Unrestricted

Full Supporting Guidance for AOSP / SSPs

1. The **requirement for Operators to develop a security programme started in 1974** with the first Annex 17, **but with the State of the Operator only** … "*operators of aircraft of its registry to adopt a security programme"* (Standard 6.1.1, 1974).

2. The **requirement** for Operators to develop security programmes **for all States of the Operators and States of the operations exists since 1986** (Amendment 6 to Annex 17).

3. IOSA requires Operators to develop Security Programme for all IOSA-registered airlines since the first edition of **IOSA Standards Manual (ISM) in 2003**. The requirements became the development of Air or Aircraft Operator Security Programme (**AOSP**) in all States where operations are conducted.

4. **The challenges for Operators with the development of AOSPs for both the States of the Operators and the States of the operations were the incremental administrative burden with duplication of documents and translations, maintenance, and accountability issues.**

5. **The challenge for regulators was the requirement to review and approve individual foreign airline's AOSPs without acknowledging or trusting the review/approval granted by the respective States of the Operators.**

6. In **2019**, the African Civil Aviation Commission (AFCAC) outlined the challenges States are facing with the implementation of the ICAO AOSP Standard (3.3.1) and "the inconsistency in its implementation, notably due to the challenges in meeting the approval obligation, which could be attributed to the interpretation". The AVSEC Panel approved the review of existing **Standard 3.3.1 for the State of the Operators**, and the introduction of a new **supplementary Standard for the States of the operations**,

7. In **2022, Amendment 18 to Annex 17** proposed two new standards, **Standard 3.3.1 for the State of the Operator, with the development of AOSPs meeting the requirements of the State of the Operator (like Standard 6.1.1 in Annex 17, 1974**) and **Standard 3.3.2 for foreign operators to develop "Supplementary Station Procedures" (SSPs) that meet the requirement of the States of the operations**.

8. Supplementary Procedures to the AOSP, as indicated in the **Impact Assessment of the ICAO State Letter** presenting Amendment 18 to Annex 17 to States in March 2022 (and corrigendum in April 2022).

9. Supplementary Procedures "*annexed to the AOSP, that meet any requirements of other States where operations are conducted that are not addressed in the AOSP"* (**ICAO AOSP/SSPs public guidance**)

10. **Operators should perform a gap analysis between their AOSP and the local requirements of the States of their operations, to assess the need for Supplementary procedures (in the form of SSPs) covering the local requirements that not already addressed on their AOSP**.

11. Unfortunately, in 2024, too many States and regulators have not fully read the Impact Assessments contained in the ICAO State Letter presenting Amendment 18 to Annex 17, nor the ICAO guidance material made available publicly and in the ICAO Aviation Security Manual (Doc 8973, Restricted).

12. Moreover, the USAP-CMA Protocol Questions related to Standards 3.3.1 (AOSP) and 3.3.2 (SSPs) remained misaligned with the Impact Assessments contained in the ICAO State Letter and the guidance provided by ICAO, since their latest revision in April 2025. Past confusion with the implementation by States should now be reduced, pending potential further clarification at the provisions level in the future.

Essential Implementation Considerations

For AOSPs:

1- AOSPs are required by Annex 17 since 1997 (and mandatory in ISM since 2003)
2- AOSP is established, implemented, and maintained by each Aircraft Operator
3- AOSP is developed in a written form and must meet the requirements of the national civil aviation security programme (NCASP) of the State of the Operator
4- States of the Operators (and the operations) shall share the appropriate parts of their NCASP and/or relevant information or guidelines with aircraft operators (both national and foreign) enabling them to meet the requirements of the NCASP (Annex 17, Standard 3.1.9, 2022)
5- AOSP should be approved, reviewed, verified by the State of the Operator and an acknowledgment provided to the Aircraft Operator (Doc 8973, para 15.2.5 and footnote containing the information to be provided in the acknowledgment)
6- In its Letter of Acknowledgement for AOSP, the State of the Operator should state they perform regular quality control and compliance functions over their registered Aircraft Operators for maintaining the strict relevance of the AOSPs with the national security requirements applicable.

For Supplementary [to AOSP] Station Procedures (SSPs):

7- When receiving the appropriate parts of the NCASP of the State of the operation (#4 above), the Aircraft Operator should **perform a gap analysis** between its AOSP and the local requirements with the view to assess the need to develop Supplementary Station Procedures (SSPs)
8- SSPs are supplementary to the AOSP and should only be issued when the requirements of the NCASP of the State of the operations are not already addressed in the AOSP (ICAO AOSP/SSPs public guidance)
9- When SSPs are required, Aircraft Operators should establish one single "national" set of SSPs per State of the operations. National SSPs templates, ICAO Doc 8973 Appendix 24 or the Operations Security Implementation Verification Checklist shared in the SeMS Toolkit for ESPs could be used as templates
10- SSPs should be approved, reviewed, verified by the States of the operations and acknowledgment provided to the aircraft operator (Doc 8973, para 15.2.7 and footnote containing the information to be provided in the acknowledgment).

For the specific security standards of the Operator (ISM SEC 1.2.1):

13. The security standards of the Operator mentioned in ISM SEC 1.2.1 should be either included in the main body, or as a separate appendix of the AOSP, or included in the SSPs (when the local environment is judged unsatisfactory by the Operator). In all cases, security standards of the Operator should be endorsed by the appropriate authorities of the State of the Operator (if in the AOSP) or the State of the operations (if in the SSPs).

Reference documents

ICAO State Letter presenting Amendment 18 to Annex 17 (17 March 2022)
Corrigendum of the Impact Assessment of the State Letter (19 April 2022)
ICAO AOSP/SSPs public guidance

SeMS Aviation Community (require access via aviationsecurity@iata.org)
IATA SeMS Toolkit for ESPs (For the Appendix 1 - Operations Security Implementation Verification Checklist)

IATA AOSP/SSPs webpage (via the IATA Aviation Security webpage)

Aircraft Operator Security Programme (AOSP) and Supplementary Station Procedures (SSPs)

This document is close, but different, to what regulators could read in the Appendix 24 of the ICAO Aviation Security Manual (Doc 8973, Restricted). The content of that document has been originally developed by the participants of the IATA AOSP/SSPs Workshop held in Singapore in June 2024, shared with ICAO for inclusion in Doc 8973, and finetuned by IATA for distribution. For any question, please contact aviationsecurity@iata.org.

GENERAL

1. For historical purposes, the international requirement for Operators to develop a Security Programme is present in ICAO Annex 17 since its first Edition in 1974, but it was limited to what is now called the Aircraft Operator Security Programme (AOSP) with the State of Registry (or State of the Operator). The extension to all States (of the Operators and of the operations) was introduced by ICAO in 1986. Finally, the separation between the AOSP for the State of the Operator and potential Supplementary Station Procedures (SSPs) for the States of the operations was introduced in 2022 (Amendment 18) with Standards 3.3.1 (AOSP) and 3.3.2 (SSPs).

2. Additionally, aircraft operators have also been required to develop a documented Air Operator Security Programme (AOSP) as part of the IATA Operational Safety Audit (IOSA) Standards Manual (ISM) for more than two decades. All IOSA registered airlines, and most airlines conducting commercial operations, must maintain an AOSP that documents all the relevant international provisions contained in Annex 17, and where applicable, the international guidance set forth in the ICAO Aviation Security Manual (Doc 8973, Restricted).

3. As of today, each aircraft operator shall establish, implement and maintain an appropriate written Aircraft Operator Security Programme (**AOSP**) that meets the requirements of the National Civil Aviation Security Program (NCASP) of the **State of the Operator**. Should there be requirements of a **State of the operations** not already captured in the AOSP, then Supplementary Station Procedures (**SSPs**) should be added that would address only the missing requirements. ICAO guidelines on AOSP and SSPs are publicly available.

4. AOSPs and SSPs should be clear and sufficiently comprehensive documents, free of legal terms or technical jargon, risk-based and operations-focused, and should be readily available to staff who are responsible for implementing security measures, including from External Service Providers (ESPs) when outsourced.

5. Once completed, the AOSP should be endorsed, signed and dated by the aircraft operator's accountable executive and submitted to the appropriate authority of the State of the Operator for review or verification, and when possible, approval. The State of the Operator should establish a means to confirm their approval, review or verification of the AOSP and provide such acknowledgment to the aircraft operator.

6. The AOSP should be reviewed and, if required, updated by the accountable executive at least once every 12 months. The AOSP, usually developed in the language of the State of the Operator, should also be provided in English for international audit and sharing purposes.

7. When differences between the appropriate parts of the respective NCASPs of the States concerned (State of the Operator and State of the operations, or two States of the operations different from the State of the Operator) are identified, those States shall engage in a consultation process as any differences in the security requirements contained in respective NCASPs could conduct in the formal request for "additional measures" by one of the States concerned in the context of Annex 17 Chapter 2.4 – *International Cooperation*, and more precisely Standards 2.4.1 and 2.4.2.

8. In this situation, the requesting State is required to demonstrate that appropriate consultation and consideration of alternative measures proposed by the State receiving the request has occurred, as per Annex 17 Chapter 2.4 – *International Cooperation*, and more precisely Standards 2.4.1 and 2.4.2. Additional measures may not always be implemented by the aircraft operators, but by airport operators, thus raising the question of their relevance in AOSP (and any need for SSPs) when States accept these additional measures.

9. Additional measures (or alternative measures) should normally be included (even when temporary) in the respective State's NCASPs depending on acceptance by both States concerned (State of the Operator and State of the operations). As these additional measures are designed to mitigate risks derived from new or emerging threats, or new mutually identified vulnerabilities, they should generate a review of the relevant elements of the NCASPs by the States concerned, as mentioned in Annex 17 Standard 3.1.3.

10. When **additional measures** (or alternative measures) **are accepted** by both States concerned, different situations could occur depending on which the States concerned are:

a. The State of the Operator and State of the operations, and the NCASP of the State of the Operator is adjusted. In this case, the additional measures should be included in the original AOSP. No need for SSPs.

b. The State of the Operator and State of the operations, but the NCASP of the State of the Operator is not adjusted accordingly. In this case, the additional measures should take the form of SSPs to be approved by the State of the operations.

c. Two States of the operations, different from the State of the Operator, meaning that the NCASP of the State of the Operator could not be adjusted. In this case, the additional measures should take the form of SSPs approved by the respective States of the operations.

11. When **additional measures are not mutually accepted** by both States concerned (State of the Operator and State of the operations, or two States of the operations different from the State of the Operator), those measures could then be called "**extraterritorial measures**" and should take the form of SSPs approved only by the requesting State. It should be noted that, in the context of Annex 17 Standard 3.5.3, the oversight of those extraterritorial measures outsourced to External Service Providers (ESPs) by the aircraft operators should be conducted based on the relevant elements (or appropriate parts) of the NCASP of the requesting State, and not automatically by the State where those measures are implemented.

12. When SSPs are required, they may be appended to the AOSP. They are usually developed in the languages of both the States of the Operator and the State of the operations and/or preferably in English (for international audit and sharing purposes).

13. When the Operator implements other security standards (as mentioned in ISM SEC 1.2.1), these measures should be either included in the main body, or as a separate appendix of the AOSP, or included in the SSPs. In all cases, security standards of the Operator should be endorsed by the appropriate authorities of the State of the Operator (if in the AOSP) or the State of the operations (if in the SSPs).

14. AOSPs, and SSPs should follow a security classification in accordance with respective national guidelines, meaning that SSPs could be appended separately from AOSP when the States of the operations (approving SSPs) do not want to share the specific local measures in place with the authorities of the State of the Operator (reviewing the AOSP). The situation could be more complex when additional or extraterritorial measures are required between two States of the operations that are not the State of the Operator.

15. The following sections present the key elements of an AOSP, and then a proposed checklist for SSPs when SSPs are required. AOSP key elements should not be repeated in the SSPs, when they are required, as SSPs are only necessary when the original AOSP does not cover both the appropriate parts of the respective NCASP of the State of the Operator and the States of the operations.

Aircraft Operator Security Programme (AOSP) Key Elements

The following AOSP key elements represent a framework for the development of new AOSPs for new aircraft operators, as well as an "international conformity reference" for aircraft operators willing to demonstrate alignment between their AOSP and recognized international guidance material. The relevant portions applicable to SSPs are listed after the AOSP key elements portion, as a separate SSPs checklist portion.

POLICY AND ORGANIZATION

16. An AOSP should be adopted as corporate policy and should describe the aircraft operator's policies and objectives with respect to security and call for the establishment of a security department and Head of Security whose responsibilities involve achieving the cited objectives. The programme should set out the related responsibilities of employees, external service providers, and other contractors. The security obligations described should be clearly defined and easily understood by those who need to implement them.

17. In developing an AOSP, the threats and risks facing the operator, and its operations should be assessed. State and facility security requirements, programme implementation timelines, staffing and financial limitations, and enhanced security requirements during times of increased threat, should also be considered. The applicability of the AOSP should also be appraised, since it may apply only to a particular airport or group of airports, a particular service or a specific State.

PRIMARY OBJECTIVE

18. The primary objective of an AOSP is to ensure the security of passengers, crew and the public by mitigating potential or actual acts of unlawful interference with civil aviation. To that end, AOSPs should:

a) meet or exceed the requirements of Annex 17 (as legislated domestically) and the NCASPs of those States in which the aircraft operator operates;

b) provide for standardized security measures and for clear security directives for crew, other employees, external service providers, and contracted staff;

c) provide for additional security measures in times of increased security threat; and

d) set performance standards, achievable through initial and recurrent training and monitored in accordance with recordkeeping requirements set out in the programme and/or the aircraft operator training programme.

LEGAL AUTHORITY

19. The appropriate authority of the State of the Operator should be empowered by national legislation to assign responsibility, through regulations, to its aircraft operators for the establishment, implementation, and upkeep of their AOSPs meeting the national requirements of the State of the Operator. The appropriate authorities of the other States, where operations are conducted, should be empowered to require foreign aircraft operators to establish, implement and maintain written Supplementary Station Procedures (SSPs) that meet the requirements of the NCASP of that State, when these local requirements are not already addressed in the AOSP.

DEFINITIONS

20. AOSPs should promote a common understanding of specific words and terms by presenting a set of definitions. Examples of terms that require an explanation include appropriate authority, NCASP, airport operator, aircraft operator, airport tenant, security restricted area, baggage, background check, catering stores and supplies, and regulated agent. The appropriate authority of the State of the Operator should provide a list of terms and acronyms it requires to be defined in the AOSP.

ROLES AND DUTIES

21. AOSPs should clearly indicate the duties, responsibilities and detailed contacts of all those involved with commercial air transport operation security, to help prevent any misunderstanding concerning the role of aircraft operators, including: their own security departments and accountable executive; crew members and other employees; airport authority management; In Flight Security Officers (IFSOs); law enforcement authority; national armed forces; government agencies; other aircraft operators, including code-sharing and alliance partners; postal authorities; regulated agents; known shippers and consignors; handling agents; and catering companies.

Accountable Executive and Security Manager

22. AOSP descriptions of an accountable executive and its security managers' duties and responsibilities should reflect the criteria shared in the ICAO AOSP/SSPs public guidance material.

Security department

23. AOSPs should provide a detailed description of aircraft operator's security department including, for example, the identity of sub-departments such as operations units, compliance and quality assurance roles, threat, risk and incident management functions, support and development sections, and investigations and crime prevention units, and a brief description of their responsibilities and authorities. A complete organizational chart, including the names and telephone numbers of the accountable executive and all security department directors, should be included in an appendix.

24. Security department principles should also be set out, and should include:

a) clear terms of reference based on the responsibilities of the accountable executive;

b) a clear order of command reflected in the structure of the department;

c) the appropriate relationship between the security department and line management. Although an aircraft operator's home base requires the bulk of security resources as many of its assets are located there, this should not be at the expense of the necessary support that should be given to line management at other locations; and

d) the security department's relationship with all other company departments.

Classification of materials

25. AOSPs should include a statement on the classification and secure handling of sensitive information. Materials may be classified under terms such as For Official Use Only or Restricted. Arrangements for protecting security-related sensitive information should also be explained and may involve limited distribution on a need-

to-know basis and the storage of materials in a secure location. Protection and distribution procedures should be developed for both paper-based and electronic documents.

Aircraft operator security programme distribution

26. As a restricted document, AOSPs (including its related SSPs) should be protected from unauthorized access. These documents should be available in part or in whole only to those with a need to know its contents. All entities and individuals provided with copies or portions of an AOSP (or SSPs) should be charged with protecting the information in their possession. A distribution list should be provided in an appendix.

Security document distribution

27. NCASPs often specify methods for distributing security documents and reports. Such information should also be indicated in the AOSP and any applicable SSPs, together with directives on how to distribute reports that may not be specified in a relevant NCASP, including reports on law enforcement actions or incidents, criminal records used in background checks, the results of internal inspections, and security directives or information circulars issued by the appropriate authority.

SECURITY OF AIRCRAFT

General

28. Basic responsibility for aircraft security rests with the aircraft operator, whose principal aim is to prevent unauthorized access. Since the first line of defence against such access is to safeguard the airside boundary, a responsibility generally designated to the airport authority, AOSPs and any SSPs should take Airport Security Programmes (ASP) into account, ensuring a coordinated effort and response. Where necessary, measures specific to an airport may be addressed in SSPs.

29. In most situations, several entities are responsible for the protection of aircraft, notably the airport, aircraft operator and law enforcement. This section of the AOSP should specifically describe each entity's role and responsibilities in this regard and should indicate the communications protocol between the aircraft operator and airport, to be followed in reporting suspicious activity, the status of out-of-service aircraft, and information concerning an increased threat. The protocol also applies to communications concerning extra security for more vulnerable flights and notification provisions for special category passengers.

Access control and flight crew compartment protection

30. AOSPs should describe measures for protecting aircraft on the ground and flight crew compartments both on the ground and in flight.

Preflight precautions

31. AOSPs should describe preflight precautions carried out on a regular basis, during high threat situations, or on request, and should cite the agencies involved and their respective tasks.

Threat notification

32. AOSPs should include procedures for responding to information that indicates that a specific aircraft may be the target of an attack. Programmes should indicate who is responsible for implementing the additional security measures considered necessary to counter a threat and should assign responsibility for informing the appropriate authority of the situation if threat notification originates with another source.

Flights under increased threat

33. AOSPs should highlight the procedures to be followed for specific flights facing a higher level of threat, including the use of isolated aircraft parking positions, arrangements for guarding individual aircraft, deployment of an escort during taxiing, and inspection of the areas underlying approach and take-off paths. A parking area plan should be appended.

Aircraft searches and checks

34. AOSPs should spell out the procedures for searching and checking aircraft during routine operations and periods of increased threat and identify the agencies or External Service Providers (ESPs) responsible for conducting a search, as well as the necessity for using proper checklists, adequate lighting, and properly trained personnel supported by air crew or aircraft engineering support staff. Actions to be taken on discovery of suspect explosive devices should be described, and the entity responsible for making decisions about moving or evacuating aircraft and suspending airport operations should be indicated.

TRAVEL DOCUMENTS

35. AOSPs should detail the check-in process, including special measures or facilities for groups or high-risk passengers, and should indicate procedures for protecting tickets, boarding passes, baggage tags and other documents (if in paper form and containing flight sensitive or passenger information). Programmes should also describe procedures for preventing e-ticket fraud and electronic information theft.

36. AOSPs should indicate where, when and how identification and travel documents are checked with respect to originating, transfer and transit passengers. Where applicable, mention should be made of the authority and responsibility of handling agents under the provisions of an NCASP.

37. Programmes should also describe procedures for off-airport or curbside check-in of hold baggage, where applicable.

PASSENGER AND CABIN BAGGAGE SCREENING

38. AOSPs should provide details regarding the operator's, or another entity's, responsibility for performing passenger and cabin baggage screening, provided the operator is responsible for the overall implementation and oversight of its outsourced security measures. Screening duties are performed by an appropriate party appointed by the State concerned, which may be any of the following entities:

a) airport authority;

b) a company contracted by the State or airport;

c) national aircraft operator;

d) national law enforcement agency; or

e) national armed forces.

39. The legal authority for applying security measures should be cited, and any local laws and procedures that apply in the event that a person refuses to comply with security measures or is denied boarding for any reason should be described.

40. The section on passenger and cabin baggage screening should include, at a minimum, the following elements provided the aircraft operator is responsible for their implementation:

a) a description of the passenger risk assessments, which may include questioning of passengers at the time of check-in at the airport, passengers' statement when checking-in online, and/or any interview techniques carried out at the airport;

b) purpose of screening and searching passengers and their cabin baggage;

b) procedures and standards for screening and manual searches of all departing and transfer passengers and cabin baggage, including details of the service provider;

d) procedures for handling suspect passengers or cabin baggage;

e) measures for the control of passenger flow;

f) measures for special category passengers;

g) measures for screening and manual searches of aircraft crew and cabin baggage;

h) policy on unruly passengers, including procedures for on the ground and in the air, and the use of restraints as a last resort, as well as reporting requirements;

i) policy on stowaways, including preventive measures and actions to be taken if a stowaway is found;

j) procedures to be followed if a person refuses to be manually searched;

k) procedures to be followed upon discovery of restricted or prohibited articles;

l) procedures for handling confiscated items, including related recordkeeping if the aircraft operator is involved in the screening process;

m) procedures to follow on discovery of undeclared dangerous goods; and

n) measures for electronic and electrical items.

Separation of screened and unscreened passengers

41. AOSPs should include a description of how screened and unscreened passengers are to be kept separate and should indicate who is responsible for ensuring such separation and the steps that should be taken if screened and unscreened passengers intermingle.

Control of firearms, weapons and ammunition

42. AOSPs should also specify the procedure for handling and transporting authorized firearms and ammunition in hold baggage or as cargo in compliance with NCASP provisions. This information should elaborate on the role of the aircraft operator and crew, and any special arrangements to be made during check-in or baggage claim.

43. National policy on the authorized carriage of firearms and ammunition in the cabin of both national and foreign aircraft should be mentioned, as well as measures in place for implementing this policy. The tasks of agencies involved, and actions expected of aircraft operators should be explained. Authority for the carriage of weapons by IFSOs and escorts for prisoners, deportees or very important persons should be described, as well as the related procedures, including the requirement to notify the aircraft operator and PIC of the presence of an armed IFSO or escort.

44. AOSPs should indicate the procedures to follow if a weapon is found during the screening of passengers, baggage or cargo, and the procedures for transporting a firearm, ammunition or weapon in the cabin or in hold baggage.

Diplomatic pouches and government couriers

45. AOSPs should explain the security control procedures that apply to diplomatic pouches and government couriers including, where applicable, specific measures for diplomatic mail in official pouches and embassy correspondence not contained in diplomatic baggage. This subject may be addressed within the special category passenger section of State of the Operator AOSPs.

Special category passengers

46. AOSPs should set out procedures for special category passengers, including those with diplomatic status, government couriers with diplomatic baggage, IFSOs, potentially disruptive persons such as deportees, passengers whose religious beliefs preclude manual searches, and those with reduced mobility such as pregnant or disabled persons. Tasks of agencies involved should be listed, and reference made to notification requirements.

HOLD BAGGAGE SECURITY

47. Each State authorizes an appropriate entity to perform hold baggage security controls. This responsibility may be delegated to either the airport authority or a third party. However, the responsibility for maintaining the security of hold baggage being transported to an aircraft rests with the aircraft operator and its External Service Providers (ESPs).

48. AOSPs should specify the legal basis for hold baggage security measures, and the procedures to follow if a person refuses to allow their hold baggage to undergo security measures.

49. Reference should be made to the appropriate Airport Security Programme (ASP) provisions on hold baggage screening and relevant local security measures. At a minimum, AOSPs should include the purpose of security measures for hold baggage, and where applicable the procedures for:

a) a description of the passenger risk assessments, which may include questioning of passengers at the time of check-in at the airport, passengers' statement when checking-in online, and/or any interview techniques carried out at the airport;

b) originating and transfer hold baggage screening and manual searches, including details

concerning the screening locations and applicable standards, search location and applicable standards, screening equipment and the operator and service provider;

c) protection of hold baggage;

d) screening and protection of hold baggage that has been checked in at curbside or an off-airport site;

e) carriage of firearms and weapons, including the applicable legal provisions and regulations, acceptance process and preflight protection;

f) handling suspect baggage; and

g) handling unaccompanied baggage that is inadvertently separated from its owner.

PASSENGER AND CREW BAGGAGE OPERATIONAL RECONCILIATION

50. AOSPs should include a description of passenger and crew baggage operational reconciliation procedures, with specific reference to the various categories of passengers and crew, whether originating, online and interline transfer, or disembarking transit. The role of automation should also be covered. Guidance on passenger and baggage operational reconciliation measures can be found on the IATA public webpages, in particular the Hold Baggage (HB) Security Procedures.

51. Descriptions of passenger and crew baggage operational reconciliation procedures should include the following elements:

a) the purpose of passenger and crew baggage operational reconciliation measures and any exceptions;

b) procedures for passenger and crew baggage operational reconciliation, including equipment details if an automated system is utilized, baggage manifest details, if relevant, and procedures for the identification of no-show and re-identification of unaccompanied baggage; and

c) procedures for confirming that appropriate screening has been performed on hold baggage becoming unaccompanied, including the applicable standards, screening locations, equipment details, and information concerning the Operator and service provider.

Mishandled baggage

52. AOSPs should also include a description of the procedures in place for safeguarding mishandled, unidentified and unclaimed baggage.

AIRCRAFT CATERING STORES AND SUPPLIES

53. AOSPs should cite the legal requirement for applying security measures to aircraft catering stores and supplies, and the entity that is responsible for ensuring compliance.

54. Catering operations may either be owned by aircraft operators or function as independent contracted companies that provide catering services for several aircraft operators. In either case, aircraft operators usually

assume responsibility for catering security or its oversight and, therefore, this subject should be adequately covered in AOSPs.

55. Catering contractors should have a written security programme that meets the requirements of AOSPs and is available for inspection by aircraft operator security personnel. Employees and visitors to catering company facilities should comply with the programme's provisions.

56. Catering security sections should include the following key elements:

a) purpose of security measures for aircraft catering stores and supplies;

b) description of security measures at the aircraft operator catering unit;

c) description of the security measures that apply to the dispatch and ground transport of catering stores and supplies, including the standard in effect for controlled access to prepared meals, in-company stores and delivery vehicles; and

d) cabin crew procedures for receiving catering items at aircraft.

57. Other subjects related to the security of catering that may be covered in AOSPs include:

a) known and unknown stores;

b) physical security measures;

c) customs bonded warehouses;

d) tamper-evident sealed goods;

e) catering carts and containers;

f) delivery of multiple loads;

g) airside catering operations; and

h) the receipt and validation of consignments entering security restricted areas.

In-company stores

58. Office supplies, marketing literature, stationery, aircraft operator uniforms, engineering stores, aircraft-on-ground parts, and company mail, are among items carried on aircraft for regular delivery to route stations, which normally constitute in-company stores, but may include supplies destined for other aircraft operators.

59. Specific security responsibilities should be assigned to staff whose duties include the handling and loading of aircraft operator stores and supplies, and descriptions of these responsibilities should be included in AOSPs.

AIRCRAFT CLEANING OPERATIONS

60. AOSPs should explain the purpose of security measures pertaining to aircraft cabin cleaning operations and should provide a description of such measures.

CARGO AND MAIL

61. AOSPs should indicate who is responsible for cargo and mail security, including screening operations. The legal authority for imposing such security measures should be specifically cited. Security measures may vary depending on whether the operator specializes in passenger transportation, all-cargo or express courier operations.

62. Outstation operations may be handled by agents, contractors or External Service Providers (ESPs). Despite such arrangements, the aircraft operator remains responsible for the security of its cargo and mail operations whenever it has been given this responsibility by the host State. Guidance on security measures for cargo and mail may be found in IATA webpages and documents.

63. AOSP sections on cargo and mail security should include the purpose of security measures for cargo and mail, including courier and express parcels, and descriptions of the following elements:

a) security measures for cargo, including procedures for accepting a cargo consignment; procedures for transporting company material; regulated agent scheme (or equivalent) and criteria; known consignor scheme (or equivalent) and criteria; unknown shippers; standard and location of screening and physical examination; details of the operator or service provider; and list of exemptions from security screening or physical examination;

b) security measures for courier and express parcels, including procedures for accepting parcels; regulated agent scheme and criteria; standard of screening and manual searches; and details of the operator or service provider; and

c) security measures for mail, including procedures for accepting mail; procedures for transporting company mail; regulated postal authority (Designated Operator) and administration scheme and criteria; known consignor scheme and criteria; standard of screening; details of the operator; and procedures to be followed in periods of increased threat.

64. In developing the section on cargo and mail security, consideration should be given to the following aspects: types of cargo and mail to be subject to screening; protection of secure cargo, routine testing and maintenance procedures, including steps to follow when equipment fails or becomes unserviceable; handling and screening of suspect items; screening of oversized articles; and nature of consolidated consignments.

Regulated agent programme

65. States are obligated under Annex 17 to ensure that regulated agents conduct secure operations. This may be achieved through provisions in AOSPs and regulated agent security programmes.

66. AOSPs should indicate whether there is a regulated agent programme for cargo, and who is responsible for certifying regulated agents. If there is no regulated agent programme, programmes should indicate how cargo is processed and how security measures are applied.

67. In the context of a regulated agent security programme, the definition of cargo includes unaccompanied baggage, mail and courier and/or express parcels.

Known shippers and/or consignors

68. AOSPs should describe the procedures in place for cargo and mail that is not screened, such as the requirement for an operator to verify known shipper security certification. Known shippers and consignors may also fall within the purview of a regulated agent programme.

Unknown shippers

69. Shippers unknown to the regulated agent and/or aircraft operator should be subject to increased scrutiny, including a requirement to provide proof of identity and agreement to have a consignment screened according to a prescribed method, all of which should be described in AOSPs. Furthermore, aircraft operators should establish procedures for applying security controls to unknown cargo so that all consignments become known cargo before they are allowed on an aircraft.

Transhipments

70. If aircraft operators are responsible for the security of transshipped cargo, that is, cargo to be transferred from one flight to another, related security measures such as screening arrangements and protection from tampering during storage should be detailed in AOSPs. A summary of the measures may be provided if another party is responsible for their application.

High-value cargo

71. Security measures for handling and protecting high value cargo when stored in cargo terminals and during aircraft loading and unloading, as well as during ground transport, should be enumerated.

Unaccompanied baggage and/or personal effects shipped as Cargo

72. AOSPs should include security measures for unaccompanied baggage that is shipped as cargo, should describe the standard of screening and manual searches, which are usually the same as for an unknown shipper, and should provide details of the screening equipment and the operator or service provider.

Diplomatic mail

73. Security procedures for diplomatic mail carriage should be included.

Protection of cargo and mail

74. AOSPs should indicate the measures in place for protecting cargo and mail. If the security of the cargo facility is the responsibility of aircraft operators, information concerning the facility's security procedures should be provided, including details concerning the deployment of guards, and the use of patrols and CCTV systems. If surveillance cameras are installed, AOSPs should indicate whether they are separate from or integrated with the airport CCTV system. Information on building security should, among other elements, indicate whether a restricted area has been delineated and whether staff are screened, as well as noting how cargo and mail is transported to aircraft. If the cargo facility is located within a Security Restricted Area (SRA), the AOSP should detail the relevant access control measures.

AIRCRAFT MAINTENANCE AREAS

75. 7Security measures in place for aircraft maintenance areas should be indicated whenever aircraft operators are responsible for such measures, for instance if such areas are leased to an operator. At a minimum, a description of the maintenance area boundaries and controlled access procedures should be indicated.

CODE SHARING, WET AND DRY LEASE

76. Clear lines of accountability are essential for implementing and subsequently monitoring aviation security measures for flights conducted under code sharing, wet and dry lease agreements. Although compliant with Annex 17, different arrangements may exist in the States of Registration (or Registry) of code share partners, and such differences should be resolved.

77. The State of Registration (or Registry) determines the security arrangements to be adopted by an aircraft operator under its sovereign control. Any additional security measures or different applications called for by the code-sharing partner, or in case of wet and dry lease, will need to be addressed by the operators concerned, and appended to the AOSP.

78. Code-sharing, wet and dry lease partners should have a clear line of communication regarding such matters as risk and threat assessments. Specifics about the method of communication, contact details, and so on, should be in the relevant appendix, e.g. a code-sharing operator should advise its partner any time there is a security breach or details of a heightened threat to its operation which call for additional security arrangements. The State of Registration of each code-sharing partner should also be informed of the specific threat and the additional measures proposed to counter it.

TRAINING

Security awareness training

79. All staff should undergo security awareness training. Training aspects that should be noted in an AOSP include the categories of training, designation of those responsible for providing training, methods employed, such as video, classroom discussion, pamphlet, specific topics, the requirement to maintain training records and provisions for recurrent training.

Security training

80. AOSPs should call for all frontline personnel, such as check-in agents, screening staff and cabin crew, to undergo specialized training. Details of such training should be provided, including the topics covered and the number of hours. AOSPs should also address which job positions require certification, licensing, or authorization, with the approval of the appropriate authority or another relevant authority.

Recruitment and background checks

81. Information on aircraft operator recruitment methods, including the use of background checks, should be provided in AOSPs. Guidance can be found in Chapter 8. This section should state, for example, whether any laws preclude a criminal history check and what sort of information should be provided by the job applicant.

82. Details should also be provided about the process involved in handling a job application submission, including the identity of the department responsible for processing applications, as well as background checks, if applicable, and the policy on contacting former employers or character references for verification of information, among other items.

83. Procedures to be conducted after completing a background check should also be spelled out, including whether there is a requirement for records of applications to be kept on file and, if so, by whom and for how long.

Security training programmes

84. If the development, implementation and upkeep of aircraft operator security training programmes are required by the appropriate authority, a copy of the training programme should be appended to AOSPs. The foregoing descriptions may then be shortened, and references made to the training programme, where appropriate.

CONTINGENCY PLANS

85. It is appropriate to publish aircraft operator contingency plans as stand-alone documents, cross-referenced with AOSPs for auditing purposes, or as an appendix to AOSPs.

INCIDENT REPORTING

86. AOSPs should incorporate a description of aircraft operator security incident reporting procedures, following IATA guidance and Incident Reporting systems, and the public ICAO guidance on Incident Reporting and Taxonomy (https://www.icao.int/aviation-security-policy-section/Incident-Reporting-Guidance-and-Taxonomy).

QUALITY CONTROL

87. Aircraft operators may be required by an NCASP or other regulations to develop, implement and maintain specific quality control functions for their security operations that are not already included in their Security Management System (SeMS). In this case, a summary of the specific quality control measures should be included in AOSPs, with the quality control programme appended. If a State does not require a quality control programme, related measures should be comprehensively addressed in AOSPs as part of the operator SeMS. Alternatively, aircraft operators may produce a separate quality control programme and cross-reference this with the AOSP.

LOCAL AIRPORT PROCEDURES

88. Local airport responsibilities regarding the security of aircraft operations that have not already been addressed in the AOSP should be covered in the Supplementary Station Procedures (SSPs) relevant for that State of the operations. Proposed SSPs checklist is following.

Supplementary Station Procedures (SSPs) Checklist

As indicated in the previous sections, SSPs should only be required when the AOSP of the State of Operator is not meeting the requirements of the State of the operations as indicated in the Impact Assessment of the ICAO State Letter presenting Amendment 18 to Annex 17 in March (and April for its corrigendum) 2022, as well as in the ICAO public guidance on AOSP and SSPs. In lieu of requesting SSPs, States of the operations may rely upon a foreign AOSP approved, endorsed, reviewed or acknowledged by the State of the Operator or accept the formal acknowledgement[1] that the AOSP has been approved, reviewed or verified by the State of the Operator in directly requesting it from that State.

89. To assist in the mutual recognition process, aircraft operators should share (as part of compliance with IOSA ISM SEC 1.2.1) a "Letter of Confirmation" or "Letter of Endorsement" stating that the AOSP presented by an aircraft operator has been developed with sufficient details to meet the appropriate parts of the NCASP shared by their State of the Operator, and following the relevant ICAO guidance (public and in Doc 8973).

90. Before international operations are conducted, the States of the operations should share with foreign aircraft operators, and in advance of the operations, the appropriate parts of their NCASP and/or relevant information or guidelines to enable those aircraft operators to meet the national requirements (Annex 17 Standard 3.1.9). Those States should also share, in a practical and timely manner, any relevant information that could impact the risk assessments relating to an aircraft operators' operations (Annex 17 Standard 3.1.5).

91. When receiving the appropriate parts of the NCASP of the State of the operation, the aircraft operator should **perform a gap analysis** between its AOSP and the local requirements with the view to assess the need to develop Supplementary Station Procedures (SSPs). As previously indicated, SSPs are, by nature, supplementary to the AOSP and should only be issued when the requirements of the NCASP of the State of the operations are not already addressed in the AOSP.

92. When SSPs are required, aircraft operators should make full use of national SSPs templates, ICAO Doc 8973 Appendix 24, or the Operations Security Implementation Verification Checklist shared in the SeMS Toolkit for ESPs could be used as templates

93. SSPs should be approved, reviewed, verified by the States of the operations and acknowledgment provided to the aircraft operator (Doc 8973, para 15.2.7 and footnote containing the information to be provided in the acknowledgment).

94. SSPs could also be required when additional operational details are felt necessary by the State of operations. SSPs should be risk-based and only adding useful security information not covered by information given in the AOSP.

95. The States of the operations requiring SSPs are responsible to ensure those SSPs, developed in addition to AOSPs, meet the specific additional requirements of their NCASP. To achieve this, States, under their national legislation and/or policy, may consider the need to formally approve the SSPs and/or subject it to appropriate review or verification processes based on established procedures. States of the operations should ensure that the aircraft operators are aware of their policy and applicable processes, and should establish a means to confirm their approval, review or verification of the SSPs and provide such acknowledgement to the aircraft operator as a proof that the international requirement (in Annex 17 Standard 3.3.2) is met.

---

[1] States should consider including the following information when providing acknowledgment: aircraft operator accountable manager, reference # AOSP (or SSPs) presented, date of approval of AOSP by the operator, accountable official from the State of the Operator (AOSP) or operations (SSPs), Station and State (SSPs), reference of the NCASP used for compliance, confirmation that national requirements are met.

96. SSPs should be tailored for each airport/station where operations are conducted, and only include regulatory or procedural-related security and operational information.

97. In the cases where an aircraft operator operates to multiple locations within a State and the procedures are identical at each location, it should be possible to submit a single "national" SSPs to cover all locations. SSPs could also be comprised of a "national component" applicable to all stations within the same State, and local specific SSPs that could be used as Standardized Operating Procedures (SOPs) for the different External Service Providers (ESPs) implementing the security measures outsourced by aircraft operators at each airport/station.

98. SSPs are usually developed in the languages of both the States of the Operator and the State of the operations (to be used by External Service Providers on the ground), and in English (for international purposes).

99. The State of the operations may propose a template to assist the aircraft operator to complete SSPs. In these cases, it should not be expected that the aircraft operator will repeat sections from their AOSP but rather reference them in the SSPs if applicable. This increases efficiency and contributes to the transparency of aviation security measures accepted by States.

100. A holistic checklist of the measures usually covered by SSPs is displayed in the following table SSPs:

1) Passenger, Staff and Crew screening a) Originating passengers and crew b) Transfer passengers and crew c) Protection of passengers d) Behaviour detection e) Screening of ground staff	7) Aircraft Security a) Protection b) Security checks and searches c) Security patrols d) Access control within the SRA e) Transit stop procedures
2) Check in and boarding for: a) Passenger b) Crew	8) In-Flight Security Officers and Special Category Passengers
3) Hold Baggage (HB) Screening a) Screening methods b) HB protection c) Procedures for mishandled HB	9) Control of firearms and weapons
4) Authorizing and Accounting for Hold Baggage	10) Local Staff training
5) Physical Security Measures and Access Controls to airside and security restricted areas (SRAs)	11) Occurrence and Incident Reporting by External Service Providers (ESPs) staff
6) Security Measures for: a) Cargo facilities b) Cargo and Mail c) Catering in in-flight supplies d) COMAT and COMAIL e) Other supplies protection	12) Quality Control measures performed by ESPs 13) Additional Security Measures 14) Contingency and Emergencies 15) Cybersecurity

[*table SSPs – example of commonly used SSPs checklist*]

--- END ---