Council of the European Union

Brussels, 7 February 2023
(OR. en)

6124/23

AVIATION 22
IXIM 19
RECH 39

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	2 February 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2023) 37 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Working towards an enhanced and more resilient aviation security policy: a stocktaking

Delegations will find attached document SWD(2023) 37 final.

Encl.: SWD(2023) 37 final

EUROPEAN
COMMISSION

Brussels, 2.2.2023
SWD(2023) 37 final

COMMISSION STAFF WORKING DOCUMENT

Working towards an enhanced and more resilient aviation security policy: a stocktaking

Contents

EXECUTIVE SUMMARY

In line with the general objective to create a more resilient Single European Transport Area[1], this Commission staff working document brings together the content and conclusions of a series of consultations between the Commission services, Member States and stakeholders[2] over a two-year period, with a view to taking stock of the existing EU aviation security framework and identifying potential areas of improvement. Since aviation security issues have the potential to impact the experience of passengers and cargo users alike, this document addresses an audience beyond the aviation security community.

This process was triggered at the 96th meeting[3] of the EU's Aviation Security (AVSEC) Regulatory Committee[4], where some members recommended that a comprehensive review of the EU regulatory landscape for aviation security was needed. In its 103rd meeting[5], the AVSEC Regulatory Committee established a dedicated working group to carry out this task. Some 10 meetings took place where Member States and stakeholders were consulted on the EU aviation security policy, based on 5 workstreams corresponding to the main features of the aviation security ecosystem, such as threat and innovation.

In this process, a number of possible improvements to the EU security system were identified by the working group falling under the following categories: (i) the rule-making process; (ii) innovation in the sector; and (iii) the threat picture update.

This document reports on this stocktaking exercise and presents the improvements identified by the working group and stakeholders during this consultation process with a view to engaging further with Member States and stakeholders in defining a way forward towards an enhanced EU aviation security framework that is more resilient, innovative, and fit for the future.

The EU aviation security system: two decades of accomplishments

For the last 20 years, terrorists have engaged in systematic attempts to circumvent aviation security measures, always using increasingly sophisticated modus operandi. Faced with an ever-changing picture of the threat to civil aviation, including in the cyber domain, the regulatory structure of the EU aviation security system has been conceived to give an adequate, collaborative and harmonised answer to all forms of evolving threats.

During the consultation process, Member States and stakeholders have concluded that the EU aviation security system has proven its effectiveness in tackling current as well as future aviation security challenges. The success of the existing aviation security

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Sustainable and Smart Mobility Strategy – putting European transport on track for the future, COM(2020) 789 final, 9 December 2020. Chapter 4, in particular Paragraph 102.

[2] A number of members of the Stakeholder Advisory Group on Aviation Security (SAGAS), constituted under Article 17 of Regulation (EC) N°300/2008, volunteered to participate to the consultation process. The list of SAGAS members is presented in annex to this document.

[3] 14-15 March 2018

[4] Article 19 "Committee procedure" of Regulation (EC) N°300/2008 provides that the Commission shall be assisted by a Committee of EU Member States.

[5] 27 November 2019

framework in the EU has been reinforced by the well-established cooperation between the European Commission, Member States, observers and stakeholders, within the Aviation Security Regulatory Committee and the Aviation Security Stakeholder Advisory Group.

However, the security landscape is dynamic and the consultation has also revealed that in order to maintain aviation security at the highest level, the EU aviation security system would need to: (i) modernise its regulatory architecture; (ii) take measures to support the development and uptake of innovative solutions; and (iii) better tackle new types of threat.

Under all these avenues, maintaining and promoting the principle of intra-EU one-stop-security (OSS)[6] scheme is a shared objective.

Towards a more agile, flexible but also stable regulatory system

A common view expressed during the consultation process is that the EU aviation security system benefits from a comprehensive set of rules, that are neither difficult to understand nor arduous to implement. However, in response to new threats and technological developments, the corresponding and necessary regulatory adjustments have given rise to a rather complex body of rules that could lead to discrepancies in implementation. Moreover, some expressed views that constantly updated prescriptive security measures may not always be the most efficient and effective way to tackle ever-changing security threats.

To address these issues, Member States and stakeholders alike would support an optimal aviation security regulatory system that combines innovation and stability features, maintains the highest level of security at all times, and is composed of the following elements:

- an agile decision-making framework that would allow solutions to new threats to be rapidly incorporated, but also allow emerging innovative technical solutions to be used in a timely manner;
- a calendar for global reviews; and
- where appropriate, a tailor-made approach through local risk assessments based on robust, common methodology.

In this respect, a number of targeted modifications have been suggested within the existing EU legislative framework. The frequency of small regulatory amendments would be reduced and limited to the minimum necessary (e.g. transposing new International Civil Aviation Organization (ICAO) standards, adapting to changes to the threat picture or in technology). In parallel, every 5 years or so, a more thorough analysis would be carried out to review the whole set of common rules. Furthermore, additional sets of guidelines agreed between the Commission services, Member States and operators would enable Member States and operators to continuously improve implementation of the common rules.

[6] The application of the 'One-Stop-Security' concept means that passengers and their baggage departing from European airports and transferring through other European airports do not need to be rescreened.

A more ambitious security R&D development and implementation policy

Although it stems from the consultation that the EU aviation security system has so far allowed innovation to thrive, members of the working group have identified three pressing challenges that should be addressed so that the EU can maintain the highest level of security.

First, developing detection standards requires consistency and predictability. A proper regulatory environment, as well as a testing environment, are key enablers to triggering research and development on new detection standards. Clear, stable and publicly available implementation calendars should be created when adopting the relevant detection requirements and security control measures updates. One workstream could be the creation of 'standardised' processes to develop new detection standards. For instance, new detection standards would include:

- clear (and stable) implementation dates that would give certainty to the aviation industry;
- clear concepts of operations describing how to use the technology and, if needed, with clear limitations;
- dates for phasing out of old technology;
- incentives to accelerate the implementation.

Collaborating with key international partners could also enable common standards to be developed with fewer resources and more quickly. This could be particularly relevant pursue with like-minded non-EU countries.

Second, the financing of EU aviation security R&D could be improved. As a solution, the Commission services would increase Member State and stakeholder involvement in implementing Horizon Europe R&D programmes and seek to improve the way funding is mobilised to help improve the European testing capacity, in particular extending it to new technologies.

Third, consultations stressed the importance of preventing the gap between EU Member States and EU airports themselves from widening when it comes to implementing the innovative solutions. While in the recent past new aviation security technologies (e.g. security scanners, explosive detection system for cabin bags) have been successfully rolled out, the aviation security baseline established under EU's common rules has not yet been revised to reflect recent threats. Therefore, discrepancies have increased between airports that implement the newest technologies on time versus other airports that still rely on older technologies.

Towards a new, better targeted baseline

The working group recommends that the Commission services together with Member States and stakeholders develop a new EU future-proof baseline that would i) fully exploit the potential of new technologies, ii) adapt to threats that have become a priority to address, and iii) adapt to global changes and be in line with international partners' expectations.

After such a target baseline has been conceived, acceptable alternative transitory models could be developed, and an implementation timeline could be decided upon to enable

civil aviation operators to align with this new baseline in a phased and progressive transition. In this context, maintaining the OSS scheme's integrity would be a priority. It is proposed that scenarios would be created, with Member States and stakeholders, which would minimise the impacts, both for operators and passengers, of reconnecting small airports to the largest hubs.

1. INTRODUCTION

1.1. Security as a priority for the aviation sector

1. Safeguarding international civil aviation against acts of unlawful interference that affect the whole air transport industry is a key aim of regulators at international, European and national level. Ensuring secure aviation operations in the air and on the ground at all times is a fundamental condition for commercial aviation to flourish.

2. Aviation security (AVSEC) involves a combination of measures and controls that are meant to prevent a wide spectrum of unlawful interventions. These include[7]: i) unlawful seizure of an aircraft, ii) the destruction of an aircraft in service, iii) the use of an aircraft to with the purpose of causing deaths, iv) hostage-taking on board or at aerodromes, v) forcible intrusion on board an aircraft or at an airport, vi) brandishing a weapon or bringing hazardous material or a device intended for criminal purposes on board an aircraft or at an airport, and vii) communication of false information to jeopardise the safety of an aircraft. In the context of aviation's growing reliance on information technology and digital operational systems, cybersecurity is becoming ever more critical.

3. Besides the direct and immeasurable impacts on victims and their families, the economic cost of breaches in aviation security can be significant. Since 2004, terrorism, not limited to civil aviation targets, has cost the EU an estimated EUR 5.6 billion in lost lives, injuries and damage to infrastructure and property as well as an estimated loss of EUR 185 billion in GDP[8]. Although rare, major breaches in aviation security can have serious impacts. In addition to the 2 977 people killed and more than 6 000 injured, globally, the September 11 attack in 2001 had a major impact on the aviation industry as well as on the economy as a whole. In New York alone, around 430 000 jobs were lost over the 3 months following the attack[9]. Because of its potential impacts, security risks to civil aviation must be addressed in all its components, at all times.

4. To ensure an aviation security system that meets today's challenges, regulators and stakeholders alike seek to meet three requirements. First, protecting civil aviation against unlawful acts. Second, maximising a positive passenger travel experience whenever possible. Third, allowing aviation security operations to remain financially sustainable for an industry that faces important obligations in terms of green and digital transition.

5. Annex 17 to the Chicago Convention on International Civil Aviation lays down the minimum standards and recommended practices that contracting states must implement to protect civil aviation from acts of unlawful interference. At EU level, to boost civil aviation security, regulators provide the basis for a common interpretation of this Annex. In 2002, the EU Parliament and Council established the first common rules on civil

[7] ICAO, Annex 17 to the Chicago Convention on International Civil Aviation.
[8] The fight against terrorism - Cost of Non-Europe. EPRS | European Parliamentary Research - European Added Value Unit - PE 621.817 - May 2018.
[9] Dolfman, Michael L., Solidelle F. Wasser (2004). '9/11 and the New York City Economy'. Monthly Labor Review.

aviation security[10], which were superseded in 2008 by the current regulatory framework under Regulation (EC) N° 300/2008[11].

6. Under this framework, with the active support of Member States and stakeholders, the Commission's role is to determine, ensure adoption of and monitor[12] the implementation of a comprehensive set of common aviation security measures. Ensuring this coordinated EU approach through common rules was crucial in allowing the OSS concept to be established, whereby there is no need to rescreen passengers and their baggage departing from European airports and transferring through other European airports[13].

1.2. A mandate for change

7. During the 96th meeting of the AVSEC Regulatory Committee, a group of Member States[14] called for a stocktaking process to be launched and for a strategic discussion on possible next steps for the EU aviation security system. At its 103rd meeting, the AVSEC Regulatory Committee established a dedicated working group to carry out a comprehensive review of the EU regulatory landscape for aviation security.

8. Furthermore, in order to address the growing challenges related to the digitalisation of key economic sectors, in December 2020 the Commission adopted a proposal aiming to update and enhance the EU's main horizontal framework on cybersecurity, the Directive on security of network and information systems. The NIS2 Directive[15], which was formally adopted by the co-legislators in November 2022 and enters into force on 16th January 2023, sets out the baseline for cybersecurity risk-management measures and incident reporting obligations across various sectors falling within its scope, including the air transport. It also foresees the possibility for the Commission to issue implementing acts laying down more granular and sector-specific cybersecurity risk-management measures for the sectors included in its Annex I and II, including in relation to entities in the air transport subsector such as air carriers, airport managing bodies, airports and traffic management control operators.

1.3. Methodology

9. While a large part of the EU common rules on aviation security are laid down in Commission implementing regulations[16], which are publicly available, unrestricted access to other detailed measures would damage their efficacy, e.g. detection abilities of aviation security equipment operated at EU airports or the way alarms in security screenings are handled. Therefore, these measures benefit from either restricted or

[10] Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (OJ L 355, 30.12.2002, p. 1–21).
[11] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72–84).
[12] The Commission has authority to undertake aviation inspections. These inspections can cover Member State aviation security authorities, airlines and airport operators. They include the cyber domain.
[13] One-stop-security is embedded in the common rules but its full implementation varies across the EU, subject to airports having compatible infrastructures.
[14] Germany, Spain, France, Netherlands, Sweden, the United Kingdom and Switzerland (Observer State).
[15] Reference to NIS2 Directive
[16] Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015, p. 1) and its subsequent amendments.

confidential status. The Commission adopts these detailed measures under Commission implementing decisions that are notified to the Member States.

10. Due to the confidentiality and sensitivity of some common rules, the process of stocktaking and reflection on next steps for EU aviation security policy was therefore carried out in a restricted manner. It was led by the Commission services on the basis of inputs from Member States' experts on the AVSEC Regulatory Committee[17] and consultations with the Stakeholders Advisory Group on Aviation Security (SAGAS)[18].

11. During its 103rd meeting, the AVSEC Regulatory Committee launched a new working group to determine and shape improvements to EU aviation security policy[19]. The kick-off meeting took place on 27 January 2020. In the 2 years that followed, partially interrupted by the COVID-19 pandemic, the consultation process with Member States and stakeholders was completed based on five work streams:

    a. the threat picture;

    b. risk-based security: mitigation and commensurability under the EU AVSEC framework;

    c. holistic approach: security culture beyond the checkpoint;

    d. innovation in security processes; and

    e. working together to improve aviation security standards.

12. Some 10 meetings took place where Member States and stakeholders were invited to confirm the main achievements of the EU aviation security system over the last decade, identify current and expected challenges in maintaining a highly performant system, and shape possible next steps and actions to address them. The conclusions of their work are presented in this document.

2. THE EU AVSEC SYSTEM: TWO DECADES OF ACCOMPLISHMENTS

2.1. A system confronted with an ever-changing threat picture

13. For the last 20 years, the civil aviation threat picture has been constantly changing. From aircraft hijackings[20] to the attempted use of various improvised explosive devices[21], terrorists have continued to innovate in trying to circumvent security measures, which always involves more sophisticated devices and plots. The cyber domain points to a number of specific challenges, including the array of actors and motivations (beyond terrorist groups) This trend is expected to persist in the coming years, requiring the AVSEC community to be able to anticipate, prepare, and adapt at all times.

---

[17] Committee on the application of legislation and common rules on the security of civil aviation, C09100 in the Comitology Register.

[18] Expert Group X02883 in the Register of Commission Expert Groups. In addition to stakeholders and EU Member States, EFTA Surveillance Authority and Iceland and Norway are represented.

[19] Meeting minutes, document S10002, 99th meeting of SAGAS in the Register of Commission Expert Groups

[20] September 11, 2001 attack on World Trade Centre

21 Richard Reid, 2006 transatlantic aircraft plot, Umar Farouk Abdulmutallab, Daallo Airlines Flight 159, 2017 Australian aeroplane bomb plot.

14. The Commission itself does not have a specific intelligence service. Instead it relies on the EU Intelligence and Situation Centre (INTCEN), the EU Member States, and other international like-minded partners. The EU INTCEN, part of the External Action Service (EEAS) under the EU High Representative's authority, is the EU's only civilian intelligence entity. The EU INTCEN has its roots in the European security and defence policy. Since 2007, it is part of the Single Intelligence Analysis Capacity (SIAC), which combines civilian intelligence (EU INTCEN) and military intelligence (EUMS Intelligence Directorate). As part of the SIAC, both civilian and military contributions are used to produce all-source intelligence assessments.

15. This information is used in the aviation sector in two ways: i) to feed into risk assessments exercises; and ii) to develop and revise security measures. The Commission services regularly assess the risks to EU civil aviation stemming from terrorism, including threats arising from conflict zones.

16. Based on this work, security measures are designed to tackle the evolution of the threat picture in an environment facing workforce-related challenges[22]. For instance, background checks have been strengthened to mitigate insider threats. Moreover, new categories of detection equipment have been rolled out to tackle the changes in terrorists' modus operandi, such as security scanners, liquid scanners, and explosive trace detection equipment.

2.2. A major benefit: one-stop-security

17. In addition to delivering a high performance EU aviation security system, the approach to adopting common rules across the Member States has helped implement what is considered in the aviation security community as the cornerstone and probably biggest achievement of the EU aviation security system: the OSS principle.

18. OSS enables passengers, their cabin baggage, hold baggage and/or cargo departing from EU airports to be exempted from rescreening when transferring at other EU airports. OSS has several benefits. It delivers increased, speedier and more convenient luggage and passenger throughput, while achieving cost savings and maintaining an equivalent high level of security. It delivers such benefits by avoiding the repetition of security checks on people and items while they remain in a secure environment at all times since their point of departure.

19. OSS is widely established[23] across the EU/EEA and Switzerland, but its full implementation varies depending on whether airports have or do not have compatible infrastructure to automatically segregate different passenger flows (the OSS/non-OSS passengers and the intra/extra Schengen passengers).

[22] Although exacerbated by the COVID-19 crisis, issues with manpower shortage are recurrent in the AVSEC community.

[23] Study on economic and other benefits of one stop security arrangements Project Report by o&i consulting October 2018 – restricted (the OSS Study).

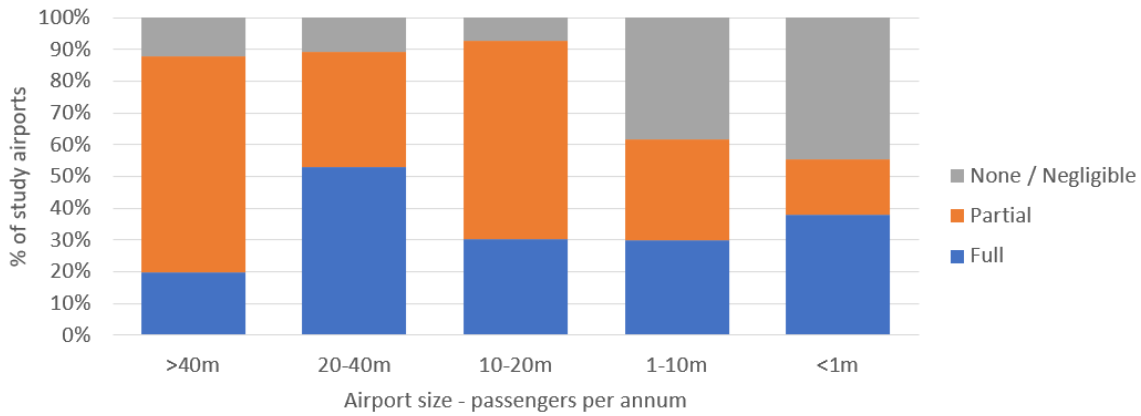

Figure 1 - OSS implementation status by airport size (2018)

20. Based on this success, the Commission has worked to extend OSS to third countries whose AVSEC measures are accepted as at least equivalent to the EU AVSEC measures in terms of security outcome. This acceptance of equivalence is formalised by OSS arrangements between the Commission and these third countries. The Commission currently has OSS arrangements in place with the following third countries and territories: the United States, Canada, Montenegro, Singapore, Faroe Islands, Greenland, Guernsey, Jersey, the Isle of Man, Serbia, Israel and the United Kingdom. Some ongoing initiatives assess the possibility to expand the list of countries participating in OSS.

21. In addition to improving the travel experience for passengers in the EU, the main direct benefit of OSS centres around reducing transfer passenger security costs, which translate into lower transfer passenger security fees. The table below shows an indicative assessment of savings for the EU/EEA and Swiss OSS market. A 2018 study on OSS assessed that already more than 70% of potential savings were made thanks to the implementation of OSS, with EUR 339 m saved each year across the EU/EEA and Swiss market.

OSS market in EU/EEA and Switzerland	Transfer passengers	% of market	Potential OSS saving
Total potential market size	116,827,418	100%	€ 571,286,000
Potential OSS market based on existing OSS countries	97,997,498	84%	€ 479,208,000
Realised OSS market based on airport implementation	69,382,229	59%	**€ 339,279,264**

Table 1 - Potential OSS market size and value of OSS within the EU/EEA/Swiss market in terms of savings in transfer passenger security fees (2018)

22. The intra-EU OSS system is therefore widely supported by EU Member States and the EU aviation industry. It also increases the positive perception that passengers have of the EU aviation security system. As a result, any measure aimed at improving how the EU aviation security system works should be assessed on, among other criteria, its impact on the participation of airports in the EU OSS system.

2.3. A system that has allowed innovation to thrive

23. Innovation in AVSEC technologies is key to anticipating and tackling ever-changing threats. Over the years, the EU has managed to adopt some of the best detection standards for new aviation security technologies. For instance, the Commission adopted

detection requirements for security scanning equipment as early as 2011[24]. The EU has also been a pioneer in some areas, for example, its adoption of detection standards for shoe explosive detection equipment or explosive vapour detection equipment[25].

24. In parallel to these achievements, the European Civil Aviation Conference[26] (ECAC) launched its common evaluation process (CEP) of security equipment to help its Member States evaluate new technologies by sharing results of tests carried out on equipment[27].

25. This evaluation process has become the foundation for the EU's regime of approval of aviation security equipment – the EU Stamp. In January 2020[28], the Commission acknowledged the CEP as a precondition for approving civil aviation security equipment in the EU. As a result, the Commission grants automatic eligibility for the EU approval (and for the EU Stamp marking) to security equipment confirmed by the CEP as meeting ECAC/EU performance standards.

26. It stems from the consultation exercise that this overall achievement has been made possible thanks to the active contribution of some Member States sharing their high level of expertise and technical resources in the appropriate forums (the AVSEC Regulatory Committee, the SAGAS and the ECAC task forces). Stakeholders also contributed to these achievements with their expertise and experience[29].

3. AN EU AVIATION SECURITY SYSTEM FIT FOR THE FUTURE: THREE CHALLENGES

3.1. Drafting EU AVSEC rules

3.1.1. The question of balance between stability and flexibility

27. Discussions in the AVSEC working group have confirmed that the EU AVSEC rules are neither difficult to understand nor arduous to implement separately or together. However, they have become more complex over the years due to the rapid pace of technological and operational changes which have necessitated numerous adjustments to ensure rules remain up-to-date as regards the threat picture and operational constraints. The resulting rapid pace and frequency of changes to the rules has been challenging for operators and regulators alike.

---

[24] Commission Implementing Regulation (EU) No 1147/2011 of 11 November 2011 amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ L 294, 12.11.2011, p. 7.

[25] Commission Implementing Regulation (EU) 2019/103 of 23 January 2019 amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification as well as strengthening of certain specific aviation security measures, OJ L21, 21.1.2019, p.13.

[26] Founded in 1955 as an intergovernmental organisation, the European Civil Aviation Conference (ECAC) seeks to harmonise civil aviation policies and practices among its Member States and, at the same time, increase understanding of policy matters between its Member States and other parts of the world.

[27] The CEP is a laboratory testing programme, which involves testing security equipment so it is line with ECAC/EU performance standards established by ECAC Member States.

[28] Commission Implementing Regulation (EU) 2020/111 of 13 January 2020 amending Implementing Regulation (EU) 2015/1998 as regards the approval of civil aviation security equipment as well as third countries recognised as applying security standards equivalent to the common basic standards on civil aviation security, OJ L 21, 27.1.2020, p. 1–5.

[29] For example, ACI Europe ACBS Joint Operational working group (Airports Council International Europe | ACI EUROPE - Aviation Security Committee (aci-europe.org)) aims to develop practical operational outputs, sharing best practices in the field of technology equipment.

28. Over the last 10 years, the Commission has adopted more than 50 implementing regulations or decisions to amend the EU AVSEC rules. These implementing acts aim to clarify, harmonise, simplify, and most importantly, strengthen EU security measures, including in the cyber domain[30], in the face of more malicious intentions and increased capabilities of hostile third parties. They have also been used to make the common rules more flexible without compromising the security outcome.

29. While Member States and operators have appreciated the flexibility added to the rules over the years, they have also called for a more stable regulatory framework. Stability is key to delivering high performance in the field by ensuring that security programmes and training remain up-to-date. Stability is also essential to allow operators plan their security technology investments and human resource needs in a timely manner. Mirroring this last point, stability is equally crucial to allow security inspectors to develop strong expertise and judgement in enforcing EU AVSEC rules.

30. A widely shared conclusion is that preparing a future-proof EU aviation security system calls for creating a new balance between the necessary stability and the desirable flexibility of EU aviation security rules.

3.1.2. The prescriptive nature of EU implementing rules

31. The working group also found that some of the aviation security implementing rules have become too prescriptive.

32. Firstly, several rules are prescriptive because they result from the transposition of ICAO standards and recommended practices that involve an extensive level of detail. An example is the procedure used for aircraft security searches carried out by the airline crew[31].

33. Secondly, other prescriptive rules in the EU aviation security system are the result of policy choices at EU level. For example, the procedure for carrying out explosive trace detection (ETD). These rules include a high level of detail that has been considered necessary to ensure efficacy in carrying out the related security controls.

34. According to Member States and stakeholders alike, this level of detail has resulted in several EU aviation security rules becoming hard to understand and may hinder innovation in technology or security measures. Therefore, some call for redefining the necessary level of prescriptiveness of the implementing rules.

3.2. The need to support the development and uptake of innovation

35. Although the EU aviation security system has so far co-funded European R&D on aviation security and allowed innovation to thrive, the working group identified three avenues that could further boost innovation in aviation security, these are: (i) improving the process for setting detection standards for aviation security equipment, (ii) increasing the availability of funding, and (iii) boosting the uptake of new equipment at all EU airports. The recommendations of the working group are presented below.

[30] For instance, cyber requirements under Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 are in force and their implementation is subject to the inspection programme of the Commission.

[31] Chapter 15.3.3 Aircraft security searches, ICAO Aviation Security Manual (Doc 8973).

3.2.1. Improving the process for developing detection standards

36. New detection standards are usually developed as a response to new technologies. For example, the Commission adopted new security rules after the new detection standards for security scanners became available. The same concerns the ongoing development of detection standards for the automated detection of prohibited items, thanks to the significant progress made by artificial intelligence technologies. The rules are also changed when there is a change to the threat picture. Developing detection standards for liquid explosive detection equipment is an example of where new detection standards were driven by the change to the threat picture.

37. When it comes to new detection standards, new technologies and new threats, those rely on different development mechanisms. Tackling new threats requires a more comprehensive analysis to assess threats before developing new standards. On the contrary, enabling new technologies like the automated detection of prohibited items with artificial intelligence is more a question of achieving the right security outcome in relation to existing threats and ensuring that new vulnerabilities are not introduced or that they are dealt with more efficiently.

38. Although the current EU aviation security framework has been successful in rolling out new technologies, stakeholders generally emphasise the need to further improve the innovation-friendliness of the regulatory environment, so it can become a key enabler to increase research and development as well as a basis to plan future investments. They call for more planning in relation to developing new detection standards.

3.2.2. Funding innovation

39. The working group recognised that the EU's investment effort in research and innovation is considerable. Horizon Europe is the key EU funding programme for research and innovation with a budget of EUR 95.5 billion for the 2021-2027 period. Security is one of its priorities with an annual budget of about EUR 240 million under the cluster dedicated to civil security. The funded projects typically aim at a technology-readiness level TRL[32] of between 3 and 8 from fundamental technology research up to technology demonstration. Besides projects focused on research and innovation, funded projects also include pre-commercial procurement[33] that helps public buyers procure future innovations and supports coordination and support actions. Over the years, the EU security research programme co-funded technology ranging from explosives detectors to risk-based security management systems, state-of-the-art of biometrics and identity security, and blast-proofing equipment[34]. In addition, part of this funding is also devoted

[32] Technology readiness level (TRL) is a system used to estimate technology maturity, notably in the fields of space, defense and security. TRL is based on a scale from 1 to 9, with 9 being the most mature technology. Using TRLs enables consistent, uniform discussions of technical maturity across different types of technology.

[33] Pre-commercial procurement (PCP) involves procuring research and development for new innovative solutions before they become commercially available.

[34] Examples including projects XP-DITE "Accelerated Checkpoint Design Integration Test and Evaluation", https://cordis.europa.eu/project/id/285311; TRESSPASS "robusT Risk basEd Screening and alert System for PASSengers and luggage", https://cordis.europa.eu/project/id/787120; MESMERISE "Multi-Energy High Resolution Modular Scan System for Internal and External Concealed Commodities", https://cordis.europa.eu/project/id/700399; MELCHIOR "Mechanical Impedance And Multiphysics Concealed And Hidden Objects Interrogation", https://cordis.europa.eu/project/id/101073899, FLY-SEC "Optimising time-to-FLY and enhancing airport SECurity", https://cordis.europa.eu/project/id/653879; SNIFFLES "Artificial sniffer using linear ion trap technology", https://cordis.europa.eu/project/id/285045; CRIMTRACK "Sensor system for detection of criminal chemical substances", https://cordis.europa.eu/project/id/313202;

to 'fast track to innovation' (FTI) projects, whose objectives are to provide funding for close-to-market innovation activities. For example, some European manufacturers (Exruptive, Point FWD) have been granted funding recently for a FTI project to market their innovative equipment for checkpoints[35]. The Horizon Europe's clusters dealing with mobility and with digitalisation – each providing funding of over EUR 1.7 billion a year – could also offer funding opportunities for R&D projects that are relevant for aviation security.

40. However, Member States and industry indicate that this funding source has not been fully exploited in specific projects by the EU AVSEC community. The EU AVSEC community does not seem to be always sufficiently aware of these different funding opportunities for aviation security R&D projects under Horizon Europe. In addition, there has been neither funding for developing detection standards themselves, nor for testing capacities. The EU has a limited capacity for testing detection technologies which requires, for example, the handling of hazardous materials such as home-made explosives: only six laboratories[36] participate in the ECAC's common evaluation process, whose funding scheme is suboptimal when it comes to increasing the testing capacity and expanding its process to new technologies.

41. Developing standards can be costly when it requires a comprehensive assessment of threats. For example, the ongoing work on chemicals, where costs are solely supported by a few contributing entities (from the few participating Member States and the Commission through the JRC's participation) while the results benefit the whole of the EU. The absence of clear funding in developing detection standards slows down the pace of this critical activity, or can even jeopardise it entirely.

3.2.3. On the uptake of new technologies

42. There is a widening gap between innovative solutions that are made possible by the EU AVSEC regulatory framework and the ECAC's support work. There is also a widening gap between the EU and some of its key international partners[37], but most importantly, between EU Member States and EU airports themselves, as seen from the Commission's inspections.

43. The recent discussions for a new roadmap[38] on implementing explosive detection systems (EDS) technologies for screening hold baggage illustrates such a gap. Many EU airports have successfully renewed their EDS in due time and some are already screening hold baggage with the newest Standard 3.1 EDS equipment. However, a significant number of other EU airports have yet to complete the phase-out of old Standard 2 EDS equipment.

MULTISCAN3D "Cosmic Ray Tomograph for Identification of Hazardous and Illegal Goods hidden in Trucks and Sea Containers", https://cordis.europa.eu/project/id/101021812; SilentBorder "Laser-plasma based source 3D Tomography for cargo inspection", https://cordis.europa.eu/project/id/101020100.

[35] Project XSPERINSE, https://www.xsperinseproject.eu/, https://cordis.europa.eu/project/id/853720

[36] https://www.ecac-ceac.org/activities/security/common-evaluation-process-cep-of-security-equipment

[37] TSA awards $781.2 million to procure additional CT X-Ray scanners for airport checkpoints (https://www.tsa.gov/news/).

[38] Commission Implementing Regulation (EU) 2020/910 of 30 June 2020 amending Implementing Regulations (EU) 2015/1998, (EU) 2019/103 and (EU) 2019/1583 as regards the re-designation of airlines, operators and entities providing security controls for cargo and mail arriving from third countries, as well as the postponement of certain regulatory requirements in the area of cybersecurity, background check, explosive detection systems equipment standards, and explosive trace detection equipment, because of the COVID-19 pandemic, OJ L 208, 1.7.2020, p. 43.

44. The use of security scanner equipment is another example of such a gap. Some Member States started trialling this new equipment as early as 2006. These trials opened the way for the Commission to adopt detection standards for security scanner equipment as early as 2011. Some 10 years later, while the added value of this technology for security has been proven, some major airports in Europe are still not using this equipment, while other airports similar in size and business model are already fully equipped.

45. Although the EU AVSEC community has managed to collectively develop and adopt new detection standards and to evaluate new categories of equipment, the uptake of innovation could be improved. The reason for this gap is mainly due to the cost of security equipment, which is difficult to finance or even justify for airports with lower passenger traffic, or for airports with high seasonality. Timely and even rollout of innovatory technologies can improve the performance of the EU aviation security system as a whole, as well as the passenger travel experience, as they may allow dropping additional or alternative security measures, such as restrictions on the carriage of liquids, aerosols and gels in cabin baggage.

3.3. The challenge of an ever-changing threat picture

46. A clear observation of the working group has been that the threat picture for aviation security has been constantly changing. From the initial use of guns and knives to hijack aircraft, to explosives (civil and military) and more recently to home-made explosives with increasingly sophisticated devices, the spectrum of threats that need to be tackled to protect civil aviation from unlawful interventions is widening. This trend is not likely to change in the coming years.

47. The resilience of the EU aviation security system therefore continues to be tested, and hence the working group calls for regular assessments of different available technologies in the light of the expected changes to the threat picture, and in order to increase preparedness and resilience of the EU security system to those new threats.

48. In this context**,** Member States and stakeholders suggested that the enhancement of the EU aviation security system could **focus on three objectives:**

- **its rule making process** should balance **stability and flexibility** , ensuring that **the right level of detail** is contained in the common rules and promoting local risk assessments and out of the box thinking**;**
- **boost** the **development and uptake** of **innovation;**
- **update the EU baseline on security equipment** to increase **preparedness** and **resilience** to new threats**.**

4. THE RULE-MAKING PROCESS

4.1. Balancing stability and flexibility in the common rules and ensuring the right level of detail

49. As explained above, due to frequent changes in the security rules, Member States and operators experience some difficulties in promptly implementing those changes. While Member States and operators have appreciated the flexibility added to the rules over the years to adapt to some local characteristics, they also request more stability.

50. To this end, consulted parties suggested reducing the scope and frequency of amendments to the minimum necessary, limited to, for example:

    a. updating the EU AVSEC rules to address any change to the threat picture;

    b. introducing new technologies or updating detection standards;

    c. transposing new ICAO Annex-17 standards; and

    d. correcting identified problems with implementation.

51. To maintain flexibility of the system, the working group suggested that the above-mentioned approach is supplemented with a thorough revision of the complete set of rules at a regular interval, e.g. every 5 years.

52. An alternative option that had been raised could be to add limited flexibility (e.g. limited to one proposal by Member States and stakeholders per amendment exercise).

53. Another characteristic identified by the working group is the prescriptive nature of some common rules. Therefore, the group suggested, that when a rule is very prescriptive, two questions need to be asked:

    a. Is the level of detail necessary to ensure the security objective underpinning the rule?

    b. If yes, is legislation (the implementing regulation or decision) the right method to address these details?

54. One third of the AVSEC rules laid down in the implementing regulations are checklists used by validators[39] of cargo operators. While these checklists are necessary to ensure the EU AVSEC cargo regime works well, the stakeholders consider that those checklists do not necessarily have to be set out in the implementing regulations. An alternative could be to include such guiding documents in the existing KSDA database[40]. This would simplify the implementing regulations, and would also greatly help in updating or correcting these checklists without having to draw up and adopt amendments. However, it has been made clear by Member States that these checklists should still be endorsed within the AVSEC Committee.

55. Another example relates to technology, where equipment is confirmed by ECAC laboratories as meeting EU standards required for detection performance by applying 'conops' (i.e. the manual of operations). As such, one can question the added value of going into extensive detail in the common rules about how equipment should be used. In doing so, there is a risk of hindering innovation. For instance, the rules require passengers to remove their coats or jackets before being screened. New security scanners will soon be able to screen passengers without them having to remove their coats or jackets. The current level of detail in the common rules would require an amendment to allow the use of innovative technologies. This approach could be replaced and simplified with a focus on 'conops' equipment validation and production of guidance material.

[39] Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security, OJ L 299, 14.11.2015, p 42-101

[40] KSDA – EU database on supply chain security (https://ksda.ec.europa.eu).

56. As far as the aspect of cybersecurity is concerned, the NIS2 Directive lays down the baseline for cybersecurity risk- management measures and incident reporting requirements across various economic sectors, including the aviation sector. In order to avoid fragmentation of cybersecurity provisions of Union legal acts in cases where further sector-specific provisions related to the cybersecurity risk-management measures and incident reporting are considered necessary, the co-legislators tasked the Commission first to assess whether such sector-specific provisions could be stipulated in an Commission implementing act under the NIS2 Directive[41].

4.2. Better use of risk assessment to address local aspects

57. As recalled during the consultation process, devising an effective security plan that correlates to the risks posed by a threat against civil aviation is still one of the most difficult tasks for aviation security professionals. In addition, EU law explicitly requires risk assessments in a number of cases, notably when Member States derogate from the common basic standards referred to in Article 4(1) of Regulation (EC) No 300/2008 and adopt alternative security measures that provide an adequate level of protection. In this case, the risk assessment approved by the appropriate authority is carried out locally, i.e. at airports or demarcated areas of airports where traffic is limited to certain categories that exclude commercial aviation.

58. When asked if the EU aviation security system should regulate local risk assessment, the working group preferred an expertise-building approach to help authorities and operators – for instance, through guidelines on how to conduct local risk assessment when mandated by the implementing legislation. Existing methodologies in ICAO could be used to develop suitable guidance material for aviation security.

4.3. Thinking outside the box

59. As expressed by a number of stakeholders, a complementary approach to the policy changes mentioned above would be to strengthen the 'thinking outside the box' approach, i.e. allow some space in exchanges between Member States and stakeholders for innovative thinking to prepare long-term changes. In this context, cooperation with the working group on cybersecurity in aviation sector established under the above-mentioned NIS Directive could be considered. Such collaboration would include exchange of information and best practices in the cybersecurity domain.

60. An example of thinking outside the box could be to assess other approaches to rule making and if and how it could be applied to aviation security. This kind of thinking is also reflected at ICAO level where the AVSEC panel questioned the general approach taken for Annex 17 and whether the safety realm offered useful approaches adapted to the specific features of security.

61. In the EU aviation safety system, three main levels of rules exist:

    i. the Basic Regulation itself, adopted by the European Parliament and the Council;

    ii. Implementing Rules to the Basic Regulation, adopted by the Commission; and

[41] See recital 22 NIS2 Directive

iii. certification specifications, acceptable means of compliance (AMC) and guidance Material (GM) adopted by the European Union Aviation Safety Agency.

62. The ICAO working group on Annex 17 raised the possibility of using AMC in the form of appendices to Annex 17 as they do for other annexes.

63. Another way to think outside the box on new technologies could be to replace the listing of authorised screening methods in EU legislation with a 'system approach'[42]. A checkpoint could be considered as a 'black box' whose overall level of performance would be regulated without specifying in detail each possible layer.

64. Another example would be to take the life cycle of equipment into account further. Generally, a new technology is installed to meet a regulatory obligation (for example, replacing Standard 2 EDS[43] equipment with Standard 3 EDS equipment) and is not modified or updated until the next regulatory obligation, even if updates that deliver a better security outcome are available. Therefore, another example of thinking outside the box could be to request operators to exploit to the fullest the installed technology, irrespective of regulatory milestones: if an airport is equipped with a Standard 3 EDS for which an update to Standard 3.1 is available, applying this update would boost security.

65. The above examples of thinking outside the box are not changes which can be addressed in the short term. They require further analysis, and where relevant impact assessments, and the challenges for implementation need addressing. Space should be provided in the exchanges with Member States and stakeholders to collectively think outside the box when preparing for the long-term development of the EU aviation security system.

DRAFTING EU AVSEC IMPLEMENTING RULES: NEXT STEPS

- 1 - The Commission services will consult Member States and stakeholders on a new process aiming at slowing the pace and reducing the scope of amendments to EU AVSEC rules, as well as on the frequency of more thorough revisions.
- 2 - The Commission services will consult Member States and stakeholders on the level of detail contained in EU AVSEC rules in the context of the next thorough revision of these rules.
- 3 - The Commission services will present to Member States and stakeholders draft guidance on relevant topics, starting with local risk assessment for discussion and adoption in AVSEC and SAGAS.
- 4 - The Commission services will devote time in AVSEC and SAGAS to exploring 'thinking outside the box' concepts with Member States and stakeholders that could be applied in the long term.

[42] Optimising multi-layered security screening, David Anderson, JRC in Journal of Transportation Security, December 2021.
[43] EDS equipment is used for screening hold baggage.

5. BOOSTING THE DEVELOPMENT AND UPTAKE OF INNOVATION

5.1. Supporting the development of new technologies

5.1.1. Developing standardised processes for detection standards as a key enabler for innovation

66. As mentioned above, the EU aviation security system has been successful in adopting new technologies. Nevertheless, Member States and stakeholders alike have listed several courses of action that could be pursued to further improve the development and step up the adoption of new technologies in the EU.

67. One course of action suggested by the working group is the development of 'standardised' processes to develop new detection standards. Such processes would provide for:

    i. clear (and stable) implementation dates that give certainty to the industry;

    ii. clear concepts of operations describing how to use the technology, with clear limitations if needed;

    iii. dates for phasing out old technology;

    iv. incentives to accelerate implementation.

68. Moreover, Chapter 12.8, 'Methods of screening using new technologies' of Regulation (EU) 2015/1998 allows a Member State to organise trials to experiment with new screening methods. These trials have been successfully conducted in the past. The most recent example enabled the Commission to adopt detection requirements for shoe explosive detection equipment. However, the number of recent trials have been limited. These are always the same few Member States that conduct these trials, even though the regulatory requirements allowing such trials are not very stringent. Joint trials with two or more Member States so that more airports can join could be encouraged and supported. The SAGAS could, in addition to the existing documentation on trials, draw up and maintain a list of necessary trials to be carried out at European airports ('call for trials').

69. Furthermore, drawing up an official long-term capability-based technology roadmap could enable new detection standards to be adopted with accepted implementation and phase-out dates. It would inform Member States and stakeholders years in advance about the investments that would be required in the future. Adequate flexibility would allow external factors to be taken into account, such as possible changes to the threat picture that would affect technology development. The AVSEC Regulatory Committee's work programme is a useful tool for communicating the development activities of the Committee to the stakeholders. However, this document is solely indicative. Such a long-term roadmap for technologies would need to involve Member States and stakeholders years in advance and inform them about the investments that would be required in the future.

5.1.2. Improving funding for the development of innovation

70. As stated above, the EU aviation security community is often not fully aware of the possibility to fund aviation security R&D projects under Horizon Europe.

71. The working group agreed that European stakeholders must be made better aware about the opportunities for R&D on aviation security under Horizon Europe. This could be done through programming topics in Horizon Europe work programmes, targeted promotion of R&D funding opportunities in the aviation security community and better dissemination of exploitable research results.

72. A number of areas could therefore be further explored:

    i. promoting already available funding for R&D in aviation security in EU framework programmes for R&I;

    ii. identifying EU funding opportunities for R&D in aviation security in the AVSEC Committee and SAGAS;

    iii. mobilising funding to improve European testing capacity, in particular by expanding it to new technologies.

5.1.3. Promoting security by design

73. ICAO Annex 8 on airworthiness of aircraft includes only three requirements for security purposes: i) the least-risk bomb location, ii) the reinforcement of flight crew compartment (i.e. cockpit door) and iii) general considerations for deterring by design the easy concealment of weapons.

74. A possible improvement identified by the working group is to start a structured dialogue with aircraft manufacturers on security by design. Airport and cybersecurity design could also be explored as ways to increase security standards. The Commission proposal for a Cyber Resilience Act[44], which aims to lay down cybersecurity requirements for products with digital elements, such as wireless and wired products and software, used also in air transport sector, should be taken into account. As a first ever EU wide legislation of its kind, it introduces mandatory cybersecurity requirements for manufacturers and developers and vendors of products with digital elements, throughout their whole lifecycle. It aims to establish common security requirements for products with digital elements and may lead to further standardisation and the use of certification for certain products.

5.1.4. Fostering key international partnerships with like-minded countries

75. Developing detection standards and evaluating technologies is costly. Sharing the effort with some key international partners would allow the EU do more with fewer resources and act more quickly. This could be particularly relevant with like-minded countries such as the US.

76. Over the years, cooperation between the US and the EU/ECAC has grown, each party gaining an increased understanding of how the other is organised to develop detection standards and evaluate technologies. In the specific work stream on chemical threats for instance, this cooperation seeks convergence on detection standards for aviation security equipment between the EU and the US.

[44] Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM/2022/454 final)

77. According to the working group recommendations, this cooperation could be expanded further and also include cooperation in evaluating technology. In addition to cost sharing, such cooperation and aligning of standards would also benefit manufacturers by enabling access to both markets.

78. This avenue could explore various concepts of increased cooperation, ranging from increased sharing of information to mutual recognition for the evaluation of aviation security equipment, or even joint development projects. However, as the US and the Commission/ECAC/Member States have different roles and responsibilities as regards aviation security equipment (i.e. the US TSA[45] being both regulator, final user and owner of equipment), when considering different options for potential increased cooperation with the US, a level playing field for the manufacturing industry would have to be ensured. The added value of national certification in Member States, the reciprocal nature of such initiatives and their impact on the pace of innovation in the EU also have to be taken into account to determine the scope of such cooperation.

5.2. Accelerating the implementation of technology in Europe

5.2.1. Market-based solutions: the development of open architecture

79. Notably airport operators have pointed that open architecture offers an interesting path to supporting a timely uptake of innovation in aviation security. It refers to physical and software architecture where interfaces, communication and protocols are publicly available, well documented and free to use. This greatly helps in the sharing of data and in the adding, replacing and updating of modules without unreasonable difficulties (commercial barriers, proprietary protocols etc.). Open architecture issues can be particularly relevant to software architecture for airport security systems.

80. Many benefits can be generated such as enabling third party algorithms or increasing the agility of airports to adapt/evolve to new situations. For example, ACI Europe drives the initiative for developing open architecture for aviation security equipment[46] which primarily concerns supply and demand between vendors and users. The regulator's role in such context would be to ensure that potential new vulnerabilities, due to increased sharing of data between equipment, are dealt with appropriately and that the standardisation needed to enable open architecture does not hinder innovation stemming from competition.

5.2.2. Challenging a one-size-fits-all approach and supporting a more ambitious aviation security baseline

81. According to a number of Member States and stakeholders, the current 'one-size-fits-all' approach may partially explain why it has been difficult to implement new technologies, as well as phase out the old ones. The smallest European airports often struggle to afford the latest technologies. The high performance technologies (such as security scanner and EDS for cabin bags) are increasingly being put into operation in EU airports. Against this background, some participants in the working group proposed exploring alternatives to the 'one-size-fits-all' concept, as a regulatory response to mitigate the impact of uneven implementation of innovatory technologies.

[45] Transport Security Administration
[46] Open Architecture for Airport Security Systems (aci-europe.org)

82. One option would be to create a new future-proof baseline that would fully exploit present and future technology potential (See Chapter 6.2 – 'Creating a future-proof EU Baseline').

83. It is clear from the exchanges in the working group that a new updated EU baseline if based on the latest technology would be out of reach for a number of European airports, in particular smaller, regional airports. It is not always possible to build a business case that justifies the large investment necessary to operate these new technologies at those smaller airports. However, this cannot justify new technologies not being implemented in good time in other European airports. Therefore, in parallel to creating the new baseline and establishing the transition plan, it is proposed to help small, regional airports in operating the OSS network through possible additional security measures. One of the options put forward by the working group for consideration was a possible revision of Regulation No 1254/2009[47].

84. Derogation from the common basic standards under Regulation No 1254/2009 currently allows for an exclusion from the intra-EU OSS. If the Regulation were to be revised, the extent to which the smaller EU airports would have to bear such a drastic consequence could be explored. Exploring these concepts requires an analysis of if or how risk assessments could reconcile derogation from the common basic standards and inclusion in the intra-EU OSS. This would call for several options to be explored for passengers departing from small airports under Regulation No 1254/2009 and transferring in larger hubs:

    i. passengers coming from a '1254/2009 airport' and transferring in a larger hub would need to be rescreened (end of OSS for these small airports);

    ii. based on risk assessment, only those passengers that transfer to a 'high risk' flight would need to be rescreened;

    iii. based on risk assessment, a percentage of those passengers would need to be rescreened (wherever the destination);

85. In examining such options, one criterion should be their impact on the positive perception and engagement of passengers with regard to security measures.

BOOSTING THE DEVELOPMENT AND UPTAKE OF INNOVATION: NEXT STEPS

- 5 - The Commission services will consult Member States and stakeholders on creating 'standardised' processes to develop new detection standards.
- 6 - The Commission services will organise a focused and regular dialogue between the AVSEC community (i.e. Member States and stakeholders) to programme adequate funding to projects relevant to aviation security.
- 7 – The Commission services will explore with Member States and stakeholders alternative concepts to the 'one-size-fits-all' approach while ensuring minimal impact on the OSS regime.
- 8 – The Commission services will explore with Member States and stakeholders the possibility to adopt official technology roadmaps to enable detection standards to be adopted, implemented and phased out in future.
- 9 – The Commission services will explore with Member States and stakeholders the

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

possibility to support trials of new technology with 'calls for trials'.

- 10 - The Commission services will consult Member States and stakeholders on a possibility to increase cooperation in developing detection standards and evaluating equipment with the US and other like-minded international partners.
- 11 - The Commission services will consult Member States and stakeholders on starting a structured dialogue with aircraft manufacturers on security by design.

6. CREATING A FUTURE-PROOF BASELINE FOR AVIATION SECURITY IN THE EU

6.1. Updating the mapping of risks and prioritising threats

86. Faced with an increasingly complex and multi-faceted threat, the priority of the current EU security aviation system is to ensure a maximum level of security while providing positive passenger experience to the extent possible. This in practice requires identifying and maintaining a precise mapping of risks to better support development efforts and optimise the interaction of different technologies over time.

87. Although the Commission services regularly monitor changes to the threat picture and regularly update Member States on the mapping of risks, the working group noted that the last complete mapping exercise was carried out in 2014. Therefore, the working group called on the Commission services to consult Member States about the launching of a new mapping exercise. For what concerns cybersecurity, at the request of the Council[48], the Commission, the High Representative of the Union for Foreign Affairs and Security Policy, and the NIS Cooperation Group[49] are developing risk evaluations and risk scenarios for digital infrastructure security. The focus will in the first instance be on cybersecurity in only four sectors, including transport. This exercise aims to further increase the protection of critical infrastructure, against large-scale cyberattacks.

88. In addition to the mapping of risks, the working group has also pointed that increasing threats make it more challenging for the technical experts to develop detection standards. The current approach, by which new threats are added without removing the 'old threats' could soon reach its limits. Each new layer in the automatic detection of threats comes with false alarms that need to be addressed, hindering throughput and facilitation. Therefore, the AVSEC Committee suggests looking at better prioritising threats by tasking a dedicated subgroup that would inform technical experts developing equipment detection standards about the most relevant threats.

6.2. Creating a future-proof EU baseline

89. Over the last decade, aviation security technologies have improved to a point where it has become difficult to presume that all screening technologies deliver the same level of security performance. As expressed in the working group, even if the newest technologies have drawbacks and weaknesses, comparing the performance of old technology like walk-through metal detectors with security scanners no longer seems relevant, especially when considering emerging threats that need to be addressed today.

90. Therefore, the EU AVSEC regime baseline would need to be reassessed in the light of changing threats and available technologies. To deliver the expected benefits, a new

[48] Council conclusions on the development of the European Union's cyber Posture; ST09364/22, 23 May 2022
[49] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

passenger checkpoint baseline should fully benefit from new and cutting-edge technologies while addressing the highest priority threats (based on the updated mapping of risks mentioned above) and allowing for agile adaptation to changes to the threat picture. Simultaneously, smaller airports should be given the opportunity to continue participating in the EU OSS system. Therefore, such a new baseline would require:

i. a transition plan that would bring airports in line with this new baseline at a sustainable pace;

ii. an assessment of whether alternative plans are acceptable to deliver equivalent security performances, e.g. whether it would be acceptable to continue operating walk-through metal detection equipment with a higher rate of random ETD checks, or by how much would random ETD checks need to increase to be considered as equivalent to operating a security scanner.

CREATING A FUTURE-PROOF BASELINE FOR AVIATION SECURITY IN THE EU: NEXT STEPS

- 12 - The Commission services will consult Member States on a complete revision of the mapping of risks, including in the cyber domain.
- 13 – The Commission services will consult Member States on the creation of a subgroup of the AVSEC Regulatory Committee to maintain a list of prioritised threats.
- 14 - The Commission services will consult Member States and stakeholders on the creation of a new future-proof EU baseline.

7. CONCLUSION

91. The above contribution of the working group constitutes an ambitious programme for taking the EU aviation security strategy forward. The working strands set out in this document will serve as a basis for the Commission services to carry out further exploratory work in consultation with Member States and stakeholders as laid down in the Next Steps boxes above.

92. A progressive phasing in of new measures would be necessary. Moreover, all of these actions are interconnected in some shape or form. For instance, a technology roadmap would not only have to incorporate changes in the threat picture, but would also have to take into account the rhythm of Horizon Europe programmes in order to try and secure financing.

93. Similarly, a change of baseline should help in increasing the uptake of innovation by airports. However, the pace of innovation uptake would have to be carefully adjusted to minimise the negative impact for smaller airports that are connected to major hubs.

ANNEX

Organisations represented in the SAGAS

Abbreviation	Full name	Website
ACI EUROPE	Airport Council International Europe	https://www.aci-europe.org
ASSA-I	Aviation Security Services Association – International	https://assa-i.org
CLECAT	European Association for forwarding, transport, logistic and customs services	https://www.clecat.org
EAASP	European Association of Airport and Seaport Police	https://eaasp.org
EASA	European Aviation Safety Agency	https://www.easa.europa.eu
ECA	European Cockpit Association	https://www.eurocockpit.be
EEA	European Express Association	https://www.euroexpress.org
EOS	European Organisation for Security	www.eos-eu.com
ERAA	European Regions Airline Association	https://www.eraa.org
ETRC	European Travel Retail Confederation	www.etrc.org/
EUROCONTROL	European Organisation for the Safety of Air Navigation	https://www.eurocontrol.int
EVAAS	EU Validators' Association for Aviation Security	https://evaas.eu
Hume Brophy	Consultancy	https://humebrophy.com
IATA	International Air Transport Association	https://www.iata.org
ICAO	International Civil Aviation Organisation	https://www.icao.int
POSTEUROP	European public postal operators	https://www.posteurop.org/