Department for Transport

Better regulation for aviation security consultation document

July 2011

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text will be made available in full on the Department's website. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
76 Marsham Street
London SW1P 4DR
Telephone 0300 330 3000
Website http://www.dft.gov.uk/
General email enquiries FAX9643@dft.gsi.gov.uk

Better regulation for aviation security

Contents

1. Foreword by the Secretary of State for Transport

1.1 I am clear as the Minister with regulatory responsibility for aviation security that the UK faces a real and ongoing threat from international and domestic terrorism. Aviation has been a terrorist target for at least forty years. But the nature of that threat has changed significantly. Early threats were mainly related to hijacking. More recently, terrorists have sought to destroy aircraft in flight, using devices carried by passengers and concealed within cargo, or to crash aircraft into targets on the ground. Terrorists have also attacked airports.

1.2 The aviation sector continues to be targeted by terrorists. We cannot afford for our security arrangements to fail. The human and economic impact of a successful attack can have consequences on a par with a major natural disaster, and the continuing and evolving threats have brought about extensive international, European and domestic aviation security regulations designed to protect passengers, crew and those on the ground.

1.3 The Government's recent strategic review of defence and security set out its proposals for securing Britain in an age of uncertainty[1] and included a commitment to improve aviation security. The public rightly has a high confidence in the security of aviation in the UK, and the challenge to both the Regulator and the industry is to improve security, in a way which minimises inconvenience to passengers.

1.4 In order to reflect best practice in regulation, the current regime needs modernising which the Government believes can be achieved with an outcome focused, risk-based approach. This will provide the industry with more freedom to deliver bespoke solutions, focused on achieving security outcomes rather than having to follow prescriptive measures. This would maintain the existing high security standards, but more efficiently and with greater focus on the passenger. This is in line with the Government's policy of decentralisation - allowing more control to those who deal with passengers on a day-to-day basis.

1.5 Government will always retain its ultimate responsibilities for aviation security, continue to establish the threat and risk picture, and specify security outcomes for the industry to meet. This will include a list of priority risks for which operators must have adequate mitigation. There will also be a rigorous monitoring framework to ensure the aviation industry discharges its responsibilities effectively.

1.6 This approach offers a new partnership between Government and the industry dedicated to maintaining the highest standards in aviation security whilst also improving the passenger experience. I hope all interested parties will contribute their views on these proposals over the coming months. We look forward to hearing from you.

[1] http://www.parliament.uk/business/news/2010/10/strategic-defence-and-security-review/

2. Executive summary

2.1 The events of Lockerbie, September 2001, and more recent attempts to attack aircraft using explosive devices concealed in shoes, liquids, underwear and air cargo show that the aviation sector is constantly under a high level threat of terrorist attack. The UK is recognised internationally as having one of the most effective aviation security regimes in the world. However, we believe that improvements are still necessary and the prescriptive nature of the current regime presents barriers to a rapid and effective response to evolving threats. Furthermore, the current regime does not sufficiently incentivise the industry to innovate or improve security outcomes. It is vital that we make best use of our airports and improve security, whilst also improving the passenger experience.

2.2 Modernising the regulatory regime for aviation security forms part of a cross-departmental approach to improving aviation security set out in the government's strategic defence and security review. Effective aviation security regulations complement the wider border security role of the UK Border Agency and ports policing operations which, for example through passenger screening, contribute to aviation security, to driving up security standards and to improving passengers' experience.

2.3 This consultation seeks responses to the Department's proposed changes to the UK's aviation security regulatory framework. Under the new proposals the current 'direct and inspect' regulatory regime will be replaced by an outcome focused, risk-based (OFRB) approach. This is consistent with modern regulatory principles and mirrors the approach taken to regulate aviation safety in the UK.

2.4 So what does an OFRB approach mean? Under the new regulatory approach the focus will primarily be on the delivery of security outcomes rather than the delivery of specified processes. It will be for the Department to set overall requirements based on the level and nature of threat at the time. The industry will then be able to design security processes that deliver specified security outcomes rather than having to follow detailed rules. Examples of how security outcomes could work in practice can be found at Annex C. There are baseline regulatory requirements, such as EU common basic standards[2], that those responsible for their implementation must continue to meet. Directions made under the Aviation Security Act 1982 (ASA) must also be complied with.

2.5 However, one of the aims of an OFRB approach is to provide the industry with greater ownership of security considerations and give more freedom to integrate security within day-to-day business activities. The more innovative the business the more likely it is to offer a better travelling experience for the passenger compared with commercial rivals. The new approach is about moving to a system that further prioritises inspections based on risk and incentivises the industry to collectively raise overall security performance.

[2] 'EU common basic standards' is used throughout to mean Regulation (EC) No 300/2008 on common rules in the field of civil aviation security and the accompanying implementing and supporting legislation.

2.6 Under the proposed approach, those responsible for implementing the EU regulations and all directed parties under the ASA ('the industry') would be required to implement a Security Management System (SeMS) – a framework through which an operator plans and delivers its security processes. A SeMS requires a system to ensure an overall high standard of security and includes a number of key components:

- the assessment and mitigation of security risk[3]
- the security policy and outcomes, including management accountabilities and responsibilities
- the defining and recording of appropriate security measures to be implemented across the organisation
- security assurance through regular reporting in terms of occurrences and performance, data analysis and review, internal and external audit, covert testing, and arrangements for continuous improvement
- security promotion through staff training and communications to deliver a strong security culture.

2.7 A SeMS is a dynamic management process which is continually monitored and reviewed to take account of changes in the threat environment, organisational changes and the results of analysis. A key feature would be a process whereby the industry itself regularly reports on its own security performance, significantly increasing the volume of performance data available to the security Regulator. The reporting of certain serious lapses would be mandatory (comparable to safety incident reporting in industry) with criminal penalties applying that are available in existing legislation. As mentioned previously, all entities that are required to comply with EU common basic standards and domestic directions will of course continue to have to do so.

2.8 Under the current approach the Regulator specifies detailed requirements and then verifies adherence with these (direct and inspect). Under the new approach the Regulator will specify security outcomes and then examine the effectiveness of the systems proposed to meet these (process assurance).

2.9 The industry will still be subject to baseline monitoring and compliance by the Regulator (including inspections by the European Commission). However, the Department is also examining how a more risk-based approach to this might work. The intention is that capability and performance will be rewarded with ‘earned autonomy’, whereby the Regulator is able to reward a robust system of aviation security with greater trust in how they deliver the specified security outcomes. Conversely, the level of scrutiny by the Regulator needs to increase proportionately to any lowering of performance.

2.10 The move to an OFRB approach is part of a package of regulatory reforms that also includes the transfer of certain day-to-day security regulation functions from the Department to the Civil Aviation Authority (CAA). A consequence of this proposed transfer is that the cost of aviation security regulation will be recouped

[3] Threat and Risk information will be provided by DfT based on information supplied by the Joint Terrorism Analysis Centre (JTAC) and other Government agencies.

by the CAA from the industry.

2.11 This is consistent with the approach taken to the funding of aviation safety regulation and for the other aspects of aviation security where the costs are met by the 'end user'. The transfer of functions will be enabled through primary legislation that will be subject to Parliamentary scrutiny and debate, and is not part of this consultation. However, when the Parliamentary process begins we shall be writing to industry seeking views.

2.12 The Department's objectives for these reforms are:

- **to maintain and improve security standards:** the current approach to security regulation, based on a direct and inspect approach, whilst effective, risks not engaging the industry sufficiently in delivering security, nor enabling the industry to integrate security fully within its own systems;

- **to adopt the principles of better regulation[4]:** our proposals seek to improve the relationship between the Regulator and the industry by moving away from 'tick box' regulation to a more up-to-date OFRB approach;

- **to apply the 'user pays' principle**: the aviation industry already pays for the costs of safety, consumer and economic regulation. Security regulation is funded by the taxpayer. The transfer of certain compliance and regulation functions will enable the cost to be recovered by the CAA;

- **to make aviation security consistent with a 'better not bigger' approach being taken to airport development:** by creating a more flexible approach to regulation, the Department can enable the industry to take innovative approaches to delivering its security responsibilities, which should in turn enable the industry to operate more efficiently and provide a better experience for passengers.

2.13 Initially, we propose introducing the new approach to airports and airlines currently subject to the National Aviation Security Programme (NASP) and directions made under the ASA. The Department believes that these parts of the industry are best placed to make these changes (as many already operate a SeMS) and improve the passenger experience. The new approach will need to reflect the considerable difference in scale of operations and this consultation asks how this could best be done. Once the new approach is embedded it is intended to roll it out to other parts of the aviation industry (i.e. cargo and in-flight supplies).

2.14 We are not expecting these changes to be implemented for every affected party on a specific date. Rather we are proposing a phased implementation over a number of years as it will take time to embed the new approach and for new SeMS to mature.

[4] http://www.bis.gov.uk/policies/better-regulation/policy

2.15 An Impact Assessment (see section 5, page 23) on ‘Reforms to the Aviation Security Regulatory Framework (Better regulation for aviation security)’ has been published in addition to this document on which we are also seeking views.

3. How to respond

3.1 The consultation period started on the 14th July and will close on the 7th November. Any responses received after that date will not be considered so please ensure that your response reaches us by that date. If you would like further copies of this consultation document it can be found at http://www.dft.gov.uk/consultations or you can contact us at the address below or by phone on 0207 944 2692 if you would like alternative formats (Braille, audio CD, etc).

3.2 A response form is provided on our website with the consultation document but you may respond to the consultation in a number of ways:

- *online* https://consultation.dft.gov.uk/dft/dft-2011-21/

- *email*
  avsec.reform@dft.gsi.gov.uk

- *post*
  Better regulation for aviation security consultation
  The Department for Transport
  25/1 Great Minster House
  76 Marsham Street,
  London
  SW1P 4DR

3.3 When responding, please state whether you are responding as an individual or representing the views of an organisation. If responding on behalf of a larger organisation please make it clear who the organisation represents, and where applicable, how the views of members were assembled.

3.4 We have included a list of consultees within this document but please let us know if there are any other parties who would be interested in responding to this consultation who we may have missed.

3.5 Thank you for taking time to respond to this consultation. Please note we will not be responding individually but will consider all responses, and then publish a summary report along with next steps.

Freedom of information

3.6 Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the Freedom of Information Act 2000 (FOIA) or the Environmental Information Regulations 2004.

3.7 If you want information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence.

3.8 In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

3.9 We will process your personal data in accordance with the Data Protection Act and in the majority of circumstances this will mean that your personal data will not be disclosed to third parties.

4. The proposals

Introduction

4.1 The UK is recognised internationally as having one of the most effective aviation security regimes in the world. However, we believe that the current security regulatory system is too prescriptive, adding unnecessarily to the industry's costs. Furthermore, it does not sufficiently incentivise the industry to innovate or improve security. It is vital that we make best use of our airports and improve the passenger experience.

4.2 The ease with which passengers are able to go through aviation security processes forms an important part of their overall journey experience. When done poorly, it can add time, cost and inconvenience to their journey. While there can be no compromise over essential security standards, it is important to consider the passenger experience while ensuring that security is delivered effectively.

4.3 In discussions with aviation industry and passenger groups, airport security is usually raised as a key area where there is potential for improvement.

The current regulatory approach

4.4 The UK aviation security regulatory system is currently based on directly applicable EU civil aviation security regulations establishing common basic standards across Member States and on Directions made under the Aviation Security Act 1982 (ASA) laying down UK More Stringent Measures (MSMs) which the Department believes are appropriate, given the level of terrorist threat faced by the UK.

4.5 This legislative framework prescribes in great detail the security processes that must be followed by the aviation industry. The industry's legal responsibility is to implement the relevant procedures. The extent to which this is achieved is assessed through a programme of inspections, testing and audit, carried out by the Department. This involves investing time and energy in advising and working with the industry to improve compliance.

4.6 The current approach does not, in practice, greatly emphasise internal quality control by the regulated industry; and has no consideration of security outcomes; no required reporting processes by which the industry or the Regulator can gain a comprehensive picture of the quality of the security work; and almost no discretion for the industry to deliver security outcomes in other ways that may be better integrated with the way it runs the rest of its business.

The transfer of certain security functions from the Department to the Civil Aviation Authority (CAA)

4.7 The Department plans to transfer certain aviation security functions currently delivered by the Department to the CAA – the UK's specialist aviation Regulator. The CAA has specific responsibilities for air safety, economic regulation, airspace regulation, consumer protection and environmental research.

4.8 The transfer of functions will be enabled through primary legislation that will be subject to Parliamentary scrutiny and debate, and is not part of this consultation. The transfer would include the compliance and regulatory functions. The compliance function seeks to assess and improve levels of compliance with aviation security requirements through a programme of inspections, testing, audit and advice. The regulation function undertakes detailed rulemaking activity. This is expected to take place no sooner than 2013.

4.9 The CAA recovers its costs from the industry. Extending this to aviation security functions transferred from the Department is consistent with the 'user pays' principle, which is already applied to aviation safety and other aspects of aviation security (e.g. airport policing).

4.10 Following the transfer, the Secretary of State would:

- retain overall responsibility for aviation security
- remain the 'appropriate authority' responsible for coordinating and monitoring the implementation of the EU common basic standards
- retain responsibility for international negotiations and for relationships with the security and intelligence agencies
- remain responsible for the National Aviation Security Programme as required by the EU regulations and
- continue to issue aviation security directions to the industry, with advice from the CAA where applicable**.**

4.11 Bringing aviation safety and security functions within a single organisation potentially offers synergies. Transferring both regulatory and compliance functions would maintain close relationships between these functions. The Department and the CAA will work closely together to ensure aviation security functions continue to be delivered effectively during the transition.

What is a Safety Management System?

A Safety Management System (SMS) is a key component of the safety regulatory framework. This involves an operator setting out how it will deliver the specified safety outcomes that accord with the specific technical legal requirements. A SMS contains four key elements:

- the identification, assessment and mitigation of safety risk;
- the safety policy and objectives, including management accountabilities and responsibilities;
- safety assurance through regular reporting in terms of occurrences and performance, data analysis and review, internal and external audit, covert testing, and arrangements for continuous improvement; and
- safety promotion through training and communications.

A key part of this approach is the emphasis placed on operators to quality assure their own processes and show evidence that any problems are rectified promptly.

This approach accords with regulatory best practice. Furthermore, the regular information flow between the Regulator and the industry has fostered a transparent relationship which promotes a strong safety culture and continuous improvement in performance.

The regulatory approach for aviation security

4.12 The current approach to regulating aviation security is very prescriptive with careful scrutiny of inputs and processes. The prescriptive regulation and close monitoring of inputs has created an environment whereby there is no incentive to drive forward continuous improvement. In addition, it risks producing blind and reluctant compliance with the stipulated security process, rather than willing investment in delivering the right security outcomes.

4.13 An outcome focused, risk-based (OFRB) approach will incentivise continuous improvement as the Regulator will reward an effective security system with greater freedom in how specified security outcomes are delivered. Examples of how security outcomes could work in practice can be found at Annex C. Conversely, lower performance will incur increased scrutiny and direction from the Regulator and increased regulation costs.

4.14 The Department proposes to monitor performance through process assurance. This approach requires the industry to demonstrate that its security systems are effectively mitigating risks and can deliver the specified security outcomes.

The Security Management System

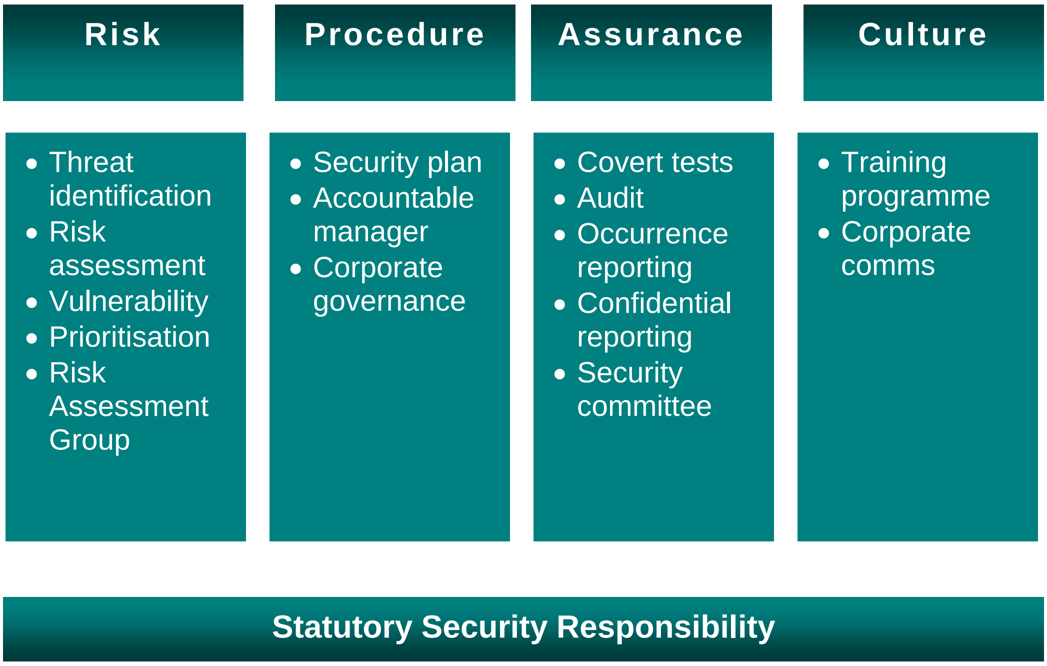
4.15 The Department believes the SMS concept outlined on page 13 can be readily transferred to aviation security. Indeed, the concept of a Security Management System (SeMS) is not new and is already being used by the CAA and the National Air Traffic Services to help protect specific infrastructure. A SeMS-based approach is also being introduced in Canada, and is already used by member airlines of the International Air Transport Association (IATA). Other states such as Australia, New Zealand and Japan are also considering adopting such an approach.

4.16 The key difference between safety and security is the identification of risk. Safety risk is comparatively static and the information which underpins safety risk analysis is widely shared and available to all operators. Security risk is driven by the ever changing threat picture, which is determined by threat and risk information provided by the Department based on information supplied by Joint Terrorist Analysis Centre (JTAC) and other Government agencies.

4.17 Such restricted information cannot be shared as widely as safety information, nor is it the responsibility of the industry to determine the threat picture. Consequently, we propose a variant of the approach in which the Department continues to have overall policy control, articulates the threat and risk picture and sets the security outcomes. As part of this, the Department proposes to issue guidance to the industry to include a list of priority risks which must be mitigated. The industry would be fully responsible and accountable for mitigating the prescribed risks. The Department will direct the industry under the ASA 1982 to have a SeMS containing the specified elements and apply it in such a way as to mitigate the risks as prescribed.

4.18 The SeMS concept is a dynamic management process, which is continually monitored and reviewed to take account of changes in the threat environment, organisational changes and the results of analysis. In-house quality assurance is vital in making this system work effectively. This is why we propose requiring the industry to have its own quality assurance system as an integrated part of the SeMS.

4.19 The SeMS concept can be seen to consist of four connected ‘pillars’: Risk procedure, assurance and culture, all of which are underpinned by a statutory security responsibility (see diagram below).



Risk	Procedure	Assurance	Culture
• Threat identification • Risk assessment • Vulnerability • Prioritisation • Risk Assessment Group	• Security plan • Accountable manager • Corporate governance	• Covert tests • Audit • Occurrence reporting • Confidential reporting • Security committee	• Training programme • Corporate comms

Statutory Security Responsibility

4.20 Under the proposed approach, those responsible for implementing the EU regulations and all directed parties under the ASA ('the industry') would be required to implement a SeMS – a structured system through which an operator plans and delivers its security processes. A SeMS demonstrates a clear commitment to provide an overall high standard of security and includes a number of key components:

- the assessment and mitigation of security risk[5]
- the security policy and outcomes, including management accountabilities and responsibilities
- the defining and recording of appropriate security measures to be implemented across the organisation
- security assurance through regular reporting in terms of occurrences and performance, data analysis and review, internal and external audit, covert testing, and arrangements for continuous improvement and
- security promotion through staff training and communications to deliver a strong security culture.

4.21 We think that this approach will bring improved security processes, benefiting both the industry and passengers. By enabling the industry to improve the integration of security measures within its own business model, and by creating incentives for good performance, it will be possible to deliver a better security outcome.

[5] Threat and Risk information will be provided by DfT based on information supplied by the Joint Terrorism Analysis Centre (JTAC) and other Government agencies.

4.22 This more flexible approach should also benefit passengers (if adopted by individual operators) as more integration of security systems with other business processes will save them time at the airport. There may be other opportunities for airports to integrate other security processes regarding landside and border control in conjunction with other security partners such as the Police and the UK Border Agency.

4.23 Attached at Annex A is more information of the structure of a SeMS and what it should include. This has been derived from the SMS approach to deliver a high degree of consistency to allow for a combined SMS/SeMS if desired. In this consultation we are not asking for comments on the detail but on the SeMS structure and whether it contains the necessary elements. The SeMS methodology and supporting documentation will be developed in further consultation with the industry and trialled at one or more operations before the new approach is implemented.

Question 1. Do you agree or disagree that a Security Management System (SeMS) is appropriate for aviation security? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Question 2. Do agree or disagree that the model of the Safety Management System (SMS), outlined on page 13, is a suitable foundation for a Security Management System (SeMS)? Are there any significant omissions you believe need to be taken into account? If so, what are they?

4.24 A key part of a SeMS is the assessment and mitigation of security threats. Government will always remain responsible for assessing the threats to aviation, overall policy based on threat and international obligations. Even under the new regulatory regime, Government will urgently direct security practices in the event of a new or heightened threat, or an attempted or successful attack. However the long term response to the changing threat picture, in terms of risk assessment and the designing of mitigation measures, will be for industry to establish. It is proposed that the Department will specify a number of key risks that will need to be mitigated (which will continually be monitored and updated) and it is then for the industry to do the next stage of the risk assessment - a local analysis of the vulnerabilities and impact, and the design of appropriate mitigation measures. It will be necessary for operators to establish a security committee or group which will oversee the internal quality assurance function of the security operation and decide on changes to the Security Plan. Where appropriate this role may be taken on by an existing security committee or group, such as the Risk Advisory Group (RAG) established under Part IIA of the ASA 1982, as amended by the Policing and Crime Act 2009. However in certain cases other structures may be more appropriate.

4.25 The requirement for a SeMS can be integrated with EU requirements. For example where an airport security programme, air carrier security programme and entity security programme meet the requirements on a SeMS, then that programme shall be capable of being the vehicle for delivering the security objectives set by the Regulator. Currently, the EU and the Department set the objectives and the specific means of delivery and the industry are required to have a security programme. Under an OFRB approach, initially for the UK's MSMs, there will be much greater flexibility in the means of delivery and the Security Programme (as long as it meets all the requirement of the SeMS) will be the principal delivery mechanism.

4.26 It is important to remember that this will be part of a 'live' process. Risk assessments should be kept under close review and adjusted in the light of experience, analysis and new information. Both the operator and the Regulator will assess the effectiveness of mitigating measures.

Question 3. Do you agree or disagree that industry is best placed for the risk assessment and design of appropriate mitigating measures? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Question 4. Do you agree or disagree that a Security Management System (SeMS) is the best system for delivering and integrating both EU regulatory requirements and outcomes of local risk assessments undertaken within an outcome focused, risk-based (OFRB) approach? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Approval arrangements for SeMS

4.27 Over time, the Government proposes that SeMS should become mandatory. Regulatory sign-off would be required to validate that an operator's first SeMS was suitable, and to permit it to move from the old system to the new. Thereafter the SeMS would be subject to regular audit.

Question 5. Do you agree or disagree that the first iteration of a Security Management System (SeMS) should be submitted to the Regulator for validation? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Proposals for an operator's statutory security responsibility

4.28 Moving to an OFRB approach to domestic aviation security regulation will give industry more scope to decide how to deliver aviation security outcomes with the Regulator setting out the risks to be mitigated, rather than processes that must be followed. The adoption of a SeMS provides a mechanism for operators to assess risks, design mitigations and monitor performance against security outcomes.

4.29 To underpin this approach, we are proposing that parties directed under the Aviation Security Act 1982 should have their responsibility to address security risks set out in security directions - a statutory security responsibility. This would provide complete regulatory cover not only for the specific security requirements set out in EU and domestic security regulations, but also steps taken to address any other security risks that they may identify.

4.30 An example might be:

An airport operator, in complying with his obligation under EU regulations to search x% of vehicles entering the Security Restricted Area (SRA) discovers a significant number of attempts to smuggle items using particular types of vehicle. The operator conducts a risk assessment and concludes that there is an increased risk that prohibited items could be brought into the SRA in this way. The operator decides to increase the percentage of vehicles checked, and/or to adapt the search process to include more checks of the relevant vehicles. This is implemented for an initial period of two months, after which the operator will review the vehicle search data and reassess the risk and establish an appropriate ongoing response.

4.31 The DfT is aware that some operators find that the restrictions of the current regulatory framework act to constrain them from addressing new or localised risks, such as described in the example above. The move to an OFRB approach removes many of those constraints, but the DfT believes that operators would benefit from having their ability and responsibility to respond to risks set out via directions. This would help to ensure that its limits are clear and that operators are acting lawfully and necessarily in addressing the risks. It could also help to offer protection against private claims for loss or injury for an alleged act of negligence by the operator and with negotiations around how the additional costs of such measures should be recouped.

Question 6. Do you agree or disagree that directed parties under the Aviation Security Act should be given a statutory security responsibility? Are there any significant considerations you believe need to be taken into account? If so, what are they?

The businesses affected

4.32 Initially we propose applying the OFRB approach to airports and airlines covered by the NASP and directions made under the ASA. The Department believes that these parts of the industry are best placed to make these changes (as many already operate a SeMS) and improve the passenger experience. The new approach will need to reflect the considerable difference in scale of operations and this consultation asks how this could best be done.

4.33 Once the new approach is embedded, which may take a number of years, it is intended to roll it out to other sectors of the aviation industry (i.e. cargo and in-flight suppliers). One option under consideration is whether those not required to follow the new approach initially, namely cargo and in-flight suppliers, may 'opt in' on a voluntary basis in advance of a full mandatory roll-out. This would involve the production of a SeMS and modifications to the MSMs as well as the inspection regime.

Question 7. Do you agree or disagree that airports and airlines should adopt the SeMS approach first, with cargo operators and in-flight suppliers being included at a later date? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Smaller businesses

4.34 We propose that all airports and airlines covered by the NASP will be required to implement all the components of a SeMS but the level of detail required will be proportionate to the scale of their operation.

Question 8. Do you agree or disagree that all airports and airlines covered by the National Aviation Security Programme (NASP) should be required to implement all the components of a Security Management System (SeMS) but with the level of detail required proportionate to the scale of their operation? Are there any significant considerations you believe need to be taken into account? If so, what are they?

The transitional arrangements

4.35 We propose phasing in the introduction of an OFRB approach over a number of years. This will help mitigate the risks associated with making such a change and give the industry sufficient time to develop and implement new security processes. However, there are many ways in which the change could be phased and compliance assessed. For example, the timetable for phasing could be linked to scale of operations as indicated below:

- from April 2013 – Category A[6] airports and large operators
- from April 2014 – Category B airports and medium-scale operators
- from April 2015 – Category C airports and smaller operators

4.36 Alternatively phasing could be based on a range of risk factors i.e. good performance under the existing regulatory arrangements.

Question 9. Do you agree or disagree that the timetable for transition, as indicated above, is realistic? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Reporting arrangements

4.37 A key feature of the OFRB approach would be mandatory reporting by the industry to the Regulator on its security performance. This would vastly increase the volume of performance data available to the security Regulator to gain a picture of the state of security measures in place. This could be done through

[6] Categories of airport are defined as follows:
Category A are those with more than 10,000,000 passengers p.a., Category B over 1,000,000 passengers p.a. and Category C are those with fewer than 1,000,000 passengers p.a.

quarterly reporting against a set of key performance indicators (KPIs), for example Threat Image Projection (TIP) and covert testing results. All airports and airlines covered by the NASP will be required to provide the Regulator with performance data but the level of detail required will be proportionate to the scale of their operation.

Question 10. Do you agree or disagree that reporting on key performance indicators (KPIs) could be a useful process in raising security performance? If you agree, what would represent an appropriate set of KPIs?

4.38 While there is an element of mandatory reporting already written into the current rules, it is mostly limited to the reporting of actual acts of unlawful interference with aircraft. The Department believes that there will be benefits from reporting certain serious lapses of security as well. This would allow the Regulator to establish whether there is a pattern of problems in the delivery of security that may need to be addressed more widely. It will also enable any operator who has discovered such a lapse to propose appropriate rectification measures to the Regulator, concentrating the joint effort on improving the delivery of security rather than punishing honest mistakes.

Question 11. Do you agree or disagree that rectification measures should be included in the reporting process? If you agree, should this form part of the initial incident report, or should rectification measures reporting take place at a separate time?

A culture of sharing best practice

4.39 Whilst airports and airlines will wish to compete with each other on price and quality of general service, it seems reasonable that they should be encouraged to co-operate in maximising security performance. At present there is no formal culture of sharing best practice and ‘lessons learned’ across the industry in relation to aviation security. For example, there is currently no industry-wide system for sharing information on maximising the performance of security officers. By developing fora in which this cross-industry dialogue could take place, ideas could be shared contributing to continuous improvement across the industry.

Question 12. Do you agree or disagree that there should be a mechanism for the industry to share best practice and lessons learned? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Confidential reporting by staff

4.40 The ability of staff to be able to report security concerns on a confidential basis provides an additional check on performance and another layer of assurance to the Regulator (and the public). The Department believes that all aviation staff should be able to raise their concerns regarding aviation security on a confidential basis and in the expectation that their report is properly investigated. Although the industry often has its own internal schemes for security matters, not all staff have access to such schemes. In contrast, an industry-wide scheme, the Confidential Human Factors Incident Reporting Programme (CHIRP), allows anyone working in the aviation sector to report any safety incidents confidentially. Further details on CHIRP can be found at Annex B. The Department considers it feasible to extend CHIRP to cover aviation security.

Question 13. Do you agree or disagree that there should be an extension of the Confidential Human Factors Incident Reporting Programme (CHIRP) scheme to cover aviation security? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Assessing compliance

4.41 The proposed approach moves away from assessing compliance through 'snap-shot' inspections towards continuous monitoring and improvement by the industry with process assurance on the effectiveness of the systems in place. Process assurance is a planned and systematic assessment of all actions undertaken to provide adequate confidence that a system meets established security outcomes.

4.42 The challenge will be defining a process that enables the Department to be satisfied that the industry's account of its own performance is credible and meets essential standards whilst ensuring that the UK's international obligations relating to aviation security are fulfilled.

4.43 In addition to a baseline level of monitoring, the new regulatory regime will operate a more risk-based approach, with more auditing and testing of poorer performers. The recovery of costs by the Regulator (post transfer to the CAA) from the industry may result in higher charges for those requiring greater regulatory scrutiny and direction, thus strengthening the incentive to improve performance as good performers will pay less once the system has bedded in.

Question 14. Do you agree or disagree that process assurance is an appropriate method of compliance? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Creating the right market incentives

4.44 The development of technological solutions for security issues is an important part of delivering robust and cost-effective security. Ideally, the driver behind technological development of aviation security systems is the industry, as it is best placed to see where possible technological solutions may improve efficiency and the passenger experience. The Department believes that the flexibility to innovate will provide an incentive for the market to develop a whole-systems security approach. Such systems integrate technology, information and process in the most efficient and passenger friendly way, consistent with maintaining high security standards. At the moment, such innovation is very difficult as the technology and process to be followed is a standard one set by the

Department. Demand for such solutions should create a market in which manufacturers of security equipment can compete.

4.45 The insurance market could also play a role in raising performance, as already seen in the safety field where insurers consider the quality of a SMS in setting the premium, with some refusing to insure if a SMS is not in place. The Department is also examining ways of bringing reputational effects into play that exist in other markets. Security considerations constrain what information on security performance can be released publicly. However, supplying information on performance and/or incident data, just to the industry, for example, could be a useful tool in raising standards. For example the CAA collates and supplies a digest of safety performance to specified individuals within the industry.

Question 15. Do you agree or disagree that the new regulatory approach gives greater scope for equipment manufacturers, the industry and process design specialists to work together to deliver whole-system security solutions? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Question 16. Do you agree or disagree that the Regulator should make security performance information available to other aviation industry operators? If so, what form should this take? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Accreditation

4.46 A key part of the OFRB approach is quality assurance which can be provided by covert testing, auditing, and the verification of technical processes. Under an OFRB approach, the demand for such services could be expected to increase as the industry improves internal quality assurance processes. An accreditation process by the Regulator would ensure an acceptable standard, and that tests were done on a common basis to ensure equivalence of performance data.

Question 17. Do you agree or disagree that providers of covert testing and other similar services should be accredited by the Regulator? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Staff training

4.47 A key element of the SeMS process is the promotion of security through training and communications. Currently the industry is required to provide training in line with the requirements of EU common basic standards and domestic legislation. An alternative OFRB approach would require the industry to provide a suitable training programme covering all posts with security responsibilities - satisfying EU common basic standards as appropriate. The suitability of the training programme and whether it is effective would be assessed in the monitoring process.

Question 18. Do you agree or disagree that training programmes should be reported against and monitored as part of the Security Management Systems (SeMS)? Are there any significant considerations you believe need to be taken into account? If so, what are they?

5. Impact assessment

5.1 An initial Impact Assessment is published alongside this consultation document and can be found at:

www.dft.gov.uk/consultations/open/

5.2 This includes examples where potential savings could be made under the new regulatory system.

Question 19. Do you agree or disagree that the Impact Assessment provides an accurate representation of the costs and benefits of the proposals? Are there any significant costs and/or benefits you believe need to be taken into account? If so, what are they?

6. Consultation questions

The Security Management System (page 14)

Question 1. Do you agree or disagree that a Security Management System (SeMS) is appropriate for aviation security? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Question 2. Do agree or disagree that the model of the Safety Management System (SMS), outlined on page 13, is a suitable foundation for a Security Management System (SeMS)? Are there any significant omissions you believe need to be taken into account? If so, what are they?

Question 3. Do you agree or disagree that industry is best placed for the risk assessment and design of appropriate mitigating measures? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Question 4. Do you agree or disagree that a Security Management System (SeMS) is the best system for delivering and integrating both EU regulatory requirements and outcomes of local risk assessments undertaken within an outcome focused, risk-based (OFRB) approach? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Approval arrangements for SeMS (page 17)

Question 5. Do you agree or disagree that the first iteration of a Security Management System (SeMS) should be submitted to the Regulator for validation? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Proposals for an operator's statutory security responsibility (page 17)

Question 6. Do you agree or disagree that directed parties under the Aviation Security Act should be given a statutory security responsibility? Are there any significant considerations you believe need to be taken into account? If so, what are they?

The businesses affected (page 18)

Question 7. Do you agree or disagree that airports and airlines should adopt the Security Management System (SeMS) approach first, with cargo operators and in-flight suppliers being included at a later date? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Smaller businesses (page 19)

Question 8. Do you agree or disagree that all airports and airlines covered by the National Aviation Security Programme (NASP) should be required to implement all the components of a Security Management System (SeMS) but with the level of detail required proportionate to the scale of their operation? Are there any significant considerations you believe need to be taken into account? If so, what are they?

The transitional arrangements (page 19)

Question 9. Do you agree or disagree that the timetable for transition, as indicated above, is realistic? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Reporting arrangements (page 19)

Question 10. Do you agree or disagree that reporting on key performance indicators (KPIs) could be a useful process in raising security performance? If you agree, what would represent an appropriate set of KPIs?

Question 11. Do you agree or disagree that rectification measures should be included in the reporting process? If you agree, should this form part of the initial incident report, or should rectification measures reporting take place at a separate time?

A culture of sharing best practice (page 20)

Question 12. Do you agree or disagree that there should be a mechanism for the industry to share best practice and lessons learned? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Confidential reporting by staff (page 20)

Question 13. Do you agree or disagree that there should be an extension of the Confidential Human Factors Incident Reporting Programme (CHIRP) scheme to cover aviation security? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Assessing compliance (page 21)

Question 14. Do you agree or disagree that process assurance is an appropriate method of compliance? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Creating the right market incentives (page 21)

Question 15. Do you agree or disagree that the new regulatory approach gives greater scope for equipment manufacturers, the industry and process design specialists to work together to deliver whole-system security solutions? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Question 16. Do you agree or disagree that the Regulator should make security performance information available to other aviation industry operators? If so, what form should this take? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Accreditation (page 22)

Question 17. Do you agree or disagree that providers of covert testing and other similar services should be accredited by the Regulator? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Staff training (page 22)

Question 18. Do you agree or disagree that training programmes should be reported against and monitored as part of the Security Management System (SeMS)? Are there any significant considerations you believe need to be taken into account? If so, what are they?

Impact Assessment (page 23)

Question 19. Do you agree or disagree that the Impact Assessment provides an accurate representation of the costs and benefits of the proposals? Are there any significant costs and/or benefits you believe need to be taken into account? If so, what are they?

7. What will happen next?

7.1 The consultation runs until 7th November 2011. During that time we shall be meeting with the industry to run through these proposals and answer any questions. If you are interested in these events see our website for more information, www.dft.gov.uk.

7.2 Please make sure your responses reach us by the closing date, as any responses received after that time will not be included. We will then consider all responses and publish a summary report along with next steps.

7.3 This section is followed by a questions and answers brief. If you have any further enquiries not addressed in this document please contact us:

- *telephone*
  020 7944 2692

- *email*
  avsec.reform@dft.gsi.gov.uk

- *post*
  Better regulation for aviation security consultation
  The Department for Transport
  25/1 Great Minster House
  76 Marsham Street,
  London
  SW1P 4DR

8. Questions and answers

8.1 Below is a list of frequently asked questions about these proposals. If you still have questions after you have read this section please contact:

- *telephone*
  020 7944 2692

- *email*
  avsec.reform@dft.gsi.gov.uk

- *post*
  Better regulation for aviation security consultation
  The Department for Transport
  25/1 Great Minster House
  76 Marsham Street,
  London
  SW1P 4DR

What does 'outcome focused, risk-based' regulation actually mean and how would it work in practice?

Aviation security requirements are set out in directly applicable EU regulations and in directions made under the Aviation Security Act 1982 (ASA). Compliance with these requirements is assessed through a programme of inspections, testing and audits, delivered by the Department and funded by the taxpayer.

Under the proposed outcome focused, risk-based (OFRB) approach the Department would specify the outcomes it wants achieved e.g. prohibited items that must be prevented from being taken onboard an aircraft. It would be for the industry to design and implement the necessary processes to deliver this outcome, ensuring compliance with existing EU regulations and UK directions.

The industry would be legally required to quality assure the process, monitor the performance of its process and report this to the Regulator along with any serious lapses (possibly including the rectification measures that have been put in place to prevent reoccurrence). During the auditing process, the Regulator would look for evidence that prohibited items had been prevented from entering the aircraft. If the Regulator concluded that inadequate processes were in place, it could ultimately direct detailed processes.

Does this approach replace the European requirements and the UK's More Stringent Measures (MSMs)?

The EU common basic standards will still apply. This approach may provide more flexibility in how some of those obligated requirements are delivered. An OFRB approach will apply to the UK's MSMs some of which build on EU common basic standards.

How can I make savings given that the EU common basic standards will still apply?

The industry will have more flexibility in how it delivers the UK's MSMs. One of the aims of this proposed regulatory reform is to provide individual businesses with greater ownership of security considerations and give them greater freedom to integrate security within their day-to-day business activities. The extent of any savings will be totally dependent on the industry's ability to innovate and develop efficient security processes that are centred around improving the passenger experience.

I am going to face additional costs as a result of the transfer of security functions to the Civil Aviation Authority (CAA). Will the introduction of an outcome focused, risk-based approach to regulation allow me to recoup these extra costs?

Provided all relevant EU and domestic requirements are complied with, businesses will be provided with the freedom to develop security processes. This will provide opportunities to deliver savings greater than the additional security costs that will arise from the transfer of functions to the CAA. Whether an individual business does so depends on how they embrace the opportunities being offered and the extent to which they innovate.

What is a Security Management System (SeMS)? And what will I need to do to produce one?

A SeMS is a dynamic management process, which is continually monitored and reviewed to take account of changes in the threat environment, organisational changes and the results of analysis. Annex A provides a summary of the proposed structure. Following further consultation with industry guidance will be issued.

How will my SeMS be assessed?

Your SeMS will be routinely audited. Regulatory sign-off would be required to validate that an operator's first SeMS was suitable, and to permit it to move from the old system to the new.

Will I be able to introduce new technological approaches without the Regulator's approval under the new approach?

We propose to facilitate the introduction of new technological approaches provided the industry and the Regulator are satisfied that the process delivers the intended security outcome.

How much will it cost me to produce and implement a SeMS?

This will vary from business to business depending on the complexity and scale of operation, and the extent of SeMS components already in place. Many operators already have some components in place such as risk management, internal reporting, in-house and external audits. In these cases a SeMS would therefore just formalise the existing arrangements.

Will this approach be extended to the rest of the aviation sector?

Initially it is proposed to introduce the OFRB approach for UK airports and all airlines covered under the National Aviation Security Programme (NASP). Once the new system is embedded it is intended to roll out the new regulatory model to other entities within the aviation sector (e.g. cargo and in-flight supplies).

The Department is also considering whether to allow the industry to opt into OFRB on a voluntary basis, where it would be beneficial to do so. The Regulator would also need to be satisfied the necessary security outcomes could realistically be met. This could be based on performance under the existing regulatory regime.

What data will I need to supply to the Regulator?

This is still to be decided and is subject to the outcome of this consultation. The intention is to establish a working group to work out these details taking account of the consultation responses.

How will my performance and Mandatory Occurrence Reporting (MOR) data be used by the Regulator?

The performance data supplied will be combined with other sources of information (e.g. covert testing results) to assess performance and help inform the level of compliance activity required. It is not envisaged that the MOR data would be used in the same way (as this may discourage the supply of such information) as the performance data. Instead the MOR data would be used to assess policy and to inform the industry of the kind of problems to avoid.

How can performance data supplied by the industry itself be relied upon?

Non-reporting of specified incidents or falsifying returns will be a criminal offence. In any case, the Regulator will not be judging performance solely on the performance data supplied. Other information will be taken into account, e.g. the Regulator's covert testing results, and observation-based inspections of the type that are already carried out. All operators will be audited by the Regulator.

What happens if an airport or airline is not delivering to the required standards under the new approach?

At present the security Regulator has powers to impose special measures on any individual industry operator including supervision. This would not change under the new approach. However, following the transfer of security functions to the CAA, the cost of any extra regulatory resource required would be met by the operator concerned, and not the taxpayer as is currently the case.

As a passenger how will the new proposals affect me when I go through airport check-in?

It will depend on the approach taken by the airport operator. All airports are required to provide a high level of security in accordance with EU and UK legal requirements but with an OFRB approach they will have more flexibility in how they deliver those requirements. This could mean that passengers are subject to different arrangements when travelling from different airports. Airports are private businesses and the Department believes it should be up to them to decide how to deliver security outcomes.

How will you ensure that security standards do not fall as the industry uses the opportunity to cut costs?

The Industry will still be required to meet the existing legal standards, set in out in EU common basic standards and in UK directions. Furthermore, the new approach incentivises continuous improvement, as higher performance would reduce the level of compliance activity required by the Regulator (which would be charged for) and insurance premiums could be lowered as a result of strong performance.

Who is legally responsible for delivering security under the new regulatory model?

The EU common basic standards are directly applicable to all Member States. UK MSMs are set out in directions made under the ASA which specify the directed parties responsible for ensuring compliance with security measures. This will not change under the move to an OFRB approach.

Does the day-to-day transfer of functions from the Department to the CAA mean that the industry will be charged by the Regulator?

Yes, in line with the ‘user pays’ principle. The details around the charging mechanism are still to be decided. It is expected that the introduction of the OFRB approach will provide individual businesses with the opportunity to make savings in excess of the extra costs.

Isn’t this just cost-cutting?

No, this is about maintaining and improving security performance whilst adhering to best practice in regulation. It also allows operators to optimise their security processes by designing a bespoke service centred around their business needs and the passenger experience.

How can the public be assured that effective security will be delivered by the industry?

The security outcomes surrounding aviation security have not changed. The proposed OFRB approach will incentivise continuous improvement in security performance. The Regulator will have in place a robust monitoring framework.

Furthermore, the industry will be legally required (for the first time) to report regularly on performance and certain occurrences to the Regulator, enabling the Regulator to have a greater picture of performance than under the current approach.

Will you have sufficient auditors/inspectors to check the aviation industry?

Yes. The CAA will be responsible for the inspection of the industry rather than the Department, following the transfer of security functions. The OFRB approach will allow the CAA to deploy their regulatory resources more efficiently. Furthermore, the CAA will be able to optimise the level of inspections to meet requirements and recoup the costs from the industry.

Who will be responsible for determining the threat from terrorism?

Threat and Risk information will continue to be provided by the Department based on information supplied by the Joint Terrorism Analysis Centre (JTAC) and other Government agencies.

CAA is a non-security specialist. Won't this hamper its ability to regulate security effectively?

No. It is hoped that all parties will be able to benefit from the CAA's operational focus and experience. Posts in aviation security within the Department at present will be transferred to the CAA (subject to legislation). Furthermore, the Department will work closely with the CAA during the transition to build up the necessary security expertise within the CAA.

9. The consultation criteria

9.1 The consultation is being conducted in line with the Government's Code of Practice on Consultation. The criteria are listed below. A full version of the Code of Practice on Consultation is available on the Better Regulation Executive website at: http://www.bis.gov.uk/files/file47158.pdf

9.2 If you consider that this consultation does not comply with the criteria or have comments about the consultation process please contact:

Consultation Co-ordinator
Department for Transport
Zone 2/25, Great Minster House
76 Marsham Street
London SW1P 4DR

Email address consultation@dft.gsi.gov.uk

The seven consultation criteria

When to consult: formal consultation should take place at a stage when there is scope to influence the policy outcome.

Duration of consultation exercises: consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.

Clarity of scope and impact: consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.

Accessibility of consultation exercises: consultation exercises should be designed to be accessible to, and clearly targeted at those people the exercise is intended to reach.

The burden of consultation: keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.

Responsiveness of consultation exercises: consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.

Capacity to consult: officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

10. List of consultees

This consultation will be of most interest to all entities directed under Part II of the Aviation Security Act 1982 but will also be of interest to:

- Aviation representative organisations
- International aviation bodies
- Security service providers and equipment manufacturers

11. Glossary

Audit - a systematic check or assessment, professional advice service and assurance; especially of the effectiveness of systems or processes, typically carried out by an independent assessor.

Better regulation - adherence to the principles laid down by the Better Regulation Executive. These principles provide a framework for good regulation: transparency, accountability, proportionality, consistency and targeting. This reflects the Coalition desire to *"end the culture of 'tick-box' regulation, and instead target inspections on high-risk organisations through co-regulation and improving professional standards."*[7]

Civil Aviation Authority (CAA) - a public corporation, established by Parliament in 1972 as an independent specialist aviation Regulator and provider of air traffic services. The CAA is the UK's independent specialist aviation Regulator. Its activities include economic regulation, airspace policy, safety regulation and consumer protection. The UK Government requires that the CAA's costs are met entirely from its charges on those whom it regulates

Confidential Human Factors Incident Reporting Programme (CHIRP) - the aim of CHIRP is to contribute to the enhancement of aviation and maritime safety in the UK by providing an independent and confidential (not anonymous) reporting system for all individuals employed in or associated with these industries. CHIRP welcomes safety-related reports from flight crew, air traffic control officers, licensed aircraft maintenance engineers, cabin crew, and the general aviation community.

Compliance - seeks to assess whether the industry is meeting its legal requirements through a programme of inspections, testing, audit and advice.

'Direct and Inspect' - an approach to regulation whereby the Regulator specifies detailed requirements and processes and then verifies adherence with these through a programme of inspections, testing, audit and advice.

End user - the person, group or organisation directly using a product or service. In the case of airports and airlines this would be the passenger.

Joint Terrorism Analysis Centre (JTAC) - analyses and assesses all intelligence relating to international terrorism, at home and overseas. It sets threat levels and issues warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies, as well as producing more in-depth reports on trends, terrorist networks and capabilities.

Key performance indicators (KPI) - a set of quantifiable measures that a company or industry uses to gauge or compare performance in terms of meeting its strategic and operational goals. In the case of airports and airlines these will likely be based on meeting security outcomes defined by the Regulator.

[7] http://www.cabinetoffice.gov.uk/news/coalition-documents

National Aviation Security Programme. (NASP) - article 10 of Regulation (EC) No 300/2008 on common rules in the field of civil aviation security states that, '*Every Member State shall draw up, apply and maintain a national civil aviation security programme. That programme shall define responsibilities for the implementation of the common basic standards referred to in Article 4 and shall describe the measures required by operators and entities for this purpose.*'

Outcome Focused, Risk-Based (OFRB) Approach - is about the aviation industry being able to design its own security systems informed by risk which focus on delivering robust security outcomes rather than following detailed processes set by the Regulator.

Mandatory Occurrence Reporting (MOR) - a formalised system whereby the industry is required to report on certain operational lapses.

More Stringent Measures (MSMs) - security measures applied by the UK on the basis of a risk assessment that are more stringent than the EU common basic standards, as permitted under Article 6 of Regulation (EC) 300/2008.

Process assurance - the monitoring of processes and systems to ensure they are robust enough to deliver the specified security outcomes. Monitoring would be largely audit-based but could be complemented by observational inspections.

Risk Advisory Group (RAG) - an airport operator of a UK airport regulated as part of the NASP is legally required to ensure that a RAG is established. Its role is to assess risks to the airport and make recommendations to the airport's SEG.

Security Management System (SeMS) - a SeMS is a dynamic management process, which is continually monitored and reviewed to take account of changes in the threat environment, organisational changes and the results of analysis.

Safety Management System (SMS) - producing an SMS is a key component of the safety regulatory framework. This involves an operator setting out how it will deliver the specified safety outcomes that accord with specific technical and legal requirements.

Threat Image Projection (TIP) - a program to test individual x-ray operator performance and can inform training programs appropriately.

'**User pays' principle -** the principle that a user of a service or resource pays directly for the amount they use, rather than the cost being shared by all the users or a community equally.

Annex A

The Structure of a Security Management System (SeMS)

Introduction

1. This document provides guidance on the implementation of a SeMS for airports and airlines. The guidance is designed to give the reader basic information on SeMS concepts and the development of management policies and processes. The concepts and principles are very similar to those for the Safety Management System (SMS) already used in the aviation sector.

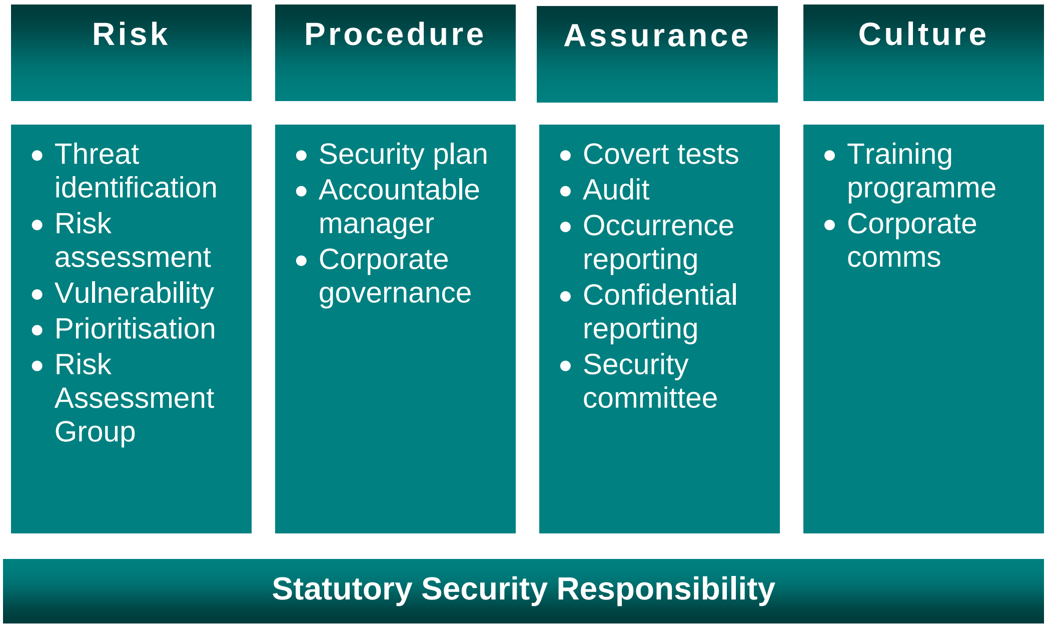
2. A SeMS is not merely a document to show to the auditors/Regulator but is a dynamic management process, which is continually monitored and reviewed to take account of changes in the threat environment, organisational changes and the results of analysis. It is a formal and risk driven way of integrating security into an organisation's day to day operations and general management systems. SeMS should be used to plan, implement and evaluate the organisation's security policy and to fulfil any regulatory requirements while managing security threats, impacts and risks in the context of the overall management framework. SeMS is performance based and focuses on setting achievable security results that are measurable and auditable by the Regulator and/or third party assessors.

3. The SeMS will be a way of delivering both the baseline regulatory requirements, such as EU common basic standards, and Directions made under the Aviation Security Act 1982 (ASA) which form the UK's More Stringent measures.

4. A SeMS highlights the benefits of a whole systems approach that traditional approaches to security cannot achieve (often based on relatively standardised prescriptive security measures set out in relevant legislative provisions). The benefits of a SeMS can be described as:

   - dynamic and 'live' i.e. tailored to the organisation and responding to a fluctuating threat picture in a risk-based way
   - comprehensive and integrated i.e. attuned to the operator's and passengers' needs
   - risk driven i.e. security programmes and countermeasures are based on careful analysis and priority ranking of risks
   - results focused and performance based i.e. based on desired security results and goals rather than on prescriptive measures to be implemented.

SeMS architecture



Risk

- Threat identification
- Risk assessment
- Vulnerability
- Prioritisation
- Risk Assessment Group

Procedure

- Security plan
- Accountable manager
- Corporate governance

Assurance

- Covert tests
- Audit
- Occurrence reporting
- Confidential reporting
- Security committee

Culture

- Training programme
- Corporate comms

Statutory Security Responsibility

Risk

5. Central to the SeMS process is a robust mechanism to identify, assess and successfully mitigate risk. Threat and risk information will be provided by the Department, based on the Common Threat Assessment (CTA) produced by the Security and Intelligence Services, and updated from time to time. It will then be for the operator to conduct a comprehensive risk assessment taking into account the CTA as well as local risks, vulnerabilities and priorities. This risk assessment process should be conducted by a group specifically designed for this purpose. Where appropriate, industry may wish to adapt existing processes or established groups in order to fulfil this requirement (such as the Risk Assessment Group at airports). Operators should be familiar with similar processes as utilised in the Airport Security Planning guidance (for landside security measures).

Procedure

6. The organisation should define the accountabilities of the Accountable Manager and the security responsibilities of key personnel. It is essential that security management is seen as an integral strategic aspect of the organisation's business by assigning the highest priority to security. With this in mind, there has to be a demonstrable board level commitment to producing and delivering an effective SeMS.

7. A management system should describe the structure of the organisation, available resources, staff accountabilities and responsibilities and how decisions are taken and managed throughout the organisation.

8. The Security Plan sets out the detailed security processes to be followed by staff within the organisation.

Assurance

9. The operator will need to implement assurance processes in order to swiftly detect and rectify deficiencies. Deficiencies could arise in two situations: non-compliance by the operator's staff with the detailed processes set down in the Security Plan; or an assessment that these processes are no longer effective in mitigating the range of threats faced.

10. This would be backed up by significantly increased reporting requirements. This means that the industry itself would regularly report on its own security performance, significantly increasing the volume of performance data available to the security Regulator. The Regulator will continue to gather its own data such as undertaking covert tests. The SeMS will also be audited by the Regulator on a regular basis.

11. The SeMS must contain clear structures that demonstrate the strategic aspects of the operation as well as the processes and procedures in place in order to enable the Regulator to audit the operation.

12. The reporting of certain serious lapses would be mandatory (comparable to safety incident reporting in industry). We also propose to extend the CHIRP confidential reporting system to cover security. All entities that are required to comply with EU common basic standards and domestic legislation will of course continue to have to do so.

13. There will also be a framework of measures or indicators against which performance is constantly assessed. These will be agreed with the Regulator and will be linked to the security outcomes that the operator is accountable for delivering. These could take the form of Key Performance Indicators (KPIs).

14. It will be necessary for operators to establish a security committee or group which will oversee the internal quality assurance function of the security operation and decide on changes to the Security Plan. Where appropriate this role may be taken on by an existing security committee or group.

Culture

15. The Department's aim is to promote a robust security culture throughout the aviation industry. There would be a requirement for industry to provide a suitable training programme covering all posts with security responsibilities - satisfying EU common basic standards as appropriate. The suitability of the training programme and whether it is effective would be assessed in the monitoring process. An operator should ensure that the SeMS is robust enough to identify security gaps when they occur and therefore drive forward a continuous improvement of the security operation. And there should be a

communications programme designed to raise staff awareness about the importance of high standards of security.

Annex B

A proposal for the establishment of a confidential reporting programme for aviation security staff

Summary

1. Incident reporting systems have proved to be valuable tools for identifying procedural and systematic weaknesses, and promoting the implementation of appropriate corrective actions.

2. We believe it would be beneficial to establish a confidential reporting programme for aviation security using the existing aviation safety reporting programme (Confidential Human Factors Incident Reporting Programme or CHIRP) as a model.

3. The existing CHIRP organisation has indicated that they are willing to consider establishing an independent confidential security reporting system mirroring the existing safety programmes.

4. We believe that a confidential reporting system for aviation security would work well with the OFRB approach, providing an additional reporting mechanism alongside mandatory occurrence reporting and regulatory reporting requirements. The programme would be available to all aviation security posts, as well as aviation industry employees.

What is the aim of Confidential Reporting?

5. The aim of the CHIRP is to contribute to the enhancement of aviation and maritime safety in the UK by providing an independent and confidential (not anonymous) reporting system for all individuals employed in or associated with these industries.

6. CHIRP welcomes safety-related reports from flight crew, air traffic control officers, licensed aircraft maintenance engineers, cabin crew, and the general aviation community. The maritime programme includes individuals in the shipping industry, fishing industry and leisure users.

7. Reporters' identities are kept confidential. Personal details are not retained and are returned to the reporter or destroyed on closure of their report. The information provided is made available, with the approval of the reporter, and in a disidentified form to those who can take action to remedy the problem. Important information gained through reports, after being disidentified, is also made as widely available as possible, principally through regular feedback publications.

8. The CHIRP aviation safety programme complements the Civil Aviation Authority (CAA) Mandatory Occurrence Reporting scheme. Both aviation and

maritime programmes also complement other formal reporting systems operated by many UK organisations by providing a means by which individuals are able to raise issues of concern without being identified to their peer group, management, or the Regulator. Anonymous reports are not normally acted upon as they cannot be validated.

The role and benefits of a confidential reporting system

9. A confidential reporting system can:

- provide a reporting function that complements the current compliance regime
- supplement company and regulatory reporting schemes
- receive security related information from aviation security professionals
- permit reporting of incidents and situations without the attachment of blame
- provide non attributable information to management and regulatory agencies
- provide feedback to the reporter(s)
- provide feedback on dis-identified reports circulated to industry representatives (the CHIRP aviation safety programme has a circulation of around 30,000)
- provide feedback that would help create awareness of security issues that would be of interest to the industry, and possibly provide a forum for discussion
- provide a database of incidents and observations for analysis and identification of trends etc.

Essential requirements for an effective system

10. To be successful, a confidential reporting system has several requirements including:

- the need to be appropriate to national and professional culture
- senior management commitment to the process
- proven independence
- a process respected by regulatory and management groups
- effective methods of disseminating information and
- the ability to maintain the confidentiality of the reporter.

What happens when a report is received?

11. Once received, reports are validated as far as possible and reviewed with the objective of making the information as widely available as possible (with appropriate consideration of security sensitivities), while maintaining the confidentiality of the source. Anonymous reports are not normally acted upon as they cannot be validated. When appropriate, report information is discussed with the relevant body (airport operator management/airport operator senior management/Regulator, etc) with the aim of finding an

effective resolution.

12. Only depersonalised data are used in discussions with third party organisations and the confidentiality of the reporter is assured in any contact with an external organisation.

13. No personal details are retained from reports received. After ensuring that the report contains all relevant information, all personal details are returned to the reporter with an acknowledgement letter. Each report is allocated a unique reference identification. After the return of personal details, CHIRP is unable to subsequently contact the reporter. The reporter may, if he/she wishes, contact the CHIRP office for additional information by using the report reference identification.[8]

[8] http://www.chirp.co.uk/

Annex C

Examples of how an outcome focused, risk-based approach could work in practice

In the following *fictional* examples the current regime is compared to the theoretical equivalents of an outcome-focused, risk-based approach.

Example 1

Current regime	***Outcome focused, risk-based approach***
C4.1 Re-screening of departing passengers • All alarms from a walk-through metal detector shall be resolved by a hand search. • Where a type 256 walk through metal detector is in use, the footwear of at least x% of passengers selected at random shall be screened, in addition to the hand search. • Where a type 278 walk through metal detector is in use, the footwear of at least x% of passengers selected at random shall be screened, in addition to the hand search. • Footwear shall be screened either by: o removing and inspecting o type AS359 explosive trace detection equipment o type 789-H6 footwear screener o type HT56 cabin baggage x-ray. • Where a security scanner is used in an addition to screening by walk through metal detector and hand search, the scanner must be of type ST78 or GH890.	**C4.1 Re-screening of departing passengers** • Subject to the requirements of the EC common basic standards, Aerodrome Managers shall ensure that the frequency and method of all re-screening, all footwear screening and all secondary screening is done on the basis of a risk assessment. All methods used shall satisfy a detection standard recognised by the DfT. Commentary This new rule would allow airport operators to determine, within the requirements of EU common basic standards, the frequency and method for re-screening, footwear screening and secondary screening of passengers on the basis of a risk assessment. It also enables any method to be used, provided that it satisfies a detection standard recognised by the DfT e.g. ECAC, EU standards.

Example 2

Current regime	*Outcome focused, risk-based approach*
C8.1 Recruitment checks on staff • Directed parties shall ensure that staff undertaking security work, or working within security restricted areas, produce a criminal record certificate. • Where a person does not provide a valid criminal record certificate he or she cannot undertake security work or have access to the security restricted area unless the person meets the alternative requirements to a criminal record certificate set out in Article C. • Where a person's criminal record certificate lists a conviction set out in Schedule 1 (*note: this schedule contains a detailed list and disqualifying offences and the disqualifying criteria*), and the Secretary of State has not issued a notice of exemption in respect of that conviction, that person cannot undertake security work or have access to the security restricted area. The procedure and form to be used in applying for a notice of exemption is set out in Schedule 2. • Employers shall ensure that written confirmation is obtained from employers, educational establishments or other sources capable of verifying the information provided by the member of staff. • Where a person was self employed during any of the period covered by the check, written confirmation of the dates of the periods shall be obtained from independent	**C8.1 Recruitment checks on staff** • Subject to the requirements of the EC regulations, working in security restricted areas, shall pass a test of criminal records which satisfies the airport operator that the person is suitable to hold a pass. Details of the criminal record test, including the criteria used to assess staff, shall be made available to staff at the point that they make their application. • Employers shall obtain, verify, record and retain confirmation of the employment or educational history, including any periods of self employment and unemployment, of all staff members undertaking security work or working in a security restricted area. The information obtained shall be used to prevent a person who, in the opinion of the employer or directed party, is unsuitable to undertake such work. Commentary This new rule will enable the directed party to determine their own systems and processes for applying a test to the criminal history as part of the recruitment checking of airport staff. It removes several pages of detailed regulation. This rule would also provide employers with more flexibility as to how they verify the employment history of staff deployed on security work or working in security restricted areas.

accountants, solicitors or from the relevant government department or agency. • Where a person was registered unemployed during any of the period covered by the check, verification of such periods of registered unemployment shall be obtained from the relevant government department or agency.	Employers and directed parties will be in a position to make judgments on whether to deploy persons into particular roles on the basis of their assessment of the criminal history and employment history information. There is much published guidance on this, including from the Centre for the Protection of National Infrastructure, the Metropolitan Police Service and reputable bodies such as the British Standards Institute.