.

12.4.2.4 *Omitted*

12.4.2.5 All EDS installed as from 1 September 2014 shall meet standard 3.

12.4.2.6 All EDS shall meet standard 3 as from 1 September 2021 at the latest, unless point 12.4.2.3 applies.

12.4.2.7 All EDS equipment designed to screen cabin baggage shall meet at least standard C1.

12.4.2.8 All EDS equipment designed to screen cabin baggage containing portable computers and other large electrical items shall meet at least standard C2.

12.4.2.9 All EDS equipment designed to screen cabin baggage containing portable computers and other large electrical items and LAGS shall meet at least standard C3.

12.4.3 *Omitted*

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.

Where CTI TIP is deployed with EDS equipment used exclusively for hold baggage screening, the requirement in point (b) shall only apply as of 1 September 2020 .

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.

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.

12.6 EXPLOSIVE TRACE DETECTION (ETD) EQUIPMENT

12.6.1 ETD equipment shall be able to collect and analyse trace levels of particles or vapour from contaminated surfaces, or the contents of baggage or consignments, and indicate, by means of an alarm, the presence of explosives. 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.

There shall be standards for ETD set for particulate and vapour sampling.

12.6.2 The standard for ETD equipment that uses particulate sampling shall apply to ETD equipment deployed from 1 September 2014.

12.6.3 The appropriate authority may permit ETD equipment not certified to comply with attachment 12-L that was deployed before 1 July 2014 and uses particulate sampling to continue to be used until 1 July 2021 at the latest.

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.

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.

12.7.2 Standards for Liquid Explosive Detection Systems (LEDS) equipment

12.7.2.1 There shall be three standards for LEDS equipment.

12.7.3 *Omitted*

12.8 METHODS OF SCREENING USING NEW TECHNOLOGIES

12.8.1 The Minister with responsibility for Civil Aviation 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 *Omitted*

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.

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.

12.9 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.

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.

12.9.1.7 An EDD team shall be approved by or on behalf of the appropriate authority.

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 *Omitted*

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.

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.

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.

12.9.3.2 The content of training courses shall be specified or approved by the appropriate authority.

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.

Initial training for EDD Teams

12.9.3.7 An EDD team shall be subject to initial training.

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 *Omitted*

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.

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;

(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 *Omitted*

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.

12.9.6 *Omitted*

12.10 *Omitted*

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.

12.11.2 *Omitted*

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.

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.

12.12.2 Standards for SMD

12.12.2.1 There shall be two standards for SMD.

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 *Omitted*

12.13 AUTO CLEAR SOFTWARE (ACS)

12.13.1 General principles

12.13.1.1 Auto clear software (ACS) shall be able to assess all radioscopic images produced by x-ray or EDS equipment to ascertain if they may contain threat items and should be able to directly clear simple images without threat items.

12.13.1.2 ACS shall display to a screener those images that contain possible threat items or are too complex for the software to analyse.

12.13.1.3 ACS shall not impair the performance and normal functioning of x-ray and EDS equipment.

12.13.1.4 When ACS is running, a visual indication shall be given to the screener.

12.13.1.5 When used on EDS equipment ACS shall not prevent an alarm indication.

12.13.1.6 ACS shall not clear CTI and the radioscopic images produced by x-ray or EDS equipment containing FTI projected by TIP.

12.13.1.7 The means for managing the ACS shall be protected and accessible only to authorised persons.

12.13.2 *Omitted*

12.14 EXPLOSIVE VAPOUR DETECTION (EVD) EQUIPMENT

12.14.1 Standards for EVD

12.14.1.1 All EVD equipment used for the screening of hold baggage or cargo shall meet at least standard 1.

12.14.1.2 All EVD equipment used for the screening of persons or cabin baggage shall meet at least standard 3.

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.