Equipment, Support, and Technology for UK Defence and Security: A Consultation Paper

Equipment, Support, and Technology for UK Defence and Security: A Consultation Paper

Presented to Parliament
by the Secretary of State for Defence
By Command of Her Majesty

December 2010

Cm 7989 **£14.75**

© Crown copyright 2010

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence/ or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or e-mail: psi@nationalarchives.gsi.gov.uk.

Any enquiries regarding this publication should be sent to us at

Green Paper Consultation Enquires
DGDC
5.N.25
MOD Main Building
Whitehall
London
SW1A 2HB

or

E-mail: DGDCSecIP-Consultation@mod.uk and start your subject as "Enquiry"

This publication is also available on http://www.official-documents.gov.uk/

ISBN: 9780101798921

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID P002405833 12/10

Printed on paper containing 75% recycled fibre content minimum.

Foreword

We are very pleased to begin formal consultation on how the UK Government should acquire equipment, support, and technology for UK defence and security. This Green Paper follows on from the Strategic Defence and Security Review and is part of the process of developing a White Paper on these issues to be published in 2011.

This Green Paper ranges across many important issues and we therefore hope that many individuals and organisations will contribute to the debate.

Peter Luff MP

Minister for Defence Equipment, Support and Technology

The Rt Hon Baroness Neville-Jones DCMG PC

Minister of State for Security and Counter Terrorism

Executive Summary

i. The security of our nation is the first duty of Government. The UK today faces a different and more complex range of threats than it did in the last century, so we have a different, more wide-ranging approach to handling them, as we set out in our National Security Strategy earlier this year. The most serious potential dangers are from international terrorism, hostile attacks upon UK cyberspace, a major accident or natural hazard, or an international military crisis. But there is a much broader range of other risks as well. So it is essential that the UK equips itself with the right tools to tackle current and future threats.

ii. This means the Government must have access to the critical technologies and skills that underpin the UK's national security capabilities, so that we can ensure our Armed Forces, the wider National Security community, and the Law Enforcement agencies are given the training, equipment, and support that they need to operate effectively. But this must also be at a reasonable cost to the tax-payer, especially given the economic situation we face.

iii. To achieve this, the Government needs to be clear about how it plans to:

- acquire the equipment it needs;
- support that equipment and its users; and
- invest in or acquire the necessary technologies to secure these objectives both now and in the future.

iv. Our default position is to use open competition in the global market, to buy off-the-shelf where we can, and to promote open markets in defence and security capabilities. We will take action to protect our operational advantages and freedom of action, but only where essential for national security.

v. The more clarity and certainty the UK can give about its intentions, the more confidence we will create around the value of investment in research and production in the UK. This is important because our suppliers also have choices about where to conduct their business, which can be a national security issue, as well as having broader economic consequences for the UK. But that clarity and certainty will, we anticipate, not always be welcome. At a time of very tight financial constraints, we cannot afford to spend taxpayers' money on anything that is not absolutely necessary to protect our nation.

vi. The Strategic Defence and Security Review (SDSR) began the process of defining our needs and our future approach to these issues. This Green Paper takes the next step, beginning the process of consultation on our future policy towards them.

vii. The last Government published a Defence Industrial Strategy in 2005 and a Defence Technology Strategy in 2006. We believe that the thinking behind these documents needs to be rethought significantly in the light of our new National Security Strategy and set more firmly in the current challenging context of affordability.

viii. That challenge has already driven some difficult decisions with regard to defence capabilities; many contracts are being renegotiated and a thorough programme of review will follow for those that remain. The so-called 'Yellow Book', which sets the terms for non-competitive contracts, is being reviewed. Tough targets have been set for financial savings at MOD and this is one of the reasons why the department remains committed to off-

the-shelf procurement wherever possible. As set out in 'The Path to Strong, Sustainable, and Balanced Growth', one of the key challenges for the Government is securing benefits from acting as a more intelligent customer in sectors where it is a major purchaser and can promote innovation. It is against that background that this consultation is being conducted and our future relationship with industry will be viewed.

ix. We believe that the convergence of defence and security that underpinned the SDSR - and is reflected in the commercial responses of many companies who are moving from defence into more general security - means that we should seek to bring together in one document our approach to equipment, support, and technology in both the defence and security sectors. This Green Paper is the first manifestation of an integrated approach that we expect to develop further in the future.

x. We have included cyber security as a separate section because it is a new and fundamental challenge. Cyberspace pervades the modern world and affects nearly every aspect of our lives. It is a factor in our national security, but also in our economic prosperity. It is therefore one of the principal benefits of the modern world, but also one of the biggest risks unless managed effectively.

xi. We recognise that the market in defence and security capabilities is unusual, because it is heavily influenced by national security and diplomatic factors, as well as other countries' national interests. A key priority, therefore, is identifying the handful of critical areas where the UK has or needs an operational advantage and freedom of action for a particular capability, where we may have to take action to sustain the underpinning technologies and skills in order to protect our national security. To achieve this, especially at a time of financial challenge, may involve encouraging innovative approaches to and opening up wider markets for important capabilities. It may also require acceptance of greater mutual dependence on some of our key allies.

xii. This is one of the reasons we are committed to doing more to promote exports of both defence and security products from the UK to responsible nations, as well as to boost the role of small and medium sized enterprises, both in their direct and indirect supplies to the Government and its agencies. We will strengthen the machinery to assist companies to export world-class products and ensure that the UK's defence and security requirements are set with exportability in mind. The Government is proactively supporting business and commercial diplomacy internationally, understanding the importance of exports to the strengthening of the British economy. The Government has taken strides to elevate our links with many international partners across the spectrum of this activity and has made clear that this includes defence and security. The Government is keen through this process to secure the views of industry on how this can be achieved most effectively.

xiii. We are clear that spending on defence and security capabilities must be for the sole purpose of protecting our national security. However, there are wider benefits from having competitive and viable technological and industrial sectors in the UK: participation in international programmes and successful exports help build relationships with and capacity in other countries, as well as contributing to UK growth. These sectors can, therefore, help to sustain our security and diplomatic objectives, as well as our economic ones.

xiv. There are some areas in which policy decisions have already been taken – for example, the UK has recently signed treaty undertakings with France in defence acquisition that we are determined to drive ahead quickly. In other areas, we are open to alternative approaches. So parts of this Green Paper contain statements of policy, whilst others are more consultative in nature. There is also parallel work underway on acquisition reform in

defence. We do want to encourage the most open consultation possible - and will listen to all the suggestions and challenges we receive. The seriousness of both our security and financial situation demands that.

xv. We look forward to the consultation that begins with the publication of this Green Paper and to developing a soundly-based approach to equipment, support and technology for UK defence and security for the period between now and the next SDSR in 2015. We will publish this as a White Paper in 2011.

Part One: Overview

1.1: Introduction

1. The first duty of Government is to safeguard our national security. We have, therefore, published our National Security Strategy (NSS), which sets out the context in which we operate and our goals; and conducted the first Strategic Defence and Security Review (SDSR), which sets out how we will achieve those goals.

2. Two key factors in delivering the SDSR will be: our ability to understand and use technology to give the UK an advantage when confronting threats; and our ability to get the best from our suppliers – the advanced engineering and specialist services companies that provide much of the equipment and support for the national security apparatus in this country. The Government is, therefore, proposing that the United Kingdom should have, for the first time, a formal statement of our approach to equipment, support, and technology in both the defence and security areas.

3. This Green Paper marks the start of public consultation on that policy. It is in four parts:

   Part One is an overview of the context and the Government's current thinking, including our proposed key principles.

   Part Two discusses the key cross-cutting equipment, support, and technology issues that will shape the formulation of our specific policy choices in the defence and security sectors. It looks at how national security requirements shape technology and procurement choices and at broader policy issues.

   Part Three focuses on specific issues related to defence and security, as well as the emerging cyberspace domain. Short summaries highlight their importance and the challenges they pose.

   Part Four gives details of how to take part in this consultation and provides the opportunity for all interested parties to get involved in helping us to develop this policy. Throughout this paper we are asking questions about both our general approach and about specific issues. We welcome your views on these points and on any other matters that you believe should be considered.

4. Once consultation is complete next spring, we intend to publish a White Paper setting out our approach to equipment, support, and technology issues in the defence and security areas until the next strategic review, which is scheduled for 2015.

1.1.1 Strategic background

5. In October 2010, the Government published the NSS and the accompanying SDSR[1]. The National Security Strategy of the United Kingdom is: to use all our national capabilities to build Britain's prosperity, extend our nation's influence in the world, and strengthen our security. The networks we use to build our prosperity we will also use to build our security. We live in an uncertain world, but are prepared to take advantage of the opportunities that arise as a consequence.

---

1 The NSS and SDSR are the essential precursors to this Green Paper. For reasons of space, much of the important analysis in them is not repeated here.

6. The SDSR addressed the threats highlighted in the NSS and directed where resources and effort should be placed to deliver defence and security priorities. The SDSR also set a clear target for the national security capabilities the UK will need by 2020 and charted a course for getting there.

7. The NSS and SDSR recognise that the security and defence challenges faced by the UK are increasingly similar and can only be addressed through integrated working between the defence and security sectors. In many cases, the technology underpinning key national security capabilities is very similar. Occasionally it is identical. The NSS and SDSR also recognise that the UK faces a number of new threats that need to be assessed and appropriately addressed. Foremost amongst these are cyber threats, where an investment of £650m over the next four years will be made through a transformative National Cyber Security Programme. We aim to build upon the UK's nascent comparative advantage in key areas of the cyberspace technology domain.

1.2: Equipment, Support, and Technology for Defence and Security

1.2.1: Context

8. The uncertain world depicted in the NSS requires us to be more thoughtful, more strategic, and more coordinated in the way we advance our interests and protect our national security. More than ever, expenditure on defence and security must be to ensure that the UK has what it needs at a price it can afford.

9. The UK is not facing these threats alone. Its relationships with other nations and participation in international organisations provide crucial support in protecting our national security. But ultimately the UK must ensure that it has the ability to act in its own interests, where necessary and appropriate, as a sovereign nation. It is, therefore, vitally important that the UK manages properly two key factors that underpin all the capabilities that we have or will need to protect national security: technology, and the supply of equipment, support, and services.

10. As the SDSR sets out, we must invest in essential science and technology to deliver critical capabilities and decision-making for UK defence and security. In particular, we need capabilities that the market alone may not provide and where information on threats and countermeasures are restricted – for example, chemical, biological, radiological, and nuclear protection, and counter-terrorism. Our investment in science and technology must also provide us with an understanding of the defence and security environment we face in the future, allowing us to take informed decisions about equipment, tactics and training. It must also allow us to regenerate and reconstitute capability where necessary. We must be able to exploit science and technology and be an intelligent and cohesive customer.

11. Almost all the technology and equipment underpinning the UK's defence and security capabilities, together with increasing levels of support and other services, are acquired through contracting with advanced manufacturing companies and specialised service providers. The largest are trans-national enterprises with the ability to design, build, and then support complex systems. The smallest are niche firms with specialised skills that are often a source of innovative ideas. The extent of our reliance on them, and their reliance on us, however, raises common issues about the effectiveness of our relationships, their long-term viability, and assured supply.

12. Particular issues can arise in cases where our requirement includes an essential national security component and our potential suppliers are located offshore, or are onshore but subject to foreign ownership or control.

13. The technologies that we may need are often at the leading edge of what is possible. The equipment that uses them often requires expensive advanced engineering techniques to develop and integrate complex coding and software. Our programmes to deliver new defence and security capabilities may run for many years and occasionally one of them fails, which means the UK does not get the equipment and support it needs and taxpayers' money is wasted.

14. We believe, therefore, that we should have both an overarching policy and specific policies in relation to key equipment, support, and technology issues.

1.2.2: Core policy

15. Our proposed approach to equipment, support, and technology for UK defence and security consists of three key principles.

Key principle 1: The UK Armed Forces, the wider National Security community, and the Law Enforcement agencies must have the capabilities they require to protect the UK and its interests, in line with the goals set in the National Security Strategy, where and when they need them.

Key principle 2: In an increasingly global world, we will draw from wherever we can the scientific and technology developments needed to provide capability edge, while maintaining our ability to make intelligent decisions based on sound scientific evidence.

Key principle 3: These capability and technology requirements are subject to affordability and the means of fulfilling them must demonstrate value for money.

Open competition

16. Our default position is to seek to fulfil the UK's defence and security requirements through open competition in the global market. We judge that this approach maximises the likelihood of finding a solution to our needs at an affordable cost and at best value for money. We also believe this offers the best catalyst for UK industry to be efficient and competitive, which is essential for both its long-term viability and for UK growth.

17. Experience shows that acquiring technology, equipment, support, and services from the global open market works well in many important areas across defence and security. In delivering urgently needed new capabilities for our Armed Forces and other Government departments in Afghanistan, the UK has made extensive use of suppliers from around the world to meet these requirements quickly and effectively. Similarly, we make considerable use of contractors to support our Armed Forces and other UK personnel on deployed operations. The UK also uses international suppliers to provide equipment for UK security forces, such as the body armour used by the Police Service and the scanning systems used in aviation security. Our cyberspace and information assurance defences and capabilities are similarly sourced from a global, international supply base – ranging from multinational systems integrators to specialist SMEs.

18. There are, however, specific characteristics of the defence and security sectors that can inhibit the market or make it inappropriate, for reasons of national security, to use open competition to meet our needs. These are discussed in section 2.1.

19. In parallel, the Government has broader policy reasons for taking action to help UK-based companies be effective and thrive in an open, competitive market, including by commercial diplomacy, support to exports, and encouragement to SMEs. These are discussed in section 2.3.

20. Specific issues relating to defence, security, and cyberspace are discussed in Part Three.

EU legislation

21. Our commitment to open competition for the UK's defence and security requirements is also consistent with the UK's obligations as a member of the European Union (EU). The UK is required under the Treaty for the Functioning of the European Union (TFEU) to act fairly, transparently, and openly by competing defence and security requirements at an EU level. The exception is where the essential interests of our security are at stake and in those circumstances the UK can, like all Member States, derogate from the Treaty by invoking Article 346[2].

22. We are currently in the process of transposing EU Directive 2009/81/EC, otherwise known as the EU Defence and Security Directive, into national law. This Directive sets new procurement rules for contracting authorities/entities that purchase military equipment, sensitive equipment, and related goods, works, or services. It also provides rules where contracting authorities/entities purchase works and services for specifically military purposes or works and services for security purposes that involve, require, or contain classified information. The Directive is scheduled to be brought into UK national law by August 2011.

1.2.3: Government and its suppliers

23. The SDSR enables us to plan for what the UK will need in the coming years. At the heart of this are various defence and security capabilities – the combinations of trained and skilled people, equipment and support, and operating methods that enable the UK to act against the various threats we face. The Government, therefore, needs to be clear about what it expects from those who help supply current and future national security capabilities.

24. As set out above, our default position is to use open competition in the global market and to buy off-the-shelf where we can. Where essential for national security, we will take action to protect our operational advantages and freedom of action. This will sometimes, but only rarely involve action to protect underpinning technologies and skills.

25. The more clarity and certainty the Government can give about its intentions in procuring defence and security capabilities, the more confidence we will create around the value

---

2 Article 346 of the Treaty on the Functioning of the Union states:

1. The provisions of the Treaties shall not preclude the application of the following rules:

(a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security;

(b) any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes.

2. The Council may, acting unanimously on a proposal from the Commission, make changes to the list, which it drew up on 15 April 1958, of the products to which the provisions of paragraph 1(b) apply.

of investment in relevant research and production in the UK. This is important because all the major defence and security companies are trans-national businesses, which have choices about where they invest and where they situate research and industrial facilities. This potential mobility can raise national security issues, as well as having broader economic consequences for the UK.

26. We wish to increase our engagement with academia, in order to access truly innovative research in universities, and to encourage the commercialisation and pull-through of research into defence and security capabilities. A healthy UK industry in the defence and security sectors is a vital source of innovation and supply. In some cases we rely on UK industry to design, build, support, and maintain critical national security capabilities. Support for defence and security exports and enabling SMEs to fulfil their potential can also help meet our national security requirements.

27. Technological and industrial capabilities are also levers in their own right. As a leading industrial nation, the UK is able to work with other countries on research and acquisition, as a complement to its wider security relationships, and to export training and equipment, as part of broader relationship and capacity building and of wider diplomacy. This gives the UK greater influence and helps us to shape our national security environment.

28. As part of our wider policy objectives, we wish to create the conditions for greater global private sector investment in the UK and to maximise the benefits of public sector investment. A healthy industry, including SMEs, brings wider economic benefits, in terms of providing jobs, maintaining skills, and making a considerable contribution to the Exchequer. The companies involved in defence and security already sell significant volumes of goods and services abroad at a time when strong and balanced growth, driven partly by a greater level of exports, is the overriding priority of the Government[3]. They help drive technological innovation in the UK and have competitive advantages in world markets.

29. The Government supports the need for companies to make a reasonable return for their shareholders. Industry must, however, make a greater contribution to the Government's drive to reduce the costs of developing, producing, and maintaining essential defence and security capabilities, including through the contractual renegotiations currently being undertaken by MOD with all its main suppliers as a result of the SDSR and through participation in the Cabinet Office led pan-Government efficiency reform initiatives. The long-term prosperity of UK industry depends on being competitive and market sensitive, in order to offer value for money to the British taxpayer and compete successfully in foreign markets. This approach is pragmatic, not altruistic: we will be supportive, but not protectionist.

30. What Government and industry want are not mutually exclusive, but they are not exactly the same. There are, therefore, important benefits in Government and industry better understanding each others' objectives and seeking to align these more closely. This requires positive engagement and greater transparency on both sides.

---

3 'The path to strong, sustainable and balanced growth', HM Treasury and Department for Business, Innovation and Skills, November 2010.

1.2.4: Balancing choices

31. This Green Paper sets out a range of factors that may need to be considered when making choices on defence and security issues. It also seeks to bring out some of the complex interactions between those factors. One key issue is, therefore, to find the correct balance between these factors when delivering our key principles, and in particular to avoid these becoming excuses for inefficient and ineffective choices.

32. The Government has an overarching duty to provide the defence and security capabilities needed to protect the UK and its interests. Our suppliers play a critical role here. With this in mind, the Government's priorities include:

- recognising the vital importance of science and technology to our future security;
- identifying the critical areas where the UK has or needs an operational advantage and freedom of action for a particular capability;
- strengthening bilateral international co-operation and collaboration;
- enabling SMEs, which are a vital source of innovation and flexibility, to fulfil their potential; and
- giving our support to exports within a framework of responsible licensing.

33. This Green Paper gives an indication of our thinking in these areas, and many others, and invites everybody to contribute to the debate.

General Question:

Q1. Does our proposed approach, based on the three key principles, strike the right balance between the various factors influencing how we will go about fulfilling our defence and security requirements?

(NB: in Parts Two and Three of this document we are asking more focused questions about individual policy areas and issues.)

Part Two: Cross-Cutting Issues

34. This part of the Green Paper looks at the key cross-cutting topics on which we are seeking views. It covers three categories: national security, technology, and broader policy. To guide the consultation process, we have posed a general question and specific subsidiary questions at the end of each section. These indicate the areas where we are particularly interested in receiving views, but other comments are also welcome.

2.1: National Security

35. The distinguishing feature of equipment, support, and technology choices in the defence and security fields is that they are subject to overriding national security considerations. Traditionally, our national security has been viewed in terms of defence matters. The NSS recognises, however, that many of the threats faced by the UK cannot be addressed through purely military means. Of the priority risks to the UK, all of the Tier One risks and many in the other Tiers require responses from the security and intelligence agencies, police service, or other security organisations.

36. The NSS list of priority risks[4] is:

- international terrorism
- hostile attacks upon UK cyberspace
- a major accident or natural hazard
- an international military crisis
- an attack using chemical, biological, radiological or nuclear (CBRN) weapons
- major instability creating an environment that terrorists can exploit
- a significant increase in organised crime
- severe disruption of satellite communications
- a large-scale conventional military attack on the UK
- a significant increase in the activities of terrorists, organised criminals, and illegal immigrants, and in the level of illicit goods trying to cross the UK border
- disruption to oil or gas supplies
- a major release of radioactive material
- a conventional attack on another NATO or EU member
- an attack on a UK overseas territory
- disruption to international supplies of resources (e.g. food, minerals).

4 The detailed list is in the section titled 'National Security Strategy: Priority Risks', on p27 of the NSS.

37. This section of the Green Paper looks at two national security issues that potentially apply to many of these risks - sovereignty and working with other countries.

2.1.1: Sovereignty

38. Most defence and security choices in relation to equipment, support, and technology are concerned with obtaining and maintaining the various national security capabilities needed to protect the UK and its interests. However, two specific aspects of those capabilities are particularly important and require separate consideration. These are:

- operational advantage, which is fundamental to the overall effect that a given capability can achieve; and
- freedom of action, which is essential to be able to use a capability effectively.

39. These relate to the situation now and in the foreseeable future; and to current acquisition plans and long-term research priorities.

Operational advantage

40. It is a cardinal principle of defence and security operations to seek and maintain an edge over potential adversaries, both to increase the chances of success in hostile situations and to increase the protection of the UK assets involved, especially our people. This advantage can be based on factors such as superior intelligence, training and doctrine, and it is particularly important in terms of equipment and underpinning technologies.

41. Obtaining and maintaining any operational advantage inevitably requires investment, often long-term in nature. So it is essential to understand what exactly gives the UK an advantage and in what circumstances. For example, is it absolute – the possession of a national security capability that others do not have or have difficulty countering; or is it relative – the possession of a capability that is incrementally better than others have? And if it is relative, where within the overall capability envelope does the operational advantage actually lie? For example, the defensive aids suite on an aircraft going into a combat zone does not contribute directly to the delivery of effect, but is critical to survivability and therefore success.

42. This understanding is needed to inform decision-making when acquiring new national security capabilities. How much of any given advantage do we need? In effect, how much risk can we afford to take? The capability operator's position is always to maximise advantage, because the future is uncertain – warfare is famously uncertain – and therefore no edge should be foregone. But there is a balancing factor, because UK resources are finite and therefore prioritising any given advantage inevitably involves taking risk against other national security capabilities.

43. This also highlights the need for the Government to understand how much a given advantage costs to acquire. If the UK has to pay a premium to obtain it, then this needs to be properly understood. The cost of acquisition can in principle be subjected to cost-benefit analysis. The overall risk, however, cannot be reduced to monetary values, since it involves issues such as the survivability of UK forces. Nevertheless, as with all acquisition choices, operational advantage is subject to affordability and value for money.

Freedom of action

44. Possession of a national security capability, including any advantages, is not sufficient in itself. The UK also requires freedom of action: the ability to determine its internal and external affairs and act in the country's interests free from intervention by other states or entities, in accordance with EU and international law. In particular, this includes being able to conduct combat operations at a time and place of our choosing. This freedom is the essence of national sovereignty.

45. Different acquisition options offer differing levels of assurance in relation to our future freedom of action, particularly where a potential supplier is overseas. The UK may, therefore, have to constrain our acquisition approach for a particular defence or security capability, in order to maintain our freedom of action and thereby our national security.

46. The circumstances in which we will need to do this will vary according to the external situation. In each case, it will be a balance of risk. However, there are four general cases – not necessarily exclusive – in which such action is likely to be needed in the interests of national security.

47. First, where our requirement is, by its nature, fundamental to our freedom of action as a nation. The leading example of this is secure information and communications transfer at national-level. This covers the ability of the Government to conduct its business securely at the highest level, including communications with posts overseas and commanders of deployed forces. High-grade cryptography remains strategically vital across Government. The need to protect our most sensitive information, wherever it is in the world, creates a sovereign requirement to control those aspects of cryptographic production, deployment, and support that are critical to the integrity of the product and therefore to our national security.

48. Second, where the fulfilment of our requirement, or the operation of the resulting capability, is heavily dependant upon access to intelligence information or classified technologies. In these circumstances, we will only be able to consider suppliers of equipment, support, or services that meet the highest standards of trust. The leading example of this is the UK's nuclear deterrent, as regards both weapons and propulsion.

49. Third, where operational circumstances mandate changes to an in-service capability that can only be met by having an ability to respond at the highest levels of speed and agility. A leading example of this is electronic warfare and associated defensive aids, where the ability to update deployed capability in the light of intelligence is essential to survivability. However, there can also be a similar, longer term need to change and upgrade a deployed capability against demanding operational timescales.

50. Fourth, where the nature of the UK's potential operational advantage requires the highest possible assurance about one or more aspects of the performance of a capability. A key issue here is assured access to technical details of critical sub-systems, without which we are unable to judge the level of operational risk. This is often related to the design of hardware and software in complex electronic systems and the impact of changes made to them.

Acquisition choices

51. The UK's acquisition strategy for a given national security capability – including for supply, maintenance, and upgrade – must take these two factors into account. In order to ensure our operational advantage or freedom of action, we may need to place work with a limited pool of potential suppliers or a single supplier, to meet our security of

supply and security of information requirements as defined by the EU Defence and Security Directive[5]. In such cases, the UK will fulfil its requirement from suppliers who meet the highest standards of trust and assurance, which are likely to be: UK-owned companies based in the UK; foreign-owned or controlled companies based in the UK that are subject to security undertakings given to Government by the owner; or in some circumstances companies associated with our closest allies.

52. In some circumstances, the UK may also need to develop and maintain specific skills and capabilities within Government: for example, defensive measures against chemical and biological weapons.

Protecting our operational advantage and freedom of action

53. Where the UK has an operational advantage and freedom of action, it needs to ensure that these are not forfeited. We must not allow our potential adversaries to erode our advantages or use them against us, nor to constrain our freedom of action. It is therefore essential that these are not compromised by selling (or gifting) them, by accidental loss, or by espionage. A further national security consideration is, therefore, having appropriate measures in place to prevent this happening.

Market weaknesses and protecting specific industrial capabilities

54. In some defence and security capability areas there is no effective market or the market that exists is fragile. Government is the only legitimate buyer for certain items and the resulting monopsony may generate insufficient demand for a competitive market. Coupled with the high level of capital investment needed to operate in some sectors, this may result in insufficient return on investment for companies to remain in, or new suppliers to enter, such a sector. Limited demand and high technology requirements in the defence and security sector are also barriers to private venture investment, which is particularly important for research.

55. National security considerations may actually exacerbate this problem. If a supplier has a industrial capability, but is not permitted to sell or export the related products for national security or wider policy reasons, then the supplier is unable to get a return on investment or to spread its overheads. In these circumstances, there is little incentive to remain in the market and no incentive to reinvest. Moreover, UK demand in itself may not support the sustainment of that industrial capability.

56. In these circumstances, the Government may as a last resort have to invest directly to support nascent technological and industrial capabilities or sustain specific capacities in the longer term, but only where these relate to operational advantage or freedom of action and therefore our national security. We believe that skills are the key component of such capabilities – particularly scientific, technological, engineering, and mathematical skills – although specialist infrastructure and access to intellectual property are also important.

57. The UK may, therefore, need to invoke Article 346. This will only happen to the minimum

---

5 Article 22: Security of Information. 'When contracts involve, require and/or contain classified information, the contracting authority/entity shall specify in the contract documentation (contract notices, contract documents, descriptive documents or supporting documents) the measures and requirements necessary to ensure the security of such information at the requisite level.'
Article 23: Security of Supply. 'The contracting authority/entity shall specify in the contract documentation (contract notices, contract documents, descriptive documents or supporting documents) its security of supply requirements.'

extent needed for our future national security needs and will be subject to continuing demonstration of value for money. Where the UK seeks to sustain technological or industrial capabilities, this will always be a means to an end, not an objective in itself. It will not be used to subsidise inefficient, uncompetitive, or outdated industries.

58. In practice this is a complex issue. The critical advantage or freedom may not reside at the prime / platform level, but deeper into the supply chain. Some may argue that it is not possible to protect specific capabilities without supporting broader industrial capability in a sector. Moreover, with the impact of globalisation, no supply chain can be wholly on-shore. Hence there are inherent limits to the level of protection that can be achieved.

Balancing national security considerations

59. As discussed above, national security considerations involve at least two trade-offs: the levels of risk taken against operational advantage and against freedom of action. The UK may need to take action to ensure that planned operational advantage and freedom of action are successfully obtained and maintained; as well to protect the underlying technological and industrial capabilities. Our ability to do this depends on being an intelligent customer.

60. We recognise that any steps to protect national security have broader consequences. Whenever we forgo open competition, we potentially limit both our choices and our levers for driving down costs. This is why, in the SDSR, we identified the need for an approach 'that seeks to secure the independence of action we need for our Armed Forces, while allowing for increased numbers of off-the-shelf purchases and greater promotion of defence exports[6]. We must also manage our national security concerns so that they do not inhibit our ability to work with other countries.

General question:

Q2. What factors should the UK take into account when assessing the national security implications of acquisition in the defence and security sectors?

Specific questions:

Q3. Are there particular technological or industrial capabilities, including skills, that you believe are crucial to national security? If so, please give details.

Q4. Are any of these currently at risk of being lost? If so, please give details.

Q5. Are there any technological or industrial capabilities which the UK has sought to protect where you believe this is unnecessary? If so, please give details.

2.1.2: Working with other countries

61. Most of the arrangements we make to protect our national security have an international dimension. Therefore, it is often more beneficial for the UK to work directly with other nations on research and on equipment and support acquisition than to proceed alone with a market-based approach. This is true both in terms of specific programmes and in respect of broader national objectives.

---

6 SDSR page 12; box on 'National security tasks and planning guidelines', paragraph 8.

62. Very few countries now have the financial and scientific resources to develop and deliver major new defence and security capabilities alone. Delivering effective capabilities continues to be ever more expensive and now budgets are under increasing pressure, as a result of the recent global financial downturn and the need for deficit reduction. These constraints prevent the UK, and countries in a similar situation, from independently maintaining a full range of defence and security capabilities and preserving a technological edge in all areas.

63. In taking decisions in the SDSR, we gave significant weight to the fact that we and our NATO allies consciously rely on each other for particular capabilities. We will seek deepened relationships with those with whom we can share technologies, requirements, programmes, and capabilities. This will ensure that collective resources can go further through pooling and sharing where national security allows it and our freedom of action in the use of the UK's defence and security capabilities is not jeopardised.

64. The Government believes that working with other countries in acquiring capabilities is essential in a globalised marketplace. It can reduce the financial burden on individual states, boost interoperability between allies, and is a key tool of diplomacy. Within a national security context, the Government therefore seeks not only to boost cooperation with its key allies and partners, but build future partnerships with other nations and through multinational organisations.

65. It is fundamental to being able to participate in international working that the UK has itself invested sufficiently in relevant technology and capability areas to be a worthwhile partner.

Bilateral relationships

66. As set out in the SDSR, we will generally favour bilateral equipment collaboration or off-the-shelf purchase, because such arrangements are potentially more straightforward and more fruitful than complex multilateral agreements, which have delivered mixed results in the past. The criteria for equipment cooperation will include the existence of common requirements, complementary technological capabilities, and affordability for both participant nations, as well as enhanced export potential or industrial advantage. The Government seeks to engage strongly with potential partners for future projects or programmes, particularly those whose defence and security posture is closest to our own or with whom we cooperate in multinational operations.

67. The UK's most important international security relationship is with the US where we have a long history of working together on acquisition of equipment and support. The principal benefits to the UK derive from the scale of the US defence and security effort – longer (and therefore cheaper) production runs, potential access to leading-edge technologies derived from huge R&D spending – and interoperability. When partnering with the US, we are also able to exert greater influence to ensure that UK-listed companies are given an opportunity to compete for work on US projects. But UK involvement also means being subject to US legal regimes, especially International Traffic in Arms Regulations (ITAR), although the approval of the US/UK Defence Trade Cooperation Treaty by Congress has created an important new means of potentially easing this burden.

68. The US is usually the dominant partner in any joint programme, but working with it takes different forms. There is a significant difference between working with the US on acquisition when the UK is acting as a peer or niche contributor and when we are simply acquiring US-developed capability. The former role is much more advantageous in capability, as well as technological and industrial terms, but naturally requires the

UK itself to bring something to the table. The latter role can be important in capability terms, but tends to have limited technological and industrial benefits.

69. The security sector has particularly close links with the US Department of Homeland Security (DHS). There has been a wide ranging scientific and technical dialogue on many security-related issues. Since the attempted attack on Detroit in 2009, this cooperation has been enhanced through workshops, jointly funded research, and staff exchanges. The UK is also heavily involved in international collaboration on social science research for counter-terrorism. UK Government social and behavioural scientists are in close contact with their counterparts in the Human Factors Division of the Department of Homeland Security and are linked into the DHS-sponsored Studies in Terrorism and Responses to Terrorism (START) research programme at the University of Maryland. And in the cyberspace and information assurance (IA) domain, our capability benefits significantly from the uniquely close relationship with the US Government established several decades ago.

70. The UK-France Defence and Security Cooperation Treaty, signed in November 2010, builds on the increasingly similar approaches to defence that have been developed by the UK and France in recent years. France is the military power closest to the UK in terms of geography, effort, resource, profile and reach; and a shared understanding of the economic and military imperative for UK/French cooperation has become apparent through the NSS, the SDSR, and the French Livre Blanc on defence. Closer working with France will help to increase military interoperability, capability and effectiveness, and secure better value from our respective investments in defence.

71. The Treaty provides a framework for intensifying cooperation between our Armed Forces, which will include the sharing and pooling of materials and equipment, the building of joint facilities, and industrial and technological cooperation. Agreements to work together on unmanned air systems and to deliver a joint complex weapons strategy provide real opportunities for both countries to reap the potential benefits of collaboration for defence. More details will emerge over time as work begins on specific joint initiatives.

72. We are also looking to increase bilateral cooperation with a wide range of other countries. Our shared interests are most intense with our NATO and EU partners (including European allies such as Germany, Italy, the Netherlands, Norway, Spain and Sweden) with whom we have a history of close equipment or other defence cooperation. We are also seeking to build on our global relationships with countries such as Brazil, India, and Japan, and on our established defence relationships with the Kingdom of Saudi Arabia and our Gulf partners.

73. In security, there are close ties with a number of countries around the world. There is a Memorandum of Understanding between the UK Government and Australia, which has led to close cooperation on counter-terrorism science and technology. Led by the Centre for the Protection of National Infrastructure (CPNI), the UK has also a Memorandum of Understanding with Canada covering the use of science and technology in public security and safety. There is also a significant exchange of technology for combating serious organised crime with Canada, Germany, and the Netherlands.

Multilateral relationships

74. While the Government's policy preference is for substantial bilateral defence relationships with allies and partners, it does not discount the potential of multilateral acquisition projects and programmes. These can deliver the benefits of pooled requirements, longer production runs, and lower costs through greater overall demand.

They can also increase interoperability. However, multilateral projects also need to be appropriately structured and managed, as they can be hampered by contractual and political issues and suffer from over-complexity.

75. The UK is closely involved with a number of key projects that are being procured multilaterally and are delivering or set to deliver outstanding capability – for example the Typhoon combat aircraft and the A400M transport aircraft. Furthermore, we will maintain our involvement in NATO projects that aim to create common standards for basic equipment. We also remain open to discussion about potential collaborations through NATO, or other routes such as OCCAR and the European Defence Agency, where these would demonstrably benefit UK defence interests.

76. The national security of the UK is similarly closely linked with security in other nations. In the first instance, working constructively with our close allies can improve capability and maximise efficiency through sharing of requirements and technology. Equally, helping to improve security in fragile or failing states improves the security of the UK by reducing opportunities for international terrorists to find new havens.

77. In Europe, our main engagement on science and technology for security has been through the security stream of the EU and the European Commissions' Framework Programme 7 (FP7). FP7 encourages collaboration between industry, SMEs, academia, public-sector research establishments, and international partners by providing research funding to consortia investigating security issues. There are several UK projects currently running under FP7 including work on physical security, crisis management simulation and training and supply chain security.

General question:

Q6. How can the UK get the best from working with other nations, whilst avoiding the pitfalls?

Specific questions:

Q7. What are the conditions for successful bilateral/multinational procurement? How can Government best assess these before committing to a project?

Q8. How can the UK engagement with NATO allies and European partners in bilateral procurement arrangements support and benefit interoperability between all member states and other allies and partners?

Q9. What models are available which allow us to use our defence and security budget more effectively by working together with other countries to develop the capabilities we need? In what circumstances could the models be used most effectively?

Q10. What more should the Government do to ensure that the process of awarding work under international collaborative programmes is open and fair?

2.2: Science and Technology

78. Science and technology[7] plays a critical role in providing the UK with a decisive advantage over potential adversaries, delivering the NSS, and countering the many varied security threats faced by the UK. Maintaining a technological edge, with the necessary underpinning science and facilities, is often vital to keeping one step ahead of our opponents, both on the battlefield and in the wider security domain.

79. Our own investment in science and technology is critical for the understanding of the defence and security environment and allowing us to make informed, evidence-based decisions and choices. It is also critical for the regeneration and reconstitution of capability to counter resurgent threats, and critical in developing specific technologies and solutions for capability to counter new and emerging threats and opportunities. We must therefore prioritise our science and technology investment carefully, and ensure we engage with the widest and most appropriate research suppliers to reduce costs and achieve value for money. We must also ensure the balance of priorities includes the ability to be an intelligent customer of capability, which embodies and exploits science and technology either arising from our own research or from others.

80. The world is now more technologically enabled than ever before. The UK's adversaries, both at home and abroad, field weapons with increasing sophistication and use commercial technology in innovative and ingenious ways. The information domain now constitutes a potential battlefield, as the capability and skills required to launch a cyberspace 'attack' are increasingly ubiquitous. Even threats such as Improvised Explosive Devices (IEDs), which are often technically simple, require sophisticated technology to counter. This imposes costs, as we seek to maintain our technological advantage. The Government must respond to the spectrum of technological threats and opportunities in a timely manner, both in support of current operations and the longer-term requirements of future capability. As resources become constrained and more areas of technology emerge, maintaining an effective balance across technologies and the capacity to respond becomes increasingly challenging. In the fast-moving cyberspace domain, we will seek to balance the imperative to understand and exploit cutting-edge technologies with investment in mature technologies and techniques that still deliver advantage, especially on the defensive side.

81. The Government must be clear about where it needs to invest or disinvest in science and technology and in critical scientific and engineering skills, while maintaining a low level of overview activity on broader scientific and technological developments, in order to spot opportunities and avoid technology shock. We must also seek to identify clear routes for the exploitation of technology to ensure that investment benefits the operators and the wider defence and security enterprise. However, the strategic context in which we must both harness and protect against the use of technology, continues to change rapidly.

82. In short, the pace of technological change, coupled with the wider availability of technology, will lead us to face an increasingly capable asymmetric and global threat into the future. Therefore we must try to understand the key areas of technological

---

7 'Science and Technology' refers to the broad range of outputs and outcomes from our investment in research and development (R&D). The accepted definition of pure (or basic) research is primarily to acquire new scientific or technical knowledge for its own sake; applied research is where such new scientific or technical knowledge is gained for a specific aim or objective in mind; and development is where scientific or technology knowledge is used to produce new or substantially improved component, product, process, or service.

change which could impact defence and security, the threats and opportunities, over the next twenty years, and the implications for our effective response to them. Our response may increasingly include how we use existing equipment, how we train and deploy our Armed Forces and security agencies, or how we develop our tactics, operating procedures, and processes.

83. There still remain a number of technologies unique to defence and/or security. However, the breadth, speed of change, and volume of investment in science and technology outside the defence and security fields means we must now adopt and adapt civilian science and technology if we are to maintain our technical edge and ensure a good interface between civil and defence programmes.

84. MOD's Science and Technology Programme provides a significant surge activity, allowing scientific knowledge and technical solutions to be developed in order to respond rapidly to changing threats. It provides a critical bridge between the threats and challenges faced by our Armed Forces and security agencies, and the technology and solutions the market place has to offer. Recent operations in Iraq and Afghanistan have shown the value of defence science and technology in providing direct support to the front line. Forward deployed scientific advisers have demonstrated valuable operational and intelligence analysis. This has been combined with rapid reach-back into UK based laboratories (both in Government and industry) for analysis of threats and development of urgent operational requirements, for example, to counter IEDs and develop new armour solutions. The ability to respond to current operations and threats in this way is a consequence of previous decades of underpinning investment in critical areas of science and technology.

85. Science and technology has also proved essential in improving security in the UK. Following the attempted bombing of an aircraft over Detroit, science and technology was a key part in the rapid response from Government and industry to improve aviation security. Similarly, improvements in surveillance technology are essential to countering terrorism and serious organised crime while, more widely, developments in body armour have made the UK's police safer.

86. Forecasting science and technology advances, technological change and its use into the future is not precise or easy. This means that all aspects of defence and security – from setting strategy and policy, planning future capability (both military and civilian), its delivery and acquisition through to generation at the front line – require underpinning by a full understanding of the threats and opportunities posed by science and technology. The various facets of evidence-based decision making, the understanding of science and technology opportunities and technical risk reduction allows Government to be intelligent in the way we plan, buy and ultimately use capability through-life.

2.2.1: Priorities for our future science and technology investment

New challenges in accessing science and technology

87. The Government's science and technology capability comprises a mix of in-house expertise, delivery through the wider supply base, and through collaboration, both with the industrial and academic base and with international partners. At present, Government science and technology for security and defence takes place across a number of departments, each with differing requirements. Therefore, we need to consider how these can work together better to provide a more strategic approach to science and technology within Government, industry, and academia.

88. Civil investment in science and technology, driven by the commercial market, both

nationally and globally has been huge and now dwarfs defence and security specific science and technology spending. In the UK alone, Government spend in civil science and technology is over three times that spent on military science and technology. These trends in funding have already given rise to technology areas on which defence (and to a lesser extent, security) relies completely on civil developments or where MOD has little visibility or influence.

89. While there are a number of specific areas of science and technology critical for defence and security in which we must invest (these include CBRN, counter-terrorism technologies and intelligence exploitation), consumer demand continues to drive many areas of technology in new directions and at rates that cannot be controlled for military or security advantage. These include healthcare, information, robotics, energy, etc. The general trend is for existing technology applications to become more reliable, more available and at lower cost. And a number of major research fields are likely to bring benefit and new applications, particularly as they are combined to generate systems and capability. These will increasingly span both defence and security areas. In some of these areas we may need to invest in research to develop our own applications, whereas others may require scientific and engineering skills to be able to exploit the threats and opportunities successfully.

Developing fields

90. Some of the most important rapidly developing fields with potential relevance to defence and security include:

Cyberspace – There is a currently a huge dependency on information technology and modern communications which cuts across both the military and civil sectors providing a force multiplier and market advantage. Such reliance, however, can lead to vulnerability which will be exploited by new science and technology. For example, attack or damage to control and data systems that include critical national infrastructure such as power, telecommunications and food/water supply.

Biomedical science – investment in genomic sequencing has provided significant opportunities for development of new drugs, vaccines and medical treatments. Such dual use technologies extend the range of offensive chemical and biological warfare that could be used against the UK, where potentially viruses will be very hard to detect by gene sequencing, and difficult to counter or protect against.

Neuroscience – Knowledge about the human brain is rapidly increasing including: understanding pharmacological effects to enhance performance and using brain activity to control systems. As such it offers significant opportunities for defence and security in understanding adversaries' behaviours, training and improving human performance on the battlefield or in human-based security situations such as guarding or search.

Autonomous Systems – a significant investment in such systems and robotics in the civil sector will spill over into the military and security environment. This is likely to be seen in ever more sophisticated unmanned systems (in land, sea and air environments) achieving multiple effects from smaller platforms, removing the man from the platform, enabling greater risk taking and extending the performance envelope of systems that combine reconnaissance, communications and strike capable systems potentially able to make decisions for themselves, closer to the target.

New materials, including nanotechnology – an improved understanding of physics at the nano-scale enables new classes of materials with tailored properties and functionality, completely inconceivable in conventional materials, to be developed;

in some cases with mass-production techniques similar to synthetic chemistry. Such materials could, for example, be used to reduce the effect of explosives on airframes or buildings. Rapid prototyping and weight reduction will be critical for defence applications.

Energy – A huge focus on climate change and on alternative sources of efficient energy production will lead both to opportunities in new energy sources for defence and security, but also to unforeseen vulnerabilities in supply. This may lead to a greater global focus on nuclear power, giving rise to greater availability and potential proliferation of fissile materials to rogue states or terrorists, for use in either improvised nuclear devices or 'dirty' bombs.

Space – This is an area where the UK has capability but also relies considerably on its allies. Our dependency on space-based surveillance and satellite communications potentially leads to vulnerability, particularly from nations with emerging political or military ambitions in space. Space-based systems are now seamlessly integrated into many of our communication and location systems, making the UK (and other countries) vulnerable to natural disaster, accident, or deliberate attack. The criticality of these systems made satellite vulnerability one of the key risks in the National Security Strategy.

Sensor Systems – Improvements in sensing technology and communications will lead to step-changes in the abilities of sensor systems. For example, nano-materials coupled with smaller and smarter autonomous systems will enable ubiquitous sensing, using networks of sensors that are geographically spread out. The nature and size of the battlefield will change, where movement or action cannot occur without being seen and detected. Improved sensor technology will play a vital part in surveillance and counter-surveillance. Also screening, particularly for explosives, will improve, as sensors become part of a wider sensor system, which may include technical and human elements.

Identity Assurance – There is a growing requirement for identity of people, objects and services. Technologies such as automated face recognition have improved markedly, finding application in consumer-level cameras and online picture-sorting software. Trials of similar technology at the border, and in matching of photographs of unknown persons to known criminals, demonstrate the wider possibilities – while their use to secure on-line transactions and protect the contents of smartphones remain an aspiration for the future.

Civil Liberties, ethics, and social sciences – Social and behavioural sciences and ethics – the study of society and the manner in which people behave and impact in the world around us – is fundamental in our approach to both defence and security. To be truly effective in defence and security operations today we need to harness this in order to understand both our adversaries and the civil populations to which we seek to bring stability and security; to understand the motivating factors that cause someone to support or commit acts of violent extremism, or to better identify suspicious behaviours of those who wish to do us harm. And underpinning our whole approach to security for the UK are the principles of fairness and proportionality, balancing the need for security with the rights to civil liberty and privacy.

91. These fields present a range of challenges for defence and security, including:

- how we respond to the growing breadth and increasing pace of scientific and technological change;
- how we maintain military advantage where adversaries have access to

increasingly sophisticated technologies and the information and skills required to innovate;

- how we manage resources across the needs of the equipment and support programmes, capability development, and technology development while guarding against technological surprise through horizon scanning;

- what we should do to address the asymmetric threat (and opportunity) presented by cyberspace;

- how we identify areas of capability, where in some instances, quantity will out-perform quality (i.e. network low-cost sensors and autonomous systems); and

- what we do to understand public engagement with, and acceptance of, new security measures and technologies.

2.2.2: Benefits from international collaboration

92. International Research Collaboration (IRC) plays a fundamental role both in achieving value for money from our own research investment in expertise and technology, and also in supporting the development of affordable military and security capability. It provides access to, and influence over, science and technology which the UK does not have, cannot afford to have, or could only be achieved through working with a partner.

93. Bilateral relationships, for example with US or France, where the UK's own investment is 'geared' with other nation's investment, will become the norm. This gearing provides greater resource, expertise and breadth of knowledge to be applied to science and technology problems. Other bilateral and multilateral relationships, such as The Technical Co-operation Program and NATO, allow information exchanges and joint projects that are particularly valuable in sharing sensitive science and technology topics in the defence and security amongst a wider peer group, and enhancing our ability to be an intelligent customer. However, IRC cannot and should not be developed in isolation to acquisition of capability, and how science and technology can be exploited from IRC must be considered at all times.

2.2.3: Delivering our science and technology priorities through the wider supply base

94. A huge amount of innovative science and technology development takes place outside the defence and security markets. We must develop and evolve means to tap this investment to meet our science and technology requirements; seeking stronger relationships with universities and the Research Councils; removing barriers to private venture investment; and encouraging civil suppliers, SMEs and academia to participate to the fullest extent in providing new technical solutions. We need greater agility to allow pull-through of new technology from the civil sector into defence and security capability. We must ensure requirements are coherent across the large number of organisations involved in using and providing science and technology for defence and security, both to allow greater opportunities for long-term investment by suppliers, and also to allow Government to make the best decisions on quality and value for money. MOD already invests, through the Defence Science and Technology (DST) Programme Office embedded in Dstl, two-thirds of its annual research budget in projects delivered by industry and academia.

95. In the counter-terrorism field, UK Government has developed an approach to accessing innovation in the wider private sector (both industry and academia) and exploiting

innovations to help solve the most difficult challenges. Innovative Science and Technology In Counter Terrorism (INSTINCT) is a cross Government programme, led by the Office for Security and Counter-Terrorism (OSCT), which brings together Government departments and agencies to clearly articulate a problem area, and works at pace with industry partners to find innovative solutions in the broad private sector that may help contribute to solving the problem. Innovation here is defined not just as new ideas (creativity), but the application of ideas in different ways, or the novel combination of ideas, to provide a different way of tackling a problem. Its aim is to find and harness innovation by providing a fuller understanding of the innovation base across the UK (in particular SMEs and organisations who are not traditional suppliers to the defence and security sector), being better able to influence external innovation, and by being better able to exploit the outputs of innovative ideas.

96. The Home Office CONTEST Science & Technology Strategy initiatives such as the Innovative Research Call for new explosive and weapons detection capabilities, co-ordinated by the Home Office Scientific Development Branch (HOSDB), have also been successful in bringing common Government requirements together and sharing these with industry and academia. These have been achieved through pooled funding and a joint assessment of innovative ideas and proposals and are delivering new concepts for many security agencies. Similarly, Dstl has worked across the supply base and with international partners on a range of initiatives to create innovation solutions to defence needs.

97. To increase access to innovation MOD has established the Centre for Defence Enterprise (CDE). The CDE is MOD's first point of contact for anyone who wishes to submit a research idea with a defence application. CDE places its emphasis on open innovation and attracting suppliers from non-traditional areas who are new to the defence market, in particular small SMEs, academia (university departments and spin-out companies), and individual innovators.

98. Other wider engagement initiatives have been explored in recent years; these include establishing a number of Defence Technology Centres and consortia for delivery of science and technology, for example, the Haldane-Spearman Consortium for Human Sciences. Most recently, building on links within the supply chain for Weapons and improving access to SMEs, we have established a Weapons Technology Centre. This allows coherent planning and delivery of science and technology at low to medium maturity, for the Team Complex Weapons sector, providing industry with a clearer view of MOD's requirements and allowing industry to innovate and influence technology investment at an early stage of acquisition. Similarly, an Armour and Protection Science and Technology Centre established in Dstl has held successful joint calls for proposals with the Engineering and Physical Sciences Research Council.

2.2.4: Exploitation of innovation and reducing cost of ownership

99. The potential benefits of reducing cost of ownership for UK Armed Forces and security agencies of meeting the many challenges with technological ingenuity will only be realised if innovation is generated from the widest possible source of supply and, perhaps more importantly, properly exploited to be delivered in time to be used. There are, however, risks in embracing fast adoption of innovation.

100. The need for certainty on many aspects of equipment beyond mere functional performance has always created tensions in the procurement of military and security equipment. For the military, these can be relaxed for one-time use purchases in direct support of operations where increased risk is accepted, and in these instances the Urgent Operational Requirement (UOR) process has proved very effective. However, a

key driver for equipment at the core of our Armed Forces, which often comprise large, complex systems and vehicles, remains reduction in the cost of long-term ownership. This has often presented barriers to the introduction of the most recent technology into these large systems. Work has been progressing in MOD and Industry into facilitating technology insertion into systems, improving reliability and capability, and reducing the cost of ownership. In security, while there are fewer long-life systems, the need for reliability and, in some cases, secrecy, has similarly reduced the opportunities for using innovative products.

101. The key to making best use of technology opportunities will be effective exploitation of systems engineering and open systems, both to integrate new technologies into existing systems and also to allow new capability to be developed as disruptive technology comes along. Early identification of the route to exploitation is essential for science and technology. This should enable rapid improvement in military capability within the timelines commercial technology development allows. To do so effectively, Government must have, or have access to, people with the science, technology and engineering skills to understand and exploit commercial innovations through adaptation into defence and security equipment and capability.

102. In order to exploit the potential for innovation to increase efficiency and reduce costs, we must embrace the adaptation of civil technology, which may be well matured; and not confine innovation to a search for inventions and unique new technologies. Adaptation and systems integration is also likely to be a key cross-discipline approach for many sectors of the economy if the exploitation to market of technological innovation is to make an impact on the nation's financial growth.

103. Government must also seek disruptive innovation, which leads to changes in the way we approach military and security action. It is already clear that cyberspace and space utilisation has, and will continue to have, an increased influence. But the search for innovation has, like all investment decisions, to balance the exploration of game-changing phenomena with insertion of advancing technology and technological techniques into the existing concepts, equipment and infrastructure.

2.2.5: Being a customer of capabilities that are dependent on science and technology

104. Many aspects of the UK's critical defence and security capabilities are either bespoke or adapted for specific purposes and highly technical. Our capabilities are used in demanding environments and there is an essential need to understand how they behave in deployment and use. As a customer for such capabilities, we need to be intelligent in what we buy, knowing which elements of technology are important and achieving overall value for money.

105. As more capability is bought off-the-shelf, there is greater potential for it to incorporate civil technology used in ways we cannot easily determine from available information, where we have little expertise either in-house or through supply networks and close allies. This gives rise to considerable risk that Government will not have complete control and understanding of how to use and manage these capabilities in a safe way. The risks are compounded where, in achieving operational advantage, Government seeks to modify or adapt capability it buys off the shelf.

106. The main challenges facing us in planning and buying capability involving complex science and technology, are how to achieve a technical understanding necessary to achieve value for money in the procurement, and how to understand the technical aspects of safety, legal, ethical and environmental constraints in use of the capability.

Across the breadth of capability, we must decide where Government must own such scientific and technical knowledge and expertise, and where we can rely on and use networks to maintain this expertise. We also need to decide the architectures and specific systems designs we must adopt to minimise the risk that we cannot operate our capability effectively and safely. Prioritisation of our investment must provide a balance between developing new science and technology against maintaining our ability to be an intelligent customer of capability embodying science and technology, whether exploited from our own research or from elsewhere.

General question:

Q11. What should be the balance of priorities for research investment in science and technology for defence and security purposes?

Specific questions:

Q12. Given the changing defence and security threats, the breadth of science and technology providers, the pace of innovation and defence's ability to influence this, what should be the balance of priorities for the science and technology programme over the next five years and beyond, including support to setting policy, developing force structures, tactics, training and doctrine, and for planning, delivering and generating capability needs, while maintaining value for money?

Q13. How should we develop our strategy for international research collaboration to support interoperability, operations, wider diplomacy and achieve better science and technology outputs?

Q14. What should be the balance between research focused on long-term potential threats and conflicts and that supporting current operations and procurement of equipment & services in delivering the SDSR?

Q15. How can we rigorously and robustly identify those areas of science and technology that need to be sustained in order for us to have a capability a) in Government and b) within the UK?

Q16. How should we engage with the wider supplier base and exploit innovation to meet our research priorities?

Q17. How should Government access the widest possible supplier base (industry, universities, and research organisations), ensuring there are no gaps or overlaps, and what mechanisms should be used (existing or new fora, internet, etc.) to ensure both traditional and non-traditional suppliers understand our strategic direction, priorities, and detailed requirements for science and technology, yet maximise pull-through to exploitation?

Q18. What are the opportunities for expanding the role of the Centre for Defence Enterprise or using this model more widely across defence, security, and the cyberspace domain?

Q19. What mechanisms are needed to facilitate better use of science and technology to improve the export potential of equipment, either within defence or civil spin-offs, and reduce the cost of capability produced in the UK?

Q20. How can we realise the potential benefits from innovation through open systems and modular acquisition, while still achieving value for money?

Q21. How do we maintain a capability edge in the innovative use of commercial off-the-shelf (COTS) components through the life of a military or security capability?

Q22. How do we generate a technology edge for example, by new systems concepts, which focus more on particular critical areas within the overall system of capability?

Q23. In buying capability which contains complex science and technology, how should we ensure our choices are based on intelligent and sound evidence-based decisions?

Q24. What are the main elements of being an intelligent customer for capability, equipment and services which depend on science and technology, to enable better value for money and reducing the overall cost of our capability?

Q25. How do we maintain a capability edge in the innovative use of commercial off-the-shelf (COTS) components through the life of a military or security capability?

2.3: Broader Policy

107. Our policy of seeking to fulfil our defence and security requirements through competition on the global market is complemented by the actions we will take to promote the competitiveness and long-term viability of UK-based companies. In parallel, we also have specific broader requirements, for example to support civil security and resilience by certifying the quality of security professionals, products, and services.

2.3.1: Exports

108. The Prime Minister has said 'promotion of British commerce and international trade [is] at the heart of our foreign and economic policy'[8]. Our strategy includes 'getting behind those industries where Britain already enjoys competitive advantages' and 'make it easier for new companies and innovations to flourish.' The MOD Business Plan for 2011-2015 includes in its Vision the priority "To promote defence exports consistent with export control criteria; as part of a defence diplomacy programme to strengthen British influence and help support British industry and jobs".

109. The Government believes that our defence and security industry already has many positive attributes. It represents a significant proportion of the UK's advanced manufacturing base, enjoys a strong global market share, and is a world leader in research and technology development – as well as in some security-related products and services (such as key aspects of cyberspace security). UK defence and security exports have been particularly successful in recent years, achieving over £7 billion revenue in 2009 and some £54 billion over the last 10 years[9]. The UK was the second most successful defence exporter in 2009, achieving an 18 per cent share of the global market, close to the Government's longer term target figure of 20 per cent. UK security exports in 2009 were around £1.4 billion[10], an increase of 14 per cent on the previous year. We must not be complacent, however. The UK has a comparative advantage, but

8 Speech to the CBI Annual Conference, 25 October 2010.

9 Derived from Table 1.14 in UK Defence Statistics 2007 & 2008 and Table 1.13 in UKDS 2009 & 2010. In 2007, the UK was the most successful defence exporter in the world.

10 UKTI DSO symposium: https://www.eventsforce.net/OXYGEN/media/uploaded/EVOXYGEN/event_188/UKTI%20DSO%20Symposium%202010%20Market%20Review.pdf

the export potential is not being maximised. With further encouragement, companies – large and small – could benefit significantly more by increasing their exports, while simultaneously helping to fulfil our wider foreign and economic policy objectives.

Defence and security benefits

110. Exports have an important part to play in the UK's defence and security arrangements. They help to consolidate existing bilateral relationships with key allies, as well as contributing to the development of other important relationships, establishing areas of mutual interest and cooperation. By helping other nations to build up their own defence and security capabilities, we can contribute to regional security, and help tackle threats to UK national security closer to their source.

111. In the right circumstances, exports can also reduce the costs of programmes to the UK. Export customers help to spread the costs of fixed assets needed for long-term support and allow the Government to recoup some of its investment by levy. If orders are received early enough, these can help spread the very large non-recurring costs of research and development over increased production runs, and reduce the unit costs through economies of scale and learning.

112. Successful exports also improve the long-term viability of our suppliers, helping to smooth out the impact of fluctuating or limited domestic demand, and potentially ensuring that industrial capabilities that are essential to our national security are sustained.

113. In order to stimulate innovation in cyberspace security, it is necessary that the Government supports the UK's cyberspace security supply chain by promoting UK capability to foreign governments and private sector customers alike. The UK is a global leader in niche areas of cyberspace security and the Government will do more to support this important industry sector.

Exports and growth

114. Promoting exports is also part of the Government's wider agenda for export-led growth. Defence and security companies make a significant contribution to national prosperity, as well as to our advanced manufacturing and technological capabilities. We want to do more to foster a new economic dynamism, by backing those industries where we believe the UK enjoys competitive advantage, gearing our Diplomatic Service more effectively to support exports, making it easier for new companies and innovations to flourish, and ensuring SMEs have greater opportunities to reach their full potential and contribute to the UK's recovery.

Exporting responsibly

115. While we wish to promote defence and security exports and to increase the UK's share of the world market, we are committed to maintaining the effectiveness of the UK's strategic export controls to facilitate responsible exports and safeguard our national security. Through an effective framework of controls, including by assessing all applications against the Consolidated EU and National Arms Export Licensing Criteria[11], we aim to ensure that sensitive goods and technology are kept out of the wrong hands.

---

11 Consolidated EU and National Arms Export Licensing Criteria, published in Hansard on 26 October 2000 at column 200W: http://www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1084563563

116. The UK has been at the forefront of international efforts to establish global standards on arms export control. We led our partners in the EU in the adoption of a legally binding, Common Position on arms export control, which reflects the UK's own high standards; the EU Code of Conduct on Arms Exports was adopted during the UK's Presidency of the EU in 1998. And the UK has taken the lead in efforts to agree an Arms Trade Treaty (ATT), which would be a legally binding, international treaty, setting high standards for the regulation of the global arms trade. We continue to be committed to the goal of a robust and effective ATT, and play a full part in the current negotiations for an ATT. Additionally we provide British technical and political expertise in support of multilateral regimes, working to establish clear guidelines on what exports should be controlled.

117. We will retain robust export licence processes, which allow the Government to assess the risk of releasing protectively marked information and exporting controlled items. However, we will continue to keep this regime under review to ensure we are delivering an efficient and streamlined service. In particular, we will increase the use of open licences for lower risk transactions, while continuing to focus most effort on the areas of greater risk. We recognise that the speed of decision-making on export licences, whatever the outcome, is important to potential exporters.

118. We recognise that those doing business abroad, in unfamiliar cultures, may face difficult ethical issues. However, the Government's position is clear: our support for promoting UK exports does not include accepting corrupt practices. We expect all those involved in UK exports to adhere to UK law, including the Bribery Act 2010, and we will continue to engage with other exporting governments to ensure this does not disadvantage UK exporters.

Challenges

119. There are challenges to supporting defence and security exports more effectively, some of them arising from other issues in this paper.

120. In the same way that the UK values the positive contribution that exports make to bilateral relations, so some customer countries see buying from the UK as an important factor in building their relationship with the UK. They seek complete packages of capability, including equipment, support, and training, which places a premium on being able to offer such packages and to provide appropriate support at Government level.

121. Both export customers and UK exporters sometimes regard direct Government-to-Government (G2G) involvement as necessary to secure a sale[12]. This reflects the highly political and strategic nature of decisions to buy major defence capabilities. Our competitors in this market certainly use a variety of G2G arrangements to support their national industries. Direct involvement, however, raises issues about training capacity[13]; charging regimes; the extent to which Government has a formal role in, guarantees, or

12 For example, there are particular market failures in respect of adequate customer information about the quality of defence products and services. Correcting these is one of the reasons why the Government, including the Armed Forces, need to play a role in marketing to other countries.

13 For example, it is long-standing policy that UK training capacity is set according to the UK's needs and not to support export-related training.

underwrites major export packages[14]; and the prioritisation of other resources, such as project teams, needed to underpin G2G arrangements. A G2G arrangement will involve not only some significant administrative costs, but also potential financial or reputational risks for the UK.

122. Sometimes other choices we have made may limit UK export opportunities. We may prohibit the export of some goods, services, or technologies for reasons of national security. Where our requirements are being met through an international programme, this may involve significant export opportunities for UK companies within the programme, but less involvement in sales of the final platform and its through-life support. Since one of the key factors in successful defence and security exports is often having equipment in use by the UK Government, it follows that where we purchase off the shelf from overseas, the opportunities for exports are lost. Similarly, the existence of an exportable product is always the result of and therefore dependant upon an earlier decision to invest in a particular industrial capability.

123. We must also be hard-headed about our prospects. The UK has a very successful track record in defence and security exports sales, but in the defence sector this is heavily focused on specific capabilities, sectors, and markets; and in the security sector fragmented domestic and overseas customer markets inhibit our progress. It is, therefore, in the interests of Government and industry that the UK is competitive across a broader range of products and markets. And it is in all our longer term interests to protect the UK's reputation. Poor experience with a UK programme, whether on the original purchase or subsequent customer support arrangements, can harm the prospects of any UK exports for years to come.

Way ahead

124. These challenges require a fresh approach in response if we are to maintain, or increase, our share of the global export market. First and foremost, all UK Ministers are now more personally involved in supporting defence and security exports. It is a principle of this Government that, when travelling abroad, Ministers from all departments are there in part to promote the UK and what it has to offer. When visiting a country, all Ministers are briefed on and expected to raise important export prospects with their interlocutors.

125. In the past, the MOD has sometimes set its equipment requirements so high that the resulting systems exceeded any potential export customer's needs or budget. As highlighted in the SDSR, we believe one way to increase the UK's share of global defence exports is to consider export-related issues early in the MOD's own acquisition cycle, while ensuring that our Armed Forces continue to receive the equipment capabilities and support they need. We are, therefore, considering how to modify the way the MOD specifies requirements, in order to create parallel opportunities for related equipment to be sold on the global market. One approach we are exploring is to work with industry to specify broad parameters for our equipment requirements, which allow for export potential, and then to use methodologies such as modularity, open systems, and technology insertion to meet the UK's specific requirements, whilst industry adopts similar approaches to meet overseas customers' needs.

126. This also has the potential to make our defence and security capabilities themselves

14 The Export Credits Guarantee Department (ECGD) is the UK's official export credit agency. ECGD works closely with exporters, banks, buyers and project sponsors supporting exports to, and investments in, markets across the world. ECGD complements the private market by providing assistance to exporters and investors, principally in the form of insurance and guarantees to banks, taking into account the government's international policies.

more affordable. While the Government wants to ensure that defence requirements allow for future export potential, this will only be successful if industry can, in turn, offer concrete benefits to defence programmes and budgets. Early work by Team Complex Weapons and on the Global Combat Ship is demonstrating the value of linkages at the earliest stages between MOD, UKTI Defence and Security Organisation, and industry.

127. This requires adopting new approaches to our own procurement programmes, with Government and industry working together to identify how early choices could potentially improve export prospects. This means designing solutions with exportability in mind; making greater use of modularity and open systems in a cost-effective way; and adjusting programmes, having considered the qualitative and quantitative benefits to be gained from exports, underpinned by robust market analysis of customer requirements in potential export markets. The onus is on industry, however, to become ever more competitive in the global market, and to develop the world-class capabilities required by the UK Armed Forces and the wider national security and law enforcement community, while at the same time exploiting export potential.

128. The Government's principal agent for the promotion of defence and security exports will remain UK Trade and Investment (UKTI), who will operate a robust prioritisation mechanism to ensure that the Government is able to identify and focus on those campaigns which have the best prospects for the UK. However, as the SDSR acknowledged[15], many Government departments have to play a role in delivering defence and security overseas. The MOD, the Home Office, the Foreign and Commonwealth Office, and the Department of Business, Innovation and Skills have key roles in supporting defence and security exports. We will explore ways in which to bring together all the departments and agencies involved in support of a comprehensive national strategy and delivery plan for defence and security exports, on behalf of the Prime Minister.

129. Exportability will help address the competitiveness of UK industry in the next generation of equipment. The Government will continue to promote open markets in defence and security capabilities. But we also need to consider how to provide Government support to current and shorter term export prospects for existing equipment. This will include campaigns supported by departmental staff and equipment, as well as the provision of exportability planning resources. Use of these resources will have to demonstrate best value for money.

General questions:

Q26. How can the Government and industry best support responsible defence and security exports by UK-based companies?

Q27. What are the current obstacles to doing so and how could these be overcome?

Specific questions:

Q28. How can the Government diversify the destinations for UK defence and security exports and at the same time ensure it has a pan-Government approach to prioritising Government support to export campaigns?

Q29. Is a fresh approach needed for a world where export prospects will increasingly involve industrial partnership and technology transfer?

15 SDSR, section 6.4

Q30. How can Government and industry best deliver international defence training in support of exports?

Q31. To what extent can modularity and open systems – needed in future Government requirements to enable greater agility and adaptability – provide a framework for industry to generate export solutions tuned to global markets?

Q32. Can the Government streamline its security and export control processes consistent with this objective?

Q33. Are there any other aspects of Government–to–Government support which will prove particularly decisive in winning future business in a competitive environment?

Q34. To what extent should the Government provide export credit guarantee finance for defence and security exports?

Q35. How can industry incentivise Government consideration of export potential in its own requirements by providing measurable cost benefits to Government programmes?

Q36. Do any international regimes inhibit responsible exports and prevent UK exporting abroad?

2.3.2: Small and Medium-Sized Enterprises (SMEs)

130. In the defence and security sectors, SMEs are often an important source of research and innovation, as well as offering adaptability and flexibility. We are, therefore, taking steps to encourage SMEs to participate more fully in these sectors, by making opportunities more accessible and transparent, by removing disproportionate bureaucracy and by ensuring prompter payment. We are also keen to explore whether we can take steps to facilitate SME access to larger contracts normally placed with major prime contractors.

131. SMEs are those that employ 250 or fewer people[16]. We believe small businesses are often more flexible and responsive, offering imaginative solutions to defence and security requirements. These qualities are particularly valuable, as the UK must be agile and innovative in the face of emerging and evolving threats, as well as strive to find new ways to do more with less. Many SMEs in defence are employed in the manufacturing supply chains typically engaged in highly skilled, low volume, niche manufacturing. There are also many SMEs involved in providing innovation through research and technology, and in providing a wide range of services to the MOD. In the UK security market SMEs are equally important, playing a vital role supplying niche products and driving innovation.

132. Progress is already being achieved in defence and security in making Government procurement easier and more accessible for SMEs – in other words, by removing barriers to their participation. A number of measures are firmly in place, including the MOD's Defence Suppliers' Service, dedicated to helping prospective new suppliers through a helpdesk and 'outreach' service and a popular 'Selling to the MOD' brochure. Within UK Trade and Investment, a Small Business Unit operates a 'charter' scheme to help SMEs identify and pursue export opportunities. The Centre for Defence Enterprise provides an important 'gateway' between the department and innovators with new technologies

16 The EU definition of a SME includes turnover and balance sheet values.

offering potential defence applications, and the MOD's Framework Agreement for Technical Services (FATS) has been successful in streamlining the procurement of technical support, opening up that market with almost 400 companies, about 100 of which are SMEs.

133. The MOD is also a signatory and supporter of the Aerospace | Defence | Security '21st Century Supply Chains' programme, where customer organisations work coherently together to improve the efficiency and competitiveness of the supply network; and we have appointed a senior Supply Network Champion to oversee commercial policy development in relation to SMEs and supply chain companies. These initiatives have generally been extremely well-received by small businesses, but we recognise that there may be more Government could and should do, particularly in the security sector, if we are to capitalise fully on what SMEs can offer to defence and security.

134. SMEs are not, of course, unique to the defence and security sector. It is estimated that SMEs represent 99.9% of all UK businesses and account for over half of private sector employment[17]. The UK's 4.8 million SMEs are critical to the economic health of the UK, as recognised in the Coalition programme. Looking at the ways to remove the barriers to participation for the defence and security market will improve the opportunity for SMEs to provide vital innovation in supporting the Armed Forces and the wider security apparatus; but it will also contribute to the wider Government's objectives where SMEs are seen as critical to the UK's economic recovery and future growth. The Government has made a number of commitments to help small businesses, including affording them better access to public sector procurement opportunities. The Coalition programme states: "We will promote small business procurement, in particular by introducing an aspiration that 25% of Government contracts should be awarded to SMEs". Work is already underway to make Government procurement easier for small businesses[18].

Government's challenges

135. Representations received from SMEs and representative bodies suggest that they face a number of key challenges when looking to supply goods and services to the Government. These include a lack of transparency and access to new business opportunities; delays and uncertainty over programmes; often complex, demanding, and inflexible procurement processes, which favour traditional defence and security suppliers; and concerns over losing IPR when working with primes. Representations also highlight the critical importance to SMEs of receiving prompt payment from Government, primes and sub-contractors. In the security market, the lack of coherent requirements, and particularly the fragmented market-place, makes it almost impossible for an SME to move into the security area without a large company to act as a broker.

136. As we implement the SDSR, we must drive greater efficiency into our mainstream acquisition process in order to deliver our programmes more effectively and with less internal manpower. This shift in approach will create many more opportunities for

---

17 'Small and Medium-sized Enterprise (SME) Statistics for the UK and Regions 2009'; 13 October 2010 (http://stats.bis.gov.uk/ed/sme/). 75% of all SMEs have no employees (i.e. they comprise sole proprietorships, partnerships compromising only the self-employed owner-manager(s), and companies comprising only one employee director).

18 On 1 November 2010, the Government announced a series of measures to help SMEs, including: the introduction of a simplified and standardised Pre-Qualification Questionnaire for central Government Departments; an investigation into the use of more open frameworks or dynamic purchasing systems that do not lock suppliers out of contracts for up to 4 years; the launch in March 2011 of a new web portal - Contracts Finder - which will be the single place to find procurement opportunities; and to reaffirm the commitment that 80% of prime contractors are paid with 5 working days and that prime contractors pass 30 day payment terms down the supply chain.

SMEs who specialise in providing independent, specialist advice to Government as an 'intelligent customer' of the defence and security industry. The challenge will be to ensure that we do not risk losing out on innovation through having less visibility and engagement at the lower end of the supply chain. The following paragraphs describe some of the measures we are looking at to achieve this.

Greater access and transparency

137. We need to facilitate easier access for SMEs to defence, security and cyberspace programmes. As well as being advertised in the Official Journal of the European Union, defence contract opportunities over £40,000 in value are currently advertised in the Defence Contracts Bulletin, available on subscription both on-line and in magazine format. Opportunities between £20,000 and £100,000 are also displayed in the Government's Supply2.gov.uk electronic portal. To further improve access to opportunities, the Government will shortly introduce a free-to-search advertising portal, known as 'Contracts Finder', covering the whole UK public sector including defence and security. As with the Defence Contracts Bulletin, the new portal will include a facility for prime contractors to advertise opportunities for potential sub-contractors.

138. To improve transparency, new central Government tender documents for contracts over £10,000 in whole life value will be published on-line, and all new contracts are to be published in full from January 2011[19]. The Defence Technology Plan was established to provide an on-line guide identifying all MOD research requirements, but we need to build on this to determine the best means of engaging with industry and academia. In the security sector, steps have been taken to improve clarity of our requirements through the publication of several brochures in 2009 that outlined the key requirements in counter-terrorism. We would like to go further by bringing together our unclassified requirements for tackling terrorism and serious organised crime and publishing them on a regular basis.

Procurement process streamlining and improvement

139. We recognise that Government procurement processes may appear too complex and demanding for smaller companies, and indeed for larger concerns, so we are working on simplifying them. The Government has mandated the use of a single standard Pre-Qualification Questionnaire (PQQ) across central Government departments. This means that SMEs will be asked for the same basic information when applying to be selected to tender for central Government procurements. Departments will still ask for additional project-specific information. This should save suppliers time and effort.

140. The MOD recognises that subcontractors, including SMEs, would benefit from standardisation of certification requirements required by our prime contractors and we will consider how to bring improvements to the process, including consideration of whether our third party certification policy could incorporate the requirements of the A|D|S Supply Chain 21 scheme.

141. Suppliers, especially SMEs, benefit already from the MOD making available free of charge access to over a thousand UK Defence Standards from its website www.dstan.mod.uk on a 24/7 basis. However, MOD is aware that SMEs are still not contributing as much as they could to the standards-making process. MOD would like to understand

19 MOD has a very large volume of contracts and therefore has been given a limited (12 month) concession to exclude 37 warlike stores as defined in TFEU Article 346, and to redact military sensitive technical information where necessary.

how more stakeholders in UK industry could contribute to and (through early awareness) benefit from the development of defence standards. Other stakeholders such as academia and trade associations also have a role to play, but MOD is not aware of any perceived obstacles to involvement other than costs and time.

142. The 'Reverse Auction' (RA) process, now used on a range of procurements, is an e-procurement tool which may be useful to SMEs, particularly those that have little or no experience of supplying to the MOD. Unlike the traditional tendering process, the bidder has visibility of the price differential and lowest competitive bid during the auction. This kind of market information should be valuable to suppliers irrespective of whether they are successful in a RA, and can be useful to a bidder in re-examining their own supply base and processes in order to become more competitive in the future. However, we are aware that some SMEs have concerns about the process, suggesting that it can, for example, facilitate predatory pricing and focus too much on cost instead of quality and other factors. We need to use the technique with care and would welcome specific views.

Procurement approach

143. The Government acknowledges that consortia of small companies can offer a suitable route for SME engagement and welcomes proposals that represent sound business propositions and offer value for money. We will consider whether MOD guidance should encourage procurement teams in certain cases specifically to welcome bids from consortia.

144. We will also consider mandating the requirement to submit and maintain make/buy plans (which cover proposals for using competition at sub-contract level, for advertising opportunities and for encouraging SMEs to bid) when calling for non-competitive tenders. In the case of competitive tenders, we could require bidders, at the 'preferred bidder' stage, to provide a list of expected sub-contractors, including SMEs.

Framework and Consolidated Contracts

145. To improve SMEs' access we will consider publicising the list of companies being invited to bid for contracts under the Framework Agreement for Technical Support (FATS). This would help SMEs decide whether to bid, and to facilitate the creation of alliances where small companies may be able to submit a strong bid.

146. Aggregating requirements into large, centralised, contracts to maximise value for money through economies of scale can potentially close off opportunities for SMEs which might otherwise be able to bid for smaller packages of work at a more local level. We therefore need to ensure that smaller companies are able to participate, directly on occasions where they can offer better value for money, or as subcontractors.

Innovation and Intellectual Property

147. The Government expects its prime contractors to treat their suppliers fairly and to respect other companies' intellectual property (IP). Ultimately, suppliers must take responsibility for protecting their own IP, but the UK Intellectual Property Office (www.ipo.gov.uk) can provide advice and also an inexpensive mediation service to assist in the resolution of IP disputes.

148. One particular route which has allowed SMEs a route to providing innovation is through the establishment in 2008 of the Centre for Defence Enterprise (CDE). The CDE utilises a secure online proposal and assessment portal which allows simple application and rapid assessment, enabling a decision within 15 days – vital for SMEs who require a quick turnaround on decisions to match often dynamic order book and cash flows. To date around 60% of contracts from CDE have gone to SMEs.

General questions:

Q37. How can the Government ensure that SMEs are better able to fulfil their potential and contribute to the UK's defence and security requirements?

Q38. What are the current obstacles to this happening and how can these be overcome?

Q39. How can the Government manage better the risks associated with procurement from SMEs?

Specific questions:

Q40. Should new requirements be exposed to industry at an earlier stage, potentially to allow SMEs and innovators to propose 'non-traditional' solutions?

Q41. How can the Government encourage greater SME participation in major projects while still maintaining value for money?

Q42. Should MOD's prime contractors be required to advertise competitive subcontract opportunities in the Defence Contracts Bulletin and on-line portals?

Q43. Should prime contractors be required to measure the percentage of work placed with SMEs and to report this to Government?

Q44. In the case of competitive tenders, should bidders, at the 'preferred bidder' stage, be required to provide a list of expected sub-contractors, including SMEs?

Q45. How can the Government encourage greater cooperation between SMEs to form consortia and alliances to increase the competition level?

Q46. Are there any significant obstacles that prevent SMEs from contributing to the development of Defence Standards?

Q47. How can Government encourage and 'champion' greater pull-through of innovative ideas into applications and contracts?

Q48. How should the Government balance the effectiveness of consolidating its purchasing power with the importance of supporting SMEs?

Q49. What specific measures can the Government take to promote greater export success amongst SMEs?

Q50. What barriers are there to SMEs growing to compete as prime contractors for major defence contracts?

Q51. With the move to leaner and more efficient Government machinery, how can we ensure that we do not lose our ability to talk to and engage with SMEs?

Q52. What framework should be put in place, or assistance provided, that will aid SMEs to more confidently work with primes knowing they have taken the right steps to protect their IPR?

Q53. How can prime contractors work with SMEs to facilitate innovation and assist their entry into international markets?

Q54. How can Government ensure that its procurement processes take proper account of the quality of a bid and reliability of the bidder, so that SMEs are not disadvantaged?

2.3.3: Working with our suppliers

149. The Government's aspiration to get the best from our suppliers in the defence and security sectors has two distinct aspects: where to use an external provider – rather than in-house resources – to support and sometimes deliver capability; and how best to work with our suppliers over the life of a programme.

150. The boundaries between the public sector and industry continue to shift. The Government's use of contractually delivered services continues to grow and replace traditionally procured and supported equipment. We have also entered into more long-term working arrangements, which tend to involve industry becoming more deeply involved in public sector activity.

151. For example, the Police Service makes increasing use of outsourcing and the role of contractors in support of deployed operations has progressively increased in every decade since the Second World War. Virtually all aspects of central Government information technology infrastructure, development, and support are contracted-out. The growing use of outsourcing of various kinds has, however, also been the subject of criticism. The central issue for Government, therefore, is to determine the optimum boundary for industry involvement – in terms of roles, locations, and environments, based on operational, legal, safety, and commercial factors – as part of the drive to achieve greater value for money.

152. The relationship between Government and its suppliers is fundamentally commercial. Both sides' rights and obligations are embodied in contracts. Working together successfully, however, requires a broader but no less robust approach, including working jointly towards improving performance, encouraging positive behaviours on both sides, and facilitating each side to make a better contribution.

153. In the cyberspace domain, Government has clearly signalled that its transformative programme will not be deliverable without a new and innovative approach to policy and capability co-design with its suppliers. We will continue to develop this collaborative approach jointly with the private sector and will bring forward plans in parallel with the publication of a new Cyber Security Strategy in 2011.

154. We will be focusing our own research investment to ensure that the Government is an intelligent customer of the widest range of external research and that it enables industry to pull-through and develop technology for defence and security use.

155. We will, therefore, be creating opportunities for current and potential suppliers to offer solutions that are more efficient and effective in delivering our defence and security related research, equipment, and support requirements in future. And we will also be considering how methodologies such as open systems architecture, modular design, spiral development, and technology insertion can contribute to developing more flexible and agile capabilities in future.

156. We are also providing greater transparency, clarity, and therefore certainty about the Government's current activities and future intentions, in order that industry and academia can invest in the UK with greater confidence. For the MOD, this will be considered as part of Defence Reform. Providing greater clarity about future intentions in the security sector is challenging, because of the many different public sector organisations involved. We are, however, seeking to make more information available about unclassified requirements.

157. Setting standards for security equipment (for example those regarding body armour or

video analytics) has been shown to be a successful method for sharing challenges with industry and academia. Government would like to extend this approach to other parts of the security domain.

2.3.4: Wider impacts

158. The Government believes that every pound allocated for defence and security should be spent to benefit the UK's national security. The over-riding concern, especially in difficult financial times, must be to provide the UK with the capabilities it needs. However, there are significant wider impacts.

Skills

159. A skilled workforce is essential for delivering the capabilities that we need for our defence and security. This depends on retaining and developing key skills in Government departments, in the Armed Forces, the agencies, and police, and in industry. In certain areas niche skills are critical to sustaining particular industrial capabilities in the UK, in order to maintain operational advantage and/or freedom of action in the range of operations that our Armed Forces may need to conduct. The retention of such skills applies not only to those related to industrial capabilities; but also to the wider science, technology, and engineering base that provides us with the know-how to design, develop, support, maintain and upgrade key systems and sub-systems.

160. Without readily available specialised knowledge we would also lose the ability both to react quickly to urgent operational requirements, and also to make reliable informed decisions as an intelligent customer based on the correct interpretation of complex underpinning scientific and technical data. Therefore, the skills development and retention of our people is fundamental to ensure that the Armed Forces and security agencies continue to receive the essential equipment, support, services and technology they need. A strong and healthy skills base in the UK also helps the productivity and competitiveness of the economy, helping to ensure that all businesses are equipped to compete in an increasingly competitive and open market. A skilled workforce will help to stimulate the private-sector growth that will bring new jobs and new prosperity for the UK[20].

UK economy

161. The sheer scale of Government annual defence and security expenditure with industry and commerce – MOD spent nearly £19Bn with UK industry in 2008-09[21] – means that our decisions have a significant and long-term impact on the health and resilience of UK industry and therefore on the livelihood of many citizens. Many billions more are spent by the security sector. This supports thousands of suppliers and hundreds of thousands of jobs[22].

162. Defence and security research and development (R&D) investment also has an impact on the wider economy. It helps develop and maintain technological skills within the UK, and creates intellectual property for UK companies. There is also scope for spin-out and spin-in of technologies and techniques between the defence & security sectors and the wider civil sectors.

---

20 The Department for Business, Innovation and Skills' White Paper on Skills for Sustainable Growth, November 2010.

21 Table 1.11 of UKDS 2010 and similar tables in previous years.

22 It is estimated that in 2007-08 there were 300,000 full-time jobs in the UK supported either directly or indirectly by MOD expenditure and defence exports (source: table 1.10, UK Defence Statistics 2009).

163. Another area of wider benefit has come from our industrial participation policy, through which we invite potential offshore suppliers independently to propose opportunities for UK companies to bid for defence related work and to compete and win it on merit. We are reviewing our policy to ensure it remains valid and complements our key priorities. We will also ensure that any changes to our policy are compatible with EU legislation on defence offsets.

164. A competitive and viable defence and security industry is able to compete effectively for international projects and responsible exports contribute to UK growth.

165. Government also has an influence on the health of the defence and security sectors through its policies towards the wider business environment. Government has a wide range of levers with which it can affect this environment, ranging from indirect levers such as stewardship of the economy, to more specific areas of business support. In its roles as supporter, investor and regulator of business, Government has a key part to play in creating the conditions for business success.

166. The NSS emphasises that the security of our energy supplies increasingly depends on fossil fuels located in some of the most unstable parts of the planet. It also highlights our vulnerability to the effects of climate change and that competition for scarce resources, such as rare earth metals, may increase the prospect of global conflicts over access to them. Climate change and resource competition will, therefore, influence where our Armed Forces might be deployed, and the shape of future equipment requirements. The defence sector has an important part to play in helping to reduce the Armed Forces' reliance on fossil fuels, and it can also contribute to achieving the Government's wider aim of moving to a low carbon economy.

General question:

Q55. To what extent should the Government take wider economic considerations into account when taking decisions about fulfilling its defence and security requirements?

Specific questions:

Q56. To what extent does Government spending on defence and security capabilities benefit broader UK manufacturing and services? How could these benefits be increased without prejudicing value-for-money, fair and open competition, or our national security capabilities?

Q57. What approach should be taken to assessing value-for-money in fulfilling defence and security requirements and why?

Q58. What mechanisms could be used to help industry (both defence and civil) better exploit the results of investment in defence research and development?

Q59. How can the Government encourage industry to do more to develop and exploit defence and security technologies within the UK?

Q60. Are there any specific defence and security issues that we need to address for low carbon energy efficient investment and sustainable development research?

Q61. To what extent should the Government encourage/insist on the adoption of energy efficient and sustainable development policies when selecting suppliers?

Q62. How can the Government ensure that the UK creates and retains the skills necessary to support essential national security capabilities? Which skills and capabilities are most vulnerable and what might be done to protect them?

Q63. How can we ensure that our policy on industrial participation delivers the best possible value for defence and security?

Part Three: Specific Areas

167. Parts One and Two of this document looked at issues where there are commonalities and overlaps across the defence and security sectors. Part Three looks at issues that are specific to each of the defence, security and cyberspace areas, where there are differences of priority or approach to specific technology and industrial issues. It touches on a number of topics that will be dealt with in much greater detail in the subsequent White Paper.

168. The four principal areas where there are differences between the defence and security sectors are as follows:

- The market in defence equipment and support is highly focused and coherent, at least at the highest levels, and the MOD is the single buyer. The security sector is much more fragmented, with multiple owners and buyers of solutions. For example, there are 43 police forces in England and Wales with only limited coherence in procurement strategy. Furthermore, security issues are not the exclusive responsibility of Government. For example, most of the critical national infrastructure is owned and operated by the private sector, whilst most of cyberspace exists within infrastructure that is in private sector control.

- The defence market tends to be driven more strategically, with a top-down approach to requirements and a tendency to specify whole system defence capability needs. The security market is mainly driven bottom-up, with no overarching national procurement strategy and a tendency to buy individual equipment solutions, as opposed to holistic system capabilities.

- The defence sector has considerable maturity as a consciously coherent sector, including in its approach to methods of procurement, specifying system level requirements, and considering export potential (including through defence diplomacy), as well as industry acting in the collective interest. The security sector is a much newer sector, though it is developing rapidly.

- Government science and technology in the defence sector is formulated and delivered through a single organisation (Dstl), which provides independent high quality scientific and technical services that are inappropriate for the private sector, and acts as a single portal for reaching private sector innovation to deliver the non-nuclear elements of MOD's science and technology programme. In the security sector, a large number of providers of science and technology advice exist, which need to be co-ordinated together effectively.

3.1: Defence

3.1.1 Capability-related industrial sectors

169. The MOD currently buys a wide range of equipment, support, and services from external suppliers to meet its requirements. At the same time, MOD may be undertaking the relatively straightforward procurement of personal clothing alongside the development and construction of highly complex and advanced nuclear-powered submarines. MOD's current approach is structured around the industrial sectors that contribute to six broad

defence capabilities: maritime (surface ship and submarine), land, fixed-wing, rotary-wing, C4ISTAR[23], and complex weapons.

170. Open competition is used where there is a strongly competitive market for particular equipment, support or services, where the delivery risks associated with acquiring and integrating that equipment into a fighting capability are relatively low, and where there are no national security issues. This has included buying major platforms off-the-shelf when appropriate, including the recent purchase of an additional C-17 aircraft to help meet our strategic air lift requirement.

171. Sometimes there is no effective market for a specific capability or the market that exists is very fragile. In these circumstances, MOD has sometimes guaranteed a programme of work to sustain industrial capabilities that it judges are essential to our national security.

3.1.2 Urgent Operational Requirements (UORs)

172. The considerable effort that MOD has put into UOR development and delivery in recent years has enabled the rapid purchase or modification of equipment to address urgent and unforeseen capability needs. It has been used to great effect in support of our operations in Iraq and Afghanistan. The timely delivery of equipment ranging from the Mastiff protected patrol vehicle to the Sharpshooter long-range rifle has been well received by troops in theatre. Current operations have also resulted in the accelerated development of key areas of defence technology to meet urgent needs. Areas such as ISTAR, communications, unmanned air systems, precision attack, dismounted soldier kit, and vehicles have all benefited from a surge in investment and successful rapid proving trials (often in theatre). Industry support has been excellent in this area and it has also resulted in increased business for some suppliers, sometimes on a spectacular scale.

173. UOR action inevitably focuses on immediate equipment needs, rather than long-term support arrangements or the sustainability of key skills. When the current intensity of deployed operations reduces, niche suppliers may be hit particularly hard; although this could in turn be ameliorated by additional business if a UOR is subsequently taken into the core programme. One of the challenges will be to harmonise MOD's current equipment holdings with its core programme and embed best practice from the experience of managing UORs into normal business.

General question:

Q64. Is the MOD's sector-based approach, based around a dual strategy of competition on the global market and intervention where necessary, the best way to meet the UK's defence capability needs?

Specific questions:

Q65. What are the key sectors in delivering defence capability? Is MOD's current approach to these sectors appropriate in the light of likely future circumstances?

Q66. Should a different approach be taken in any specific sector? What about sectors whose nature is changing (for example, fixed-wing combat aircraft)?

Q67. Are there any other sectors whose characteristics justify a separate sector approach?

23 C4ISTAR is Command, Control, Communications, & Computers; Information/Intelligence, Surveillance, Targeting Acquisition, and Reconnaissance.

Q68. How should MOD balance the benefits of and constraints from making long-term arrangements with a supplier in a particular sector?

3.1.3 Defence support

174. Industry has always played a role in providing logistics and service support to our Armed Forces on operations. However, this role has grown significantly over the past 10 years, with contractors providing vital support in Iraq and now Afghanistan. Experience has also shown that, if used effectively, industry can offer value for money in delivering many of our support services. Therefore, we believe that industry could play an increased role in supporting our Armed Forces of the future, becoming increasingly integrated with our military to provide an optimal, cost-effective, and most critically, an assured service, that does not compromise our success on operations.

175. We are currently looking into ways of developing our support activities with industry. This could include new employment models looking at regular military, reserves, civil servants and contractors working alongside each other to deliver seamless assured support to our military commanders. We would need to be aligned in processes, procedures and information flows so that we can reduce costs, risks and administrative friction.

176. A similar challenge awaits us in the way we contract for services: our current contracting models may need to change to allow us to maximise industry's potential while also offering us an assured service. Looking further out, it is also clear that we can do better in the way both industry and the MOD uses its real estate. As we become smaller and more integrated, there will be opportunities to share facilities and costs, while still delivering an improved assured output for our future commanders.

177. Simulation and synthetic training have been rising significantly in importance in recent years - and particularly in support of current operations - to complement live training for combat and operational roles. MOD is undertaking a systematic review of defence training systems and infrastructure, the acquisition and support for those systems and the opportunities and benefits these will provide.

General question:

Q69. Does the MOD involve industry sufficiently in providing support to the Armed Forces?

Specific questions:

Q70. What support roles should only be delivered by the Armed Forces?

Q71. What support roles could legitimately be provided by industry?

Q72. How can the MOD remain an intelligent customer if it outsources more activity?

Q73. How might MOD enable wider exploitation of simulation and synthetic systems and scenarios?

Q74. How could MOD simplify interfaces, relationships, and decision making to improve the provision of support to the Armed Forces?

Q75. What legal problems do companies face when providing support to operations?

3.1.4 Defence acquisition reform

178. The scale and complexity of defence acquisition presents formidable and ever-increasing challenges, which MOD has sometimes in recent decades not met. For example, when not managing to keep programmes within agreed time, cost, and performance parameters; or not identifying and mitigating risks effectively, as in the tragic loss of the Nimrod XV230. In the latter case MOD's approach to contracting-out functions and managing the resulting industrial relationships was specifically criticised in the Haddon-Cave report[24].

179. Many of these challenges are being addressed through an ongoing major programme of reform in our acquisition framework, which will ensure that our equipment plans are realistic, agile in response to changing military needs, and adaptive to the evolving strategic context.

180. The Defence Reform Unit will fundamentally re-evaluate the way in which the MOD is structured and managed, including for acquisition. It is expected to report its findings to the Defence Secretary in July 2011. This is an internal MOD process and, therefore, not part of this consultation. Industry and other stakeholders will be consulted separately as the Defence Reform Unit's work is taken forward. However, if there are particular issues on acquisition reform that you believe are relevant to equipment, support, and technology for UK defence and security, then please tell us and we will consider them.

3.2: Security

3.2.1: The security market in the UK

181. The UK security market can be described as having four principal sectors:

- integrated security systems;
- security sub-systems, comprising many sub-sectors such as CCTV and biometrics;
- cyber security and information assurance;
- person-based services, including consultancy, training, guarding, and escorting.

182. Any marketplace comprises a demand side and a supply side. Unlike the defence market, the demand side in the security market in the UK comprise both public and private sector organisations. In some parts of the security market the public sector demand side is considerably smaller than the private sector demand side: for example, the demand for manned security guarding. Another difference is that, in defence, the MOD acts as a single source of requirements and a single procurement entity whereas, in security, there are a large number of departments and organisations who act and procure separately (most notably police forces). This separation is useful as it allows the organisations involved to be operationally independent and thus able to address their specific needs. However, this approach also fragments the market, significantly affecting its efficiency and operation.

---

24 Haddon-Cave, The Nimrod Review, 28 Oct 2009; para 25.13.

183. Many of these organisations have similar requirements but it can be difficult for technologies that meet these requirements to enter the marketplace. The lack of centralised or coordinated procurement means companies must market their product to each police force or security agency separately. This is very costly for the private sector and can mean that different parts of the Government's security infrastructure use different technology for the same ends, hampering interoperability, or worse, the private sector may not consider it worthwhile to address the public sector market.

184. In some cases centralisation and coordination of the security market could achieve large savings for Government if procurements were aggregated into national requirements for systems and services. However, such national co-ordination, requiring large-scale production and/or nationwide delivery of services, would make it much harder for SMEs to compete for this type of business. The Government is keen to encourage SMEs in all sectors, not just in the security marketplace, which is in tension with the desire for a more coherent market. An example of this is the current consultation on police purchasing and related changes to Government civilian procurement taking place in the Cabinet Office. This will move towards more consolidated Government procurement and to structural changes amongst purchasers of specific police equipment or capability, leading to joint constabulary procurement of essential services to the police, for example more standard vehicles. The formation of the National Crime Agency will also have an impact and the right balance needs to be struck to make the market more efficient without inadvertently penalising SMEs who have a niche role in the market. The adoption of open standards and open architecture will play a key role in this.

185. The nature of the security sector and the capabilities that Government needs to possess mean that Government must strictly limit knowledge of the extent of certain capabilities, and in some cases even the existence of some capabilities. This need for secrecy justifiably constrains or prevents the Government from revealing some requirements; consequently the wider industry can make no effort to meet these requirements as they are not aware of them. Furthermore, industry may try to develop a capability when Government already has more advanced capabilities, but cannot share knowledge of these capabilities. This means that companies that are unaware are unlikely to see a return on their investment from the UK Government market and industry's investment is unlikely to produce any return in the UK Government market.

186. Even when requirements can be published, there is currently a lack of coordination and coherence in the research and development strategies for the many UK security organisations (although some national-level organisations do share requirements and solutions). Rather than having a unified understanding of the issues from which requirements can be drawn, many organisations raise requirements based purely on their own needs. This 'bottom-up' approach makes it difficult for the private sector to make informed decisions regarding development and investment in the medium to long term.

187. Often technology developments in the security sector tend to be through incremental changes, rather than considering the overhaul or replacement of complete systems. This can manifest itself in a desire to purchase an improved piece of equipment, rather than buy an altogether new technology or make changes at the overarching systems level. In essence, some security customers do not consider and define requirements in a coherent fashion in the way that the defence sector does. Instead, it falls back on local purchasing, makes use of innovations in the private sector that come along, or conducts localized research and development but does not set the overall direction of travel. Aviation security is an example, in which over many years individual aspects of the system have been subject to evolutionary change, without a holistic development of the entire system development. Recent work has endeavoured to change this, moving to

a more systems level approach; ways should be considered to expand this to other areas in the security sector.

188. Taken together, these factors can:

- deter industry from investing in the sector;
- deter industry from developing technologies and/or industrial capabilities;
- increase the costs of security solutions to Government; and
- handicap UK companies wishing to use the UK market as a springboard to the export market for security products and systems.

189. One of the aims of the current work on equipment, support, and technology for UK defence and security is to reduce these problems, while maintaining the advantages of operational independence and market competition. Our policies for achieving this end will follow the key principles set out at the beginning of this document. Our default position is to seek to fulfil the UK's security requirements through open competition in the global market.

3.2.2: Science and technology requirements

190. The approach of the UK Government to tackling these risks is underpinned by the effective use of science and technology, much of which is provided by the private sector.

191. Creating an efficient and effective security science and technology market in the UK requires a much more coherent security sector than we currently have. Achieving this requires that Government: understands the threats and opportunities in science and technology; identifies and shares the key requirements of the security and intelligence agencies with private sector solution providers; effectively exploits science and technology solutions to the benefit of front line security organisations; and works closely with our international partners to address shared risks.

192. In the first place, the UK Government would like to have a more robust, transparent and secure system for identifying the capability gaps across the security domain and communicating the priority requirements to the private sector. However, identifying capability gaps can be a complex process even within a single organization and the presence of many different organizations, each with their own priorities, complicates the issue further, as does the need for secrecy in some areas. However, a comprehensive approach has been developed across the security and intelligence agencies, and the Government has already brought together its counter-terrorism requirements and published these alongside the counter-terrorism science and technology strategy, which was very well received by industry and academia.

193. Another approach is through the Home Office Scientific Development Branch (HOSDB) exhibition, which is a major security equipment showcase hosted in partnership with UKTI DSO. It is a closed, secure event that allows industry providers in the security sphere to meet directly with the users and purchasers of security technology from the UK and internationally. The exhibition provides an opportunity for visitors to discuss sensitive requirements in areas such as counter-terrorism, serious organised crime and border security. As such, it is one of the mechanisms by which Government supports the security industry, and ways should be considered to exploit this to its fullest extent.

194. Government has created strong links with the UK Security and Resilience Industry

Suppliers' Community (RISC), which is an alliance of suppliers, trade associations and academics, representing over 2,000 companies. It currently provides a focal point for the Government to communicate with industry about its counter-terrorism needs, and a number of industry advisory groups (IAGs) have been set up that consider specific counter-terrorism related problems. Ways should be explored to improve the cooperation and to expand coverage to include the wider security agenda.

195. Olympic Security is a key priority for the Government over the next two years. Engagement with industry has been an integral part of this work, and through an Olympic Industry Advisory Group we are engaging with industry partners who can provide experience and expertise to support our work and refine our requirements. The Group will continue to meet right through until the Games in 2012, and will remain an integral source of advice going forward.

3.2.3: Government laboratories and the private sector

196. Once requirements are clearly articulated, delivering national security capabilities across so many organisations is a difficult logistical problem. The Ministry of Defence, the Home Office, the police and the security and intelligence agencies all have their own methods of procurement and delivery, from purchasing commercial off-the-shelf (COTS) products to developing equipment in-house. And this is compounded by non-Government organisations in the security sector, such as airport or airline operators, with whom Government provides guidance and direction through standards, regulation or advice.

197. There are a number of Government laboratories involved in the security arena, providing a wide range of functions, including independent scientific advice, scientific support to front line operations and, in times of crisis, strategic facilities and capabilities, regulation and conduct of research and analysis with security or sensitivity constraints. These Government laboratories each report to different departments and customers, and have different remits. It is essential that all of their security-related work is considered together, to provide a coherent approach to research and development within Government and with our partners in industry. This is essential to avoid duplication and to ensure that technology crosses over easily between domains.

198. However, Government cannot and must not provide all of its security science and technology by itself; a strong relationship must exist with the private sector, including both academia and industry. Some of this work must be carried out in Government owned or run laboratories, but Government will endeavour to use private industry and academia as much as it can.

3.2.4: Security standards

199. Standards play different roles within each of the four sectors of the security marketplace. While it is difficult to create standards for an end-to-end security system, the individual systems are likely to contain product and performance standards along with interface/interoperability standards. In the information arena, standards in encryption and information assurance would be likely. Finally, for people-based services, there would be ISO standards for service delivery in guarding, training for instance.

200. Better use of standards in the security sector could provide many benefits. There could be improved assurance regarding testing and performance. Tests would need only to be carried out once for a product, which could then be marketed to multiple organisations. Standards could also increase confidence in the performance of the successful products, systems, or services. And standards could help with operational collaboration across the

UK security arena (and even internationally) through encouraging technical and process compatibility, plus encouraging investment.

201. Economically, standards can facilitate competition which improves value for money. Standards also help to prevent "tie-in" to certain products, where customers find that it is too expensive to change from their current arrangements, and they encourage the use of COTS products. International standards help to reduce export barriers in both directions: thus they open foreign export markets to UK companies, but equally open the UK market to foreign companies. When UK standards are adopted more widely overseas, this provides clear advantages to UK companies that are familiar with the standards. Such adoption may be by agreement (e.g. at EU level), or by market forces (e.g. VHS over Betamax). Depending upon the type of standard, a standard can stimulate many different companies in a marketplace; SMEs can often find suitable niches for themselves, while larger companies adopt roles that suit themselves. On the other hand, proprietary standards can encourage single winner-take-all situations, with no incentive for the winner to respond to market forces. Standards also facilitate the movement of staff between companies, which is healthy for the workforce and for the wider economy. Taken together, these factors are crucial to stimulating growth in the security market.

3.2.5: Innovation in the security sector

202. The pace of change in science and technology is increasing. New products and software are released so frequently that it is a serious challenge to keep up with developments. Government must make every effort to anticipate the technologies that could be used by our adversaries, and to harness technologies that can help us respond to the threats we face. Innovation is a key part of this to this endeavour.

203. Harnessing innovation can be hampered by the difficulties in bringing ideas to the attention of the right organisations, and by the high risks inherent in exploiting new approaches. As set out above, initiatives such as INSTINCT and the CDE will continue to be refined to improve our access to innovation and new ideas.

3.2.6: The international security market

204. The UK has a worldwide reputation for security expertise and technology. This is due to our long history of applied security, particularly with regards to counter-terrorism, along with strong science and engineering skills. UK security companies and products are thus respected for their fitness and reliability. However, exports of security products and services are not as strong as they could be. This is, in part, due to the issues outlined above.

205. However, for a small number of specialised technologies, the default position is that exports are not allowed unless a special case is made for an export version and accepted by the Government. We propose instead that the default should be that export will be allowed (either as is or as an export version) unless Government makes the case to forbid. The benefits for the private sector are that they can plan on greater sales volumes, are encouraged to invest more, and will recover investments over more sales. This will reduce prices to the Government, improving value for money, and help make other countries more secure, so aiding the UK's security position.

UK security brand

206. The fragmented demand side in the UK security market limits companies in the UK security industry, as it is harder for them to demonstrate an impressive track record of sales and approvals. This creates a handicap to the UK security industry when marketing overseas, and the effect is magnified for SMEs who are less likely to have internationally known company names or brands.

207. These difficulties need to be set against the fact that the UK has a worldwide reputation for policing, and also a long track record in combating terrorism, both domestic and international; and the UK security industry has an equally long track record in providing solutions, systems and equipment to the police and supporting the UK security and counter-terrorism authorities. The UK does not take full advantage of this reputation and this track record.

208. One approach could be to create a UK security brand, in order to promote the UK security industry, similar in concept to that used by DHS in the US. The brand could be based on some form of approval or qualification (to be defined). The system would not replace any current approval or accreditation scheme. Instead it would supplement existing Government schemes for recognition/approval/standards by creating a form of umbrella system.

209. The brand would project a set of values to potential customers, possibly including the following:

- a hallmark of excellence in security;
- track record with, or endorsement by, UK security authorities in an environment with a significant terrorist threat;
- effectiveness, quality, reliability;
- tried, tested, endorsed;
- value for money;
- satisfies the world's most respected police and security authorities.

210. There is therefore a synergy between UK security exports and UK police and security authorities: if the UK police and security authorities procure the equipment, systems, or services, then this is a strong recommendation of both quality and value for money.

Questions:

Q76. What methods can the government use to identify systemic capability gaps and communicate them to industry and academia, while maintaining national security?

Q77. What steps should be taken to make the security market function more efficiently than at present?

Q78. How can Government achieve more efficient procurement in the public sector security market without disadvantaging SMEs?

Q79. How should Government encourage co-ordinated and/or centralised procurement while maintaining competition and innovation? How should Government encourage co-ordinated and/or centralised procurement without disadvantaging SMEs?

Q80. Should the HOSDB standards model be adopted more widely by UK defence and security organisations as a method of encouraging interoperability and efficient procurement while maintaining competition?

Q81. What are the priorities for investment in standards?

Q82. What benefit would standards bring to export potential? To what extent can standards promote UK exports? What effects would standards have on industry and in particular on SMEs?

Q83. What would be the benefits of a possible UK Security Brand? How could such a brand system be operated and funded? How would a company's products qualify under such a system?

Q84. How should the system balance the competing interests of the widest possible applicability and highest standards?

3.3: Cyberspace

3.3.1: Overview

211. Cyberspace encompasses all digital networked activities. It presents substantial opportunities for the improvement of economic and social well-being, but, as the UK's first Cyber Security Strategy set out in 2009, it also harbours new risks. In particular, criminal activity in cyberspace is growing rapidly, which is why the UK must act decisively to improve law enforcement capabilities. Furthermore, there is a real threat to the future growth and prosperity of the UK from widespread economic espionage, and there are new national security risks. In addition, cyber has a cross cutting component in relation to the other topics discussed in this paper. For clarity, however, the scope of this section is, limited to the cyber domain itself.

212. In light of this, the National Security Strategy recognises cyber security as one of four Tier One risks to the security of the United Kingdom and its interests. In response, the Government announced a £650 million investment in a National Cyber Security Programme (NCSP) in the SDSR. The four-year NCSP will commence in FY 11/12 and will drive a transformation in the UK's cyber capability, guided by a new and overarching Cyber Security Strategy. While our strategic requirements in the cyber element of this Green Paper are less mature than in other established domains, we need to work quickly to refine these requirements and our associated collaborative structures with industry and academia. The UK possesses a nascent comparative advantage in this area which has the potential to be a key source of economic advantage to the UK and a driver for growth. However, it risks rapid erosion without coordinated and intelligent investment, outside as well as inside the boundaries of the formal NCSP.

213. The Government's approach to cyber security is intended to send a strong signal that we see the discipline, skills and capabilities of information assurance (IA)[25] as critical

25 Information assurance is the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

to strategic success. This is particularly the case in the science and technology field, where access to robust, flexible and reliable defensive technology that will secure our current and future information systems is a necessary prerequisite for our exploitation of cyberspace to safeguard our broader national security interests, as well as for economic advantage. The Government endorses the emerging consensus that robust IA is a crucial enabler for effective cyber security. We intend to build on our existing National IA Strategy, published in 2007 in formulating our new National Cyber Security Strategy. Further, the NCSP will address the need to ensure the ongoing viability of IA skills and capabilities across government. This will include support to CPNI's role in providing information security advice to the UK National Infrastructure, as well as action to ensure that CESG, the National Technical Authority for IA, retains its status as a world leader in the field.

214. We will not hesitate to be innovative in our approach; as set out below, Government will seek to involve our private sector partners in a new, joint programme of activity to secure the outcomes we need in an extremely challenging spending environment. The cryptographic aspect of IA will provide an early and exemplary test case for the sovereignty issues and policy covered in preceding sections of this Green Paper. As those sections set out, high grade cryptography remains strategically vital across Government. The need to protect and manage our high-grade information, wherever it is in the world, creates a sovereign requirement to control those aspects of cryptographic production, deployment and support that are critical to the integrity of the product, and therefore national security. Government therefore intends to co-develop and promulgate a coherent policy on the preservation of such a capability, as an early deliverable of the NCSP.

215. But we must also recognise that, perhaps more than in any other security field, cyber security is carried along by the rapid pace of development in information and communications technology in the round. That these developments are largely driven from outside the UK, are of a scale that can only be marginally influenced by government procurement, and present us with unique challenges.

216. The rest of this section identifies the key industry-related challenges in the cyber domain. It outlines the proposed method of engaging with Government's partners in meeting those challenges.

3.3.2: Key industry-related challenges in the cyber domain

217. We offer below a list of priority areas of activity and focus for science and technology, for comment and validation:

Achieving critical mass: we recognize the scale of global ICT development, and the limited influence that any Government could exert. So partnerships are essential – amongst Government departments and agencies, between the public and private sectors, and internationally. The Office of Cyber Security and Information Assurance (OCSIA) has a key role in ensuring coherence of approach building on existing relationships in other parts of Government.

Maintaining agility: perhaps the over-riding characteristic of cyberspace is the pace of change. Not just technological change, but changes in business processes and social interaction that this supports; changes in impacts that these in turn engender, and vulnerabilities that these expose; and contingent on all of these and on other – non-cyberspace factors – the change in threats. In such an environment we need to ensure that our response is agile and responsive – but this agility and responsiveness needs to

be delivered within a stable policy framework which encourages both the public and private sector as well as academia, to invest in skills and technology developments.

Delivering national capability: while, as described above, substantial improvements in cyber security need to be delivered through mass-market 'Commercial-Off-The-Shelf' products and services, there will remain the need for specialized 'National Capability' products and services. We need to ensure that we can continue to procure these, affordably, and with the level of assurance that such capabilities require. This will need innovative technical and commercial approaches that the public and private sectors will need to cooperate on to deliver.

Engaging the public: individuals must also play their part in securing cyberspace. Government may set the direction, and provide leadership, but the 'big society' applies as much inside cyberspace as outside it. With the private sector we need to raise awareness of cyber security issues amongst the public, and look for ways to enable the public to take more responsibility for their own safety. Community inclusion in cyber security education and practice is critical to a secure Britain. This becomes progressively more important in the context of the 'Race Online' which will increasingly shift the delivery of public sector services to online channels, and in support of the growth delivered by online private sector services.

Enabling economic growth: there is some potential to build on the UK's early lead in cyber security skills and to develop export potential. A larger prize exists in building a UK cyberspace environment that optimises the balance of opportunity and risk to support the growth of the UK economy as a whole. This will depend on public and private sector partnership to provide skills, products and services within a policy and regulatory environment that incentivises good risk management.

3.3.3: The response: defining requirements via new partnerships

218. As indicated above, partnership between the public and private sectors is an essential component of the response to the challenges of cyber security. In the first instance, we intend to pursue this partnership in five key areas:

First, we will improve our joint 'situational awareness' – establishing mechanisms for real-time sharing of information on cyber vulnerabilities in order to improve responsiveness and limit damage;

Second, we will explore ways to work more closely on 'policy co-design' – determining ways to improve the UK's cyber security environment while developing the comparative advantage of the UK cyber security industry;

Third, we will grow our collaborative efforts to develop awareness amongst the public of their cyber security responsibilities – building on initiatives such as GetSafeOnline;

Fourth, we will determine with the private sector what skills are required to support improved cyber security – and work jointly to put the delivery mechanisms in place; and

Finally, we will survey existing activity in cyber security, across the public, private and academic sectors – in order to determine where (if at all) the market is not delivering skills, knowledge and technical capability. We will examine how any gaps in delivery can be filled – particularly for specific 'national capability' with its stringent requirements on assurance.

3.3.4: Priorities

219. As we set out in the SDSR, we intend to sponsor research in collaboration with the private sector and others to fill gaps and to improve our ability to respond to long term challenges. Our initial view is that priorities for science and technology action might include:

220. Establishing an improved economic underpinning for cyber security – to provide an improved impact assessment for the UK economy as a whole, to understand and correct any market failures in delivering cyber security, and to understand how economic aspects might impact on the targeting of cyber attacks and our response to such threats.

221. Developing an improved understanding of complex systems and their behaviour under attack – visualisation methods to detect attacks or aberrant behaviour, investigation of emergent properties, and development of biologically-inspired & dynamic defence and response methods.

222. Combining understanding of human behaviour with technical measures – enhancing users' risk perception and response, and understanding the impact of the evolution of social networks on society.

223. Improving situational awareness – in particular, the real-time detection, monitoring and attribution of cyber attacks, and the dissemination of actionable information to enable the appropriate response.

224. Continuing improvement of information assurance – identification and provision of skills, and innovative means to ensure the delivery of assured capability that meets the UK's sovereign requirements.

General Question:

Q85. Have we adequately identified the key industry-related challenges for cyber security?

Specific questions:

Q86. Is our proposed partnership response the optimum approach, given the nature of the ICT industry and the current fiscal climate?

Q87. Are our proposed science and technology priorities appropriate to address the challenges we have identified?

Part Four: Consultation

4.1: Consultation Details

4.1.1: Topic of this Consultation

225. The Government is proposing that the United Kingdom should have, for the first time, a formal statement covering equipment, support, and technology in both the defence and security sectors. This Green Paper is intended to allow full public consultation on that policy. Once consultation is complete next year, we intend to publish a White Paper setting out our approach for the next five years, i.e. until the next strategic review.

4.1.2: Scope of this Consultation

226. The Green Paper is intended to allow the Government an opportunity to discuss a variety of issues that would be encompassed by a new approach to equipment, support, and technology for UK defence and security. This will assist in creating suitable policies and processes for specific issues which will be then published as a White Paper. All potential policy issues are part of the consultation and we value any constructive views.

4.1.3: Expected interested parties

227. The consultation will focus on academia, industry, service providers, trade bodies, and trade unions involved in the defence, security, and cyber sectors. We would also value comments from commentators interested in aspects of this subject and from the general public, particularly those who are not part of regular Government engagement on these subjects. We expect to have the opportunity to discuss the proposed approach with Parliamentarians during the consultation period.

4.1.4: Geographical scope

228. There is no constrictive geographical location for this consultation and we welcome views from all parties. There will be at least one formal event for industry and the general public to attend to discuss their views on issues raised by the Green Paper. This will be held in London, probably in early February. We will advertise details on the MOD website in advance of the event. Ministers and officials will visit different parts of the UK to engage with industry and the general public during the consultation period.

4.1.5: Consultation criteria

229. This Consultation has been conducted in accordance with the criteria in the Government's Code of Practice on Consultation. If you wish to have access to the full version of the Code, you can obtain it at: http://www.bis.gov.uk/policies/better-regulations/consultation-guidance

230. The Government's Code of Practice on Consultation sets out seven criteria for successful consultation:

- **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 exercise** – consultation exercises should be analysed carefully and clear feedback should be provided to participants following the consultation.

- **The burden of consultation** – keeping the burden of consultation to a minimum is essential if consultation is to be effective and if consultees buy-in to the process is to be obtained.

- **Responsiveness of consultation exercise** – 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.

4.2: Consultation Mechanisms

4.2.1: Duration

231. The consultation period starts 5 January 2011 and ends 31 March 2011 (12 weeks).

4.2.2: How to respond

232. You are able to respond online at www.defenceconsultations.org.uk/

233. A PDF consultation document will also be available to download online at www.defenceconsultations.org.uk/ and hard copy responses should be sent to:

Green Paper Responses
DGDC
5.N.25
MOD Main Building
Whitehall
London
SW1A 2HB

E-mail: DGDCSecIP-Consultation@mod.uk

234. Please contact the MOD (above) if you require information in another format, such as Braille, large font or audio, as well as if you require a hard copy of the PDF consultation document to be sent to you. These means are being used as they are deemed the most practical and efficient means of responding for both the public and the Ministry of Defence.

235. The MOD will focus on comments that have evidence backing up their views. Consideration will be given to publishing the individual responses received from this

consultation exercise. Respondents do not need to respond to all of the questions in the consultation and where they do not have an interest in all the issues considered in this conclusion, should feel free to limit their response to those questions that are of interest to them.

236. When responding, it would help us if you were able to state whether you are responding as an individual or as part of an organisation. If responding on behalf of a larger organisation, it would be helpful if you could make it clear who the organisation represents and, where applicable, how the members' views were assembled.

4.2.3: After the Consultation

237. Responses to the wider elements of the consultation period will be summarised and considered as part of further policy development. The resulting White Paper will be published in 2011.

4.2.4: Confidentiality disclosure

238. You should be aware that information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes, these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004.

239. If you want the information that you provided 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. In view of this it would be helpful if you could explain to us why you view 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 confidentially disclaimer generated by your IT system will not be regarded as binding on the department.

240. The department will process your personal data in accordance with the DPA and in the majority of circumstances; this will mean that your personal data will not be disclosed to third parties.

4.2.5: Enquires

241. If you feel that this consultation does not satisfy these criteria, or if you have any enquires or comments about the process, please contact:

Green Paper Consultation Enquires
DGDC
5.N.25
MOD Main Building
Whitehall
London
SW1A 2HB

or

E-mail: DGDCSecIP-Consultation@mod.uk and start your subject as 'Enquiry'.

4.3: Conclusion

242. This Green Paper has an unusually wide scope and poses many questions, both in terms of general policy and specific issues. This should not discourage your participation in this consultation. We are seeking views from all interested parties, whether these relate to one specific issue or to the broadest sweep of the UK national interest. Above all, we want to understand the different perspectives on equipment, support, and technology for UK defence and security, in order that we can make the best choices about what should be in next year's White Paper and therefore our approach over the next five years.

Acronym List

A|D|S	Aerospace | Security | Defence (a trade body)
ATT	Arms Trade Treaty
C4ISTAR	Command, Control, Communications, & Computers, Information/Intelligence, Surveillance, Targeting Acquisition, and Reconnaissance
CBRN	Chemical, Biological, Radiological, and Nuclear
CCTV	Closed-circuit television
CDE	Centre for Defence Enterprise
CESG	Communications-Electronics Security Group
COTS	Commercial off-the-shelf
CPNI	Centre for the Protection of National Infrastructure
DGDC	Directorate General, Defence Commercial (MOD)
DHS	Department of Homeland Security (USA)
DPA	Data Protection Act 1998
DST	Defence Science and Technology (MOD)
Dstl	Defence Science and Technology Laboratory
FATS	Framework Agreement for Technical Services
FOIA	Freedom of Information Act 2000
FP7	Framework Programme 7 (of the European Commission).
FY	Financial Year
G2G	Government to Government
HOSDB	Home Office Scientific Development Branch
IA	Information Assurance
IAG	Industry Advisory Group
ICT	Information and Communications Technology
IDT	International Defence Training
IED	Improvised Explosive Device
INSTINCT	Innovative Science and Technology in Counter Terrorism
IP	Intellectual Property
IPR	Intellectual Property Rights
IRC	International Research Collaboration
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulations
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NCSP	National Cyber Security Programme
NSS	National Security Strategy
OCCAR	Organisation conjointe de coopération en matière d'armement (Organisation for Joint Armament Cooperation)
OCSIA	Office of Cyber Security and Information Assurance
OSCT	Office for Security and Counter-terrorism
PQQ	Pre-Qualification Questionnaire
R&D	Research and Development
RA	Reverse Auction
RISC	UK Security and Resilience Industry Suppliers Community
SDSR	Strategic Defence and Security Review
SME	Small and Medium-sized Enterprise
START	Studies in Terrorism and Responses to Terrorism
TFEU	Treaty for the Functioning of the European Union
UKTI DSO	UK Trade and Investment Defence and Security Organisation
UOR	Urgent Operational Requirement
VHS	Video Home System

TSO
information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, telephone, fax and email
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/general enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

TSO@Blackwell and other accredited agents

Customers can also order publications from:
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
Telephone orders/general enquiries: 028 9023 8451
Fax orders: 028 9023 5401

ISBN 978-0-10-179892-1

9 780101 798921