Department for Business, Energy & Industrial Strategy

National Security and Investment: Sectors in Scope of the Mandatory Regime

Government Response to the consultation on mandatory notification in specific sectors under the National Security and Investment Bill

March 2021

Any enquiries regarding this publication should be sent to us at:
enquiries@beis.gov.uk

Contents

Executive Summary

Overview

1. The Government consulted on proposed descriptions of activities of qualifying entities within 17 sectors that would be captured under the National Security and Investment (NSI) Bill's mandatory regime from 11 November 2020 to 6 January 2021. The Government has sought to ensure that these descriptions will enable potential acquirers to self-identify for the purposes of mandatory notification regime while ensuring that the Government is informed of proposed acquisitions in these crucial areas and will be able to take action to investigate and, if necessary, address any national security risks. Ministers and officials have engaged with stakeholders through webinars, roundtables, and direct meetings and to take onboard their views on the definitions, and 94 formal responses were received in response to the consultation.

2. The responses from this consultation have been used to refine the definitions to provide further clarity to allow parties to self-assess whether they need to notify the Secretary of State when they are contemplating a relevant acquisition of control. The sector definitions in this document remain in draft so proposals during the remaining passage of the primary legislation can be taken into account. The final definitions will be set out in regulations in due course.

3. This document provides an overview of the responses to the consultation on the sectors in scope of the National Security and Investment Bill's mandatory regime and the Government's response to the Consultation responses follows, including revised sector definitions.

Context

4. The National Security and Investment Bill provides the Government with updated powers to scrutinise and intervene in investment to protect national security, as well as to provide businesses and investors with the certainty and transparency they need to do business in the UK. Once the regime is in place, the Government will have powers to comprehensively scrutinise and, if necessary, intervene in qualifying acquisitions of control over qualifying entities or assets across the economy if they give rise to national security risks.

5. In addition to a non-sector specific voluntary notification option and the power to scrutinise qualifying acquisitions that have not been notified, the Bill makes provision for a mandatory notification and pre-approval requirement for those sectors of the economy where it is considered national security issues are particularly likely to be an issue. The scope of this requirement, referred to as the 'mandatory notification regime', will be set out in secondary legislation before commencement of the NSI powers.

6. The new powers will require the Secretary of State to be notified in advance of certain acquisitions described in the regulations in 17 sectors. This will mean that the Government is informed of proposed acquisitions in these crucial areas and will be able to take action to investigate and, if necessary, address any national security risks. This approach brings us in line with many of our allies including the USA, France and Germany.

7. The sectors are:

- Advanced Materials
- Advanced Robotics
- Artificial Intelligence
- Civil Nuclear
- Communications
- Computing Hardware
- Critical Suppliers to Government
- Critical Suppliers to the Emergency Services
- Cryptographic Authentication
- Data Infrastructure
- Defence
- Energy
- Military and Dual-Use
- Quantum Technologies
- Satellite and Space Technologies
- Synthetic Biology (formerly known as Engineering Biology. This sector has been renamed in response to the consultation responses)
- Transport

Next steps

8. The Government has published revised draft definitions for the sectors within scope of the mandatory regime within this document to provide clarity on the refined definitions.

9. We will engage with stakeholders directly as we continue to develop and refine the definitions.

10. Final definitions will be set out in regulations as Parliamentary time allows, subject to Royal Assent for the Bill.

Background

What was the background to the consultation?

11. The UK economy thrives as a result of Foreign Direct Investment. Since 2010/11, over 600,000 new jobs have been created thanks to over 16,000 Foreign Direct Investment projects. An open approach to investment must include appropriate safeguards to protect our national security. Our current powers in this area largely date from 2002 – technological, economic and geopolitical changes mean that reforms to the Government's powers to scrutinise investment on national security grounds are required. The Government welcomes Foreign Direct Investment and is clear that the UK is open for business.

12. The Government first announced its intention to update the investment screening powers in 2016 and consulted via a Green and White Paper. Further proposals were put forward in the 2018 White Paper. However, the proposals did not go far enough in addressing a small number of acquisitions in particularly sensitive sectors. In particular, they did not go far enough to prevent hostile actors from avoiding scrutiny and acquiring critical businesses under the radar.

13. The Government introduced the National Security and Investment Bill on 11 November 2020. The Bill makes provision for a mandatory notification requirement for key sectors of the economy, accompanied by a voluntary notification option for other sectors in the economy and the power to proactively scrutinise qualifying acquisitions. This regime is in line with many of those administered by our allies.

14. The National Security and Investment regime will introduce mandatory notification for notifiable acquisitions considered most likely to give rise to national security risks. Any acquisition covered by the mandatory notification will require notification and clearance from the Secretary of State prior to taking place.

What did we consult on?

15. The Government's public consultation on the sectors in scope of mandatory notification sought responses on whether the definitions provided sufficiently clear parameters to inform businesses and investors of the need to notify, and whether the definitions were proportionate. The consultation ran for 8 weeks, from 11 November 2020 to 6 January 2021.

16. The consultation set out the 17 sectors which are most likely to give rise to national security risks. Those included: Advanced Materials, Advanced Robotics, Artificial Intelligence, Civil Nuclear, Communications, Computing Hardware, Critical Suppliers to Government, Critical Suppliers to the Emergency Services, Cryptographic Authentication, Data Infrastructure, Defence, Energy, Synthetic Biology (formerly

referred to as Engineering Biology), Military and Dual-Use, Quantum Technologies, Satellite and Space Technologies, and Transport.

17. The consultation invited comments on 22 questions, ranging from technical sector specific questions to wider questions on the scope of the definition, proportionality and testing clarity for businesses and investors. All responses have been carefully considered, and the Government is grateful for the time and expertise of those who responded, particularly those who fed back in substantial detail.

Who did we consult?

18. The consultation was published on gov.uk, the BEIS Citizen Space consultation hub and an email address dedicated to responses to the consultation was created for organisations to share their responses there. We also engaged with our stakeholders to raise awareness of the consultation. This included investors into the UK, individual businesses, trade bodies, legal and advisory firms, academics, research bodies, and regulators.

Who responded?

19. We received feedback through meetings, roundtables, and Citizen Space and formal written responses. The Government received 94 written responses from investors, individuals, regulators, individual businesses, legal and advisory firms, trade associations and industry groups, academics and regulators (the breakdown is shown in the table below). Feedback on the proposed sector definitions was also obtained through stakeholder meetings during the course of the consultation.

	Legal and advisory firms	Investors	Government, academia and research bodies	Advanced Technology	Infrastructure businesses (including trade associations)	Regulators	Individuals
Number of consultation respondents	12	9	18	4	45	1	5

Summary of consultation responses and the Government response

Summary of consultation responses

20. The requirement for mandatory notification for certain acquisitions in these 17 sectors was broadly well received as respondents identified the sensitive nature of the sectors and the potential of national security risks.

21. Responses to this consultation suggested that many of the sector definitions were very broad in scope and would require further specificity to enable acquirers to identify whether they would be in scope of mandatory notification. In particular, sector definitions for Communications, Engineering Biology (now Synthetic Biology) and advanced technology sectors received comments on the wide breadth of the proposed definitions. The potential dual-use capability of advanced technology risked widening the scope of businesses and investors captured.

22. Responses to the consultation also suggested that the inclusion of sub-contractors within some definitions, such as Critical Suppliers to Government, may pose a problem, as some sub-contractors may not be aware of the eventual destination of goods or services provided.

23. In addition to the responses on each sector, 33 responses provided additional comments on the NSI Bill and the proposed regime. These covered the approach to defining national security, thresholds within the mandatory notification regime, and in relation to the extra-territorial aspects of the regime. There was some interest in the possibility of exemptions.

24. Many respondents stated that individual sector definitions did not include the provision that the entity of the specified descriptions must carry on activities in the United Kingdom, as specified in clause 6(4) of the National Security and Investment Bill. This provision will be set out in the final regulations when they are laid later this year for all notifiable acquisitions.

25. The mandatory notification sectors will be kept under review and where there is a need to update the regulations due to emerging technology or newly identified national security risks, it will be possible to do this through secondary legislation in the future.

Government response

26. The Government is a champion for free trade, recognising that inward investment is economically highly beneficial. An open approach to international investment must also include appropriate safeguards to protect our national security and the safety of our citizens. The Government is committed to ensuring that it takes a robust but proportionate approach to investment in the UK.

27. Following the concerns and suggestions shared by businesses and investors during the consultation, the Government has significantly narrowed the definitions of the acquisitions within the 17 sectors proposed as within scope of the mandatory regime and set out in this response. These changes will ensure that the regime is targeted and proportionate.

28. Three examples from within the document are set out here:

    i. Consultation responses for the Artificial Intelligence (AI) definition suggested that the definition was too broad and required further specificity to provide reassurance to businesses and investors. Following engagement with technical and policy experts, we have narrowed the definition significantly to focus on three higher risk applications: the identification of objects, people, and events; advanced robotics and cyber security. In narrowing the definition, the definition now provides further clarity for businesses and investors as to whether notification is required, reducing the burden on the industry and supporting our ambition to grow the UK AI economy.

    ii. Quantum Technologies and Synthetic Biology (previously Engineering Biology), received responses that the definition would cover the majority of transactions relating to the sector, including the academic research community and associated supply chain sectors. The Government has tightened the scope of entities subject to mandatory notification in these definitions.

    iii. The Quantum Technologies definition is now more focussed to capture entities that develop or produce a quantum technology product.

    iv. The Synthetic Biology (previously Engineering Biology) definition has been comprehensively revised to concentrate on synthetic biology and renamed accordingly. The revised definition reflects the technical and scientific advice from stakeholders articulates entities out of scope and is clearer as a result.

29. The technologies recognised in these sector definitions are integral to a well-functioning economy and its future growth. The Government intends to carry out further, targeted engagement with the sectors to further refine the description of acquisitions that must be notified before making regulations, subject to Royal Assent to the Bill.

30. This approach will ensure that the regime is targeted and proportionate and keeps the UK firmly open for business.

We have provided the revised draft definitions for all the sectors under each section. The same five questions were asked of each sector, followed by several sector specific questions. Under each question, we have set out a summary of consultation responses and thereafter provided the Government response.

Advanced Materials

The revised draft definition for 'Advanced materials' is in Annex A of this document.

***Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant* transactions? If not, how can the definitions be improved?**

31. There were mixed views in response to this question between those who say it as providing sufficient clarity, and others who disagreed. Comments were also shared that the definition was overall too narrow and should be expanded.

32. There were recommendations to improve the clarity of the definition including creating a clearer link between paragraphs 1, 2 and 3 of the definition, and several suggestions for further descriptions of what was intended to be captured through each sub-category of materials. On nanomaterials and nanotechnology, one respondent asked why there was both a general 'nano' section and a significant 'nano' content in many other sections, notably graphene and related 2D materials, semiconductors, photonics, metamaterials.

33. Further suggestions were received highlighting materials that were missing from the definition and which were indicated as having security and defence applications.

34. Several queries were also received around how these definitions will be updated in the face of emerging and developing technology.

Government Response

35. The Government welcomes the range of suggestions received on this definition, and all other sectoral definitions. They were hugely valuable and will enable significant improvements to be made to the effective working of the regime.

36. As a result of suggestions on advanced materials, several changes have been made to the definition. Some of the materials sectors (e.g. engineering and technical polymers and ceramics) included several types of material; in some cases, these have now been split into separate categories to make it easier to follow (now called 'engineering and technical polymers' and 'engineering and technical ceramics').

37. Some of the responses relating to materials that were considered to be missing from the definition are, in many cases, contained in the legislation set out in the UK Strategic Export Control List (SECL). The Government intends to capture all materials that are considered likely to give rise to national security concerns and which are contained in the relevant legislation set out in the SECL. The Advanced Materials definition aims to further cover materials that could pose a risk to national security but are not included in the legislation set out in the SECL. The revised definition has been updated to make this clearer for users.

38. The nanotechnology and graphene sections have been further clarified, including cross-reference to internationally accepted definitions of key terms. The Government has retained its approach of having both a nanotechnology section and some content within other materials sections. This approach provides better coverage within recognised materials areas, which have scopes going beyond just nanoscale aspects.

39. The mandatory notification sectors will be kept under review and where there is a need to update the regulations due to emerging technology or newly identified national security risks, it will be possible to do this through secondary legislation in the future.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

40. The Government received a wide range of feedback that was helpful in pointing out where technical and scientific terms were unclear. This included removing technical abbreviations, providing clearer definitions of technical terms and removing ambiguous terms such as ‘state of the art’ and ‘significant’.

41. There was a suggestion to replace the sector name ‘advanced materials’ with ‘strategic materials’, because not all materials covered within the definition are advanced.

Government response

42. Terms which were highlighted as ambiguous have either been clarified or removed, for example, all terms relating to undefined scales (e.g. ‘tiny sensors’) have been removed.

43. A proposal was received to remove the reference to ‘advanced’ materials and refer to all materials of ‘strategic’ or ‘critical’ importance to national security. This was not accepted because the term ‘advanced’ is generally well understood and accepted by most responders. The term ‘strategic materials’ has a very specific meaning in the defence and military sectors, which could cause confusion. We do not intend to capture all materials used in national security applications, only those that could pose a risk to national security.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

44. A few respondents suggested narrowing the scope of the advanced materials definition by specifying the defence or military applications for which the advanced materials are being used.

Government response

45. We have refined and focused the definition to capture the areas of the materials sector that have the greatest potential to cause national security risks.

46. The defence or military applications for which advanced materials have the potential to be used cannot be shared for national security reasons. A company developing civilian applications of a particular material may be unaware of the potential or intended use of their technology for military purposes. Also, materials applications will evolve more rapidly than the definition. Therefore, we will not be specifying the defence or military applications of advanced materials in the definition.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

47. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

48. The Government received a mixture of comments regarding the scope of the definition. Some respondents suggested it was too broad and would capture acquisitions that were unlikely to pose national security risks. Others felt that the definition sufficiently captured the relevant areas of the economy, with one respondent specifically noting that advanced materials is such a broad area that narrowing the scope would be difficult.

49. Several respondents indicated that the list of critical materials referred to in paragraph 3 (j) (ii) and (iii) of the initial definition included materials that were not critical for defence and omitted some that were critical. One respondent suggested that advanced materials for Critical National Infrastructure (CNI) should be included.

50. In addition, we received several specific suggestions of materials and processes that responders considered to be missing from the definition alongside specific language suggestions to effectively narrow the scope of the definition.

Government response

51. The Government have made a significant number of improvements to the definition which we believe have addressed the majority of issues raised. We confirm that the revised scope represents a good balance between safeguarding national security and minimising the burdens placed on businesses and investors.

52. While Critical National Infrastructure is not specifically included in the definition, our analysis is that almost all applications of advanced materials in the Critical National Infrastructure sectors would be covered, either through the advanced materials

definition or other definitions e.g. Defence, Military and Dual-Use, Communications and Energy. The Bill also makes provision for a power for the Secretary of State to call-in acquisitions of control over qualifying entities.

53. We have provided a few examples of the revisions made to the definition:

- The semiconductors definition has been updated to improve its specificity and to remove ambiguity around defining a material which exceeds performance of existing technology.
- The reference to the British Geological Survey (BGS) risk list of critical materials has been replaced with a bespoke list of strategic critical materials for UK defence.
- Several items have been removed to remove duplication with the SECL list.
- The Photonics and Optoelectronics section has been substantially revised to narrow its scope significantly. In particular, the definition of lasers in scope has been narrowed.

Conclusion

54. It is vitally important to the security and prosperity of the UK that technologies that provide strategic defence applications are protected and are not transferred to hostile state actors and competitors. This would risk adverse defence, security and economic impacts on the UK in the future. We must mitigate the risks of foreign ownership and/or control, secure access to defence-critical materials, and safeguard our UK supplier base.

55. Responses received through this consultation have helped us to strike a balance between protecting critical UK technology advantage and allowing companies and their innovations to flourish and deliver non-defence products and services.

56. We have made substantial updates to the definition to help to improve the clarity of technical and scientific terms and remove ambiguous language.

57. We received many responses relating to the scope of the definition, some suggesting items for inclusion and others that the definition was too broad. There were no suggestions for providing a simpler and shorter approach to defining advanced materials. We recognise that the advanced materials definition is substantially longer and more detailed than other definitions relating to sectors; advanced materials is an extremely broad and diverse sector with an enormous range of applications, both for military and civilian use. We have refined the definition in several areas to more clearly and precisely define what is intended to be captured. The length of the definition reflects this endeavour.

Advanced Robotics

Revised Draft Definition:

Advanced robotics

1. A qualifying entity that carries out any of the following activities—

(a) developing advanced robotics;

(b) producing advanced robotics;

(c) developing or producing core components specially designed or modified for the purposes described in paragraphs (a) and (b).

2. Subject to paragraph 7, "advanced robotics" means a machine that meets either or both the descriptions set out in paragraph 3 and is capable of—

(a) carrying out multifunctional physical actions; or

(b) positioning or orientating materials, parts or tools, special devices through variable movements in three-dimensional space;

3. The descriptions referred to in paragraph 2 are—

(a) has the characteristic of autonomy set out in paragraphs 4 and 5; and

(b) is capable of using its sensors to carry out sophisticated surveillance and data collection in respect of any aspects of its environment in order to collect, store or communicate to the operator, significant volumes of high-fidelity data.

4. Advanced robotics have the characteristic of autonomy where it is capable of performing actions:

(a) independent of human control;

(b) independent of human control but complemented by—

(i) manual (including tele-operation) control;

(ii) pre-programmed operations or controls; or

(iii) control derived from other robotics or software control systems.

5. The characteristics of autonomy may include—

(a) using physical, sensory and cognitive capabilities in combination, to decide on and implement a course of action that will vary depending on:

(i) the environment;

(ii) the behaviour, dynamics, properties or arrangement of objects in the environment;

which may include the ability to self-navigate or react to stimuli or changes to improve performance;

(b) adapting and learning by carrying out actions, to improve task performance from iteration and experience, which may include—

(i) the ability to self-heal;

(ii) the capability to identify and repair damaged robots or components; or

(iii) soft robotics capabilities (robots made from compliant materials that mimic capabilities in living organisms that enable them to adapt or respond to their surroundings).

6. In this Part:

"cognitive" means having the abilities of reasoning, perception, communication, learning, planning, problem solving, abstract thinking or decision making;

"core components" mean—

(i) sensors enabling advanced robotics to track and sense its environment;

(ii) end effectors or other devices attached to advanced robotics allowing it to interact with its task or perform its operation;

(iii) locomotion, where the advanced robotics is capable of moving in its environment;

(iv) an energy source, including passive sources such as solar energy, providing power delivery enabling advanced robotics to move independently and to carry out its functions;

(v) computing capability enabling high performance and sophisticated computational capabilities, including the use of artificial intelligence to process data and data sets received from the sensors and adapt the behaviour of the advanced robotics;

(vi) communications capability, including the ability to communicate with a human operator or other advanced robotics.

7. Advanced robotics does not include—

(a) machines containing robotic systems that are readily available for purchase by consumers, including robotic toys, domestic appliances described as "smart", vacuum cleaning robots and consumer-focussed drones, where "consumer" means an individual acting for purposes that are wholly or mainly outside of that individual's trade, business, craft or profession but not including self-driving vehicles;

(b) industrial automation systems that use mechanical tools performing repetitive functions with very basic or no sensors or cognitive ability, including—

(i) simple sensing or imaging devices that do not confer any ability to react or change their behaviour given a change in circumstances, without human intervention;

(ii) devices that carry out functions that require pre-set sequences of actions or require pre-set sensing of the environment;

(c) robotic systems acquired as entire robotics systems to perform given tasks, where the acquirer will not be able to alter the core technical capabilities of the systems or combine them with other systems to perform wholly new advanced robotics systems;

(d) devices that are not independently mobile.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

58. Written responses and stakeholders attending roundtables broadly indicated agreement that all advanced robotics could present national security risks due to their dual-use potential. However, many respondents raised concerns that too broad a definition risked placing a significant burden on the business community as it would capture virtually any organisation developing, producing or using sophisticated machines. Respondents asked for the definition to be narrowed in scope to only companies developing the most advanced robotics, and for clearer guidance on exclusions.

59. Roundtable discussions concluded that advanced robotic capabilities did not solely arise from the use of artificial intelligence, and participants counselled against limiting the scope of the definition to this concept. Participants proposed that the characteristic of 'autonomy' should be at the core of a definition of advanced robotics. There were some requests for a precise level of autonomy or minimum capability, but others felt this would not be self-assessable by businesses, or possible to clearly define in legislation.

60. Roundtable participants also suggested that surveillance capabilities, even when a robot lacked artificial intelligence or similar capabilities, could have significant national security implications. They also suggested that entities within the advanced robotics supply chain should be in scope, where these entities are developing critical components that underpin national security capabilities.

Government Response:

61. The Government welcomes the input from respondents and has worked closely with roundtable participants, in particular to refine a more detailed definition, and to improve the clarity of the specific activities and capabilities that are in scope.

62. We agree with the core concept of autonomy and additional concerns raised and included these in our revised definition. Several exclusions have also been added.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

63. Many respondents sought clarity on the meanings of the terms artificial intelligence (AI) and robotics. One response regarded AI and robotics not as specific sectors or capabilities but as technologies adopted by an increasing number of companies that all might fall within scope.

64. Another respondent suggested applying a minimum threshold or proportion of AI within a company's products or portfolio. Other suggestions included assessing the functionality, data input or nature of AI-driven decisions delivered by a company or its advanced robotics, rather than on the basis that it 'used AI'.

65. Roundtable participants highlighted some of the challenges in defining the concept of autonomy. This included the absence of a widely understood industry standard definition, and the difficulty in differentiating between autonomy found in lower and higher risk applications in a legally unambiguous way. One respondent noted, by way of example, that the technology in self-driving cars and self-driving tanks would need to be regulated in the same way.

66. Many participants also felt that we needed to provide greater clarity on the supply chain components of interest (termed 'core components' in the definition).

67. Further engagement on the revised definition, including through roundtables, was broadly positive and provided further clarity.

Government response

68. We have developed the definition to reframe and clarify that autonomy is one of the core features of advanced robotics of relevance to national security, and we have described this concept in further detail with reference to the ability to sense, make decisions and act depending on their environment. Refined definitions have been added for 'cognitive capabilities' and 'core components' that support this.

69. However, we concluded that it was not possible to include specific or minimum capabilities, benchmarks or thresholds for autonomy, nor include terms like 'sophisticated' or 'significant degree of', as these cannot be objectively or unambiguously applied for self-assessment and notification.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

70. The Government received a mixture of responses to this question. Several respondents stated that the definition was too broad and raised concerns that the definition of core components potentially widened the scope to encompass a wide range of low-risk activities. An example given was advanced robotics in car production, which integrate information from multiple sensors and adapting movements in real-time but have limited national security implications.

71. One respondent suggested clarifying narrower or specific technologies most relevant to national security, or 'exclusion of non-threatening AI and/or technology'. Another suggested restricting specific machines which could be repurposed for hostile purposes. There was a suggestion to define sectors of activity, selected on the basis of the likelihood of their giving rise to national security implications.

72. A number of respondents suggested adopting the French FDI approach, which was regarded as rigorous and effective yet limited to certain activity.

73. Participants in roundtables were clear of the potential dual-use capability of advanced robotics, including in security and combating threats. A wide-ranging definition was considered essential to ensuring relevant capabilities were captured. However, it was raised that direct military capabilities would already be covered by the Military and Dual-Use sector definition. Further engagement on the revised definition yielded supportive responses and welcomed the greater coherence and clarity provided.

Government Response

74. We agree that advanced robotics have dual-use potential. The Government provides funding to and works closely with a wide range of companies developing or producing remote-control and autonomous land, air and surface vessels, underwater vehicles and

space satellites. Commercially available advanced robotics currently operating in extreme environments and components in use within autonomous vehicles could easily be reconfigured and redeployed in activities such as reconnaissance and intelligence gathering, as well as warfare.

75. There is an absence of universally recognised benchmarks to describe sophisticated autonomy or surveillance capability in legally unambiguous terms. We have worked with experts to develop bespoke descriptions of the types of adaptive and responsive behaviours that would characterise a minimum threshold of autonomy that could be sufficiently clearly understood. We also worked with experts to develop a range of exclusions, covering entities involved in areas such as consumer or toy robots, 'smart' household appliances (like robotic vacuum cleaners), and 'basic' (largely pre-programmed) industrial automation robots that are widely adopted in manufacturing processes globally.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

76. There were limited responses on this question. One respondent recommended Government introduce a 'de minimis' threshold for mandatory notification.

77. A further suggestion was to exclude internal/intra-group transactions, as they create a disproportionate impact on business and could disrupt UK companies' ability to adapt dynamically and may therefore hinder UK innovation and commercialisation.

Government response

78. Having carefully considered these suggestions, Government will not be taking them forward. The company size or turnover was not judged to be relevant an entity's ability to develop or produce advanced robotics (or critical underpinning components) with national security implications.

79. Roundtables validated a range of exclusions to help narrow the intended scope and provide greater clarity to companies.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

80. Respondents and roundtables affirmed the 'dual-use' potential of advanced robotics and the challenge of defining them clearly and correctly, without being too broad in scope. Some requested setting a baseline of the capability or tasks that advanced robotics could perform. Others suggested the definition be focused to protect where the UK has a unique capability. One respondent noted the challenge of differentiating

between toy or domestic robotics and more sophisticated or potentially threatening uses in a legally unambiguous way, given the technology can have multiple applications.

81. Further engagement on the definition highlighted the danger of having too broad a definition and requested further specificity to be provided on 'core components' to remove 'uncertainty and potential over-inclusiveness to a wide range of other companies and lower risk activities'. One response suggested narrowing to products 'specially designed or modified' for advanced robotics.

82. Additional respondents requested exclusions in terms of technology capabilities and types and scope of uses and activities. There were also requests that these should be periodically revised and updated as technology advanced. One respondent asked whether the exclusion covered self-driving cars, given that many functionalities are or will soon be commoditised and readily available to consumers, yet 'readily available for purchase by consumers' was one of the exclusions that we introduced in later revisions developed with sector experts.

Government response

83. The Government agrees that advanced robotics have 'dual-use' potential. Roundtable participants were clear that the core advanced robotic capabilities that enable applications to give rise to national security risks or threats is the characteristic of autonomy or sophisticated surveillance capabilities (or both).

84. We agree that national security risks could also arise from entities developing components (sensors, end-effectors, actuators, power sources, etc). However, to avoid capturing large segments of the UK's manufacturing supply chain, we have adopted the suggestion of narrowing the scope to components specially designed or modified for advanced robotics.

85. We agree with roundtable participants' comments that entities developing or producing advanced robotics should be in scope and entities that employ off-the-shelf advanced robotics in their operations should not be in scope. Similarly, robotics lacking autonomy, such as remote-control toys, power tools or 'simple' industrial robots should be excluded, as should readily- commodities such as consumer drones.

Question 6: Do you agree that the ability to use artificial intelligence for complex tasks (as defined) is the principal driver of national security capabilities (and threats) in advanced robotics? If not, what other capabilities would you propose be brought into scope and why?

86. The majority of written responses to the definition centring on artificial intelligence expressed concerns, including that wide potential interpretations that made it too broad in scope and likely to result in significant numbers of notifications where there were no national security implications.

87. Significant changes were made following roundtables and the majority of subsequent written responses on the revised definition agreed that it accurately reflected the principal drivers of national security capability and threat.

88. Further engagement on subsequent revisions to the definition suggesting the Government should review the core components list and ensure all components are necessary from a national security perspective. It was also identified the definition of surveillance capabilities as drafted would capture a wide range of non-robotic devices that should be out of scope (such as surveillance cameras).

Government response

89. In relation to the core components, the revised definition sought to ensure that only those specifically within the supply chain of advanced robotics would be captured. In roundtable discussions, experts were clear that advanced robotics are typically systems (or systems of systems), but that both the underlying capabilities as well as the complete system potentially raise security concerns. Beyond the requirement that they be specially designed or modified for advanced robotics, no clearly defined threshold or applications could be determined for inclusion in or exclusion from the definition. The intention was not to capture non-robotic surveillance devices, and we have accordingly amended the revised definition to make this clear.

Question 7. Are there opportunities to refine this definition to avoid capturing low risk advanced robotics, such as those that are less sophisticated or found in domestic applications?

90. There was broad support from most respondents for clear exclusions of applications or use cases considered of limited or no relevance to national security, such as robotic vacuum cleaners and consumer drones. Several respondents requested an exhaustive list of excluded activities or ‘safe harbours’, which should be reviewed periodically as technology advanced. It was suggested exclusions could be based on the sectors the advanced robotics operated in, their baseline capabilities, applications or functions or where advanced robotics was deemed at the core of a business’s activity. Other respondents requested defined inclusions, for example image recognition capabilities.

91. There were suggestions to narrow the definition by focussing on the decision-making process within the advanced robotic or excluding advanced robots where the acquirer could not ‘reverse engineer’ or reassign the task a system was designed for. Roundtable participants were clear that advanced robots with sufficient autonomy and sophistication were intrinsically vulnerable to reverse engineering or reassignment, and this is at the core of their being an advanced robotic system.

92. There was a concern that a system that is not mobile (such as a smart speaker) could still be connected to a system of systems and capable of intelligently issuing commands to systems which can move.

Government response

93. We have sought to improve the clarity with which the key capabilities are described, taking on board respondents' suggestions in consultation with sector experts, wherever appropriate. Several exclusions have also been made, namely robots that are readily and widely available on consumer markets, whether toys, domestic devices or drones, or as robotic components within widely available products or services, such as parking assistance in cars.

94. We have also excluded the mechanical, deterministic robots used in manufacturing production lines (whether large or small), where these carry out pre-set, repetitive functions and lack any sophisticated capability to sense, decide on a new course of action and implement this.

95. The Government has excluded 'end users' e.g. the acquirers of complete, finished robotic systems that were being used for their intended function and where the acquirer would not be able to alter them or combine them with others to make wholly new systems. We also excluded smart speakers or other devices that are not independently mobile.

Conclusion

96. Consultation involved written responses to an initial draft definition, followed by a series of roundtable discussions and further engagement with stakeholders on the revised definition who responded substantively to the public consultation.

97. Roundtable participants were clear that the principal driver of national security relevance was the capability of a robot to sense its environment and the autonomy to respond to it. Robots equipped with sensors capable of sophisticated surveillance and data collection (even without autonomous capabilities) was the other key capability that was recognised as highly relevant to national security.

98. Recognising that autonomy is a broad concept, we sought to clarify the types of capabilities and the level of sophistication that was of interest and by way of further mitigation, developed a list of exclusions covering areas such as consumer or toy robots, 'smart' household.

99. Overall, respondents raised concern about breadth, the substantive changes that we made with sector experts were welcomed by the majority of experts as significant improvements, with a number noting that it accurately captured the main factors that would underpin relevance to national security.

100. The sector definition will be kept under review and can be updated in the future as needed, for example as the technology evolves.

Artificial Intelligence

Revised Draft Definition:

Artificial intelligence

1. A qualifying entity carrying on activities for the purposes set out in paragraph (2), which include—

(a) research into artificial intelligence; or

(b) developing or producing goods, software or technology that use artificial intelligence.

2. The purposes are—

(a) the identification or tracking of objects, people or events;

(b) advanced robotics;

(c) cyber security.

3. In this Part—

(a) "artificial intelligence" means technology enabling the programming or training of a device or software to—

(i) perceive environments through the use of data;

(ii) interpret data using automated processing designed to approximate cognitive abilities;

(iii) make recommendations, predictions or decisions;

with a view to achieving a specific objective;

(b) "advanced robotics" has the same meaning as in [Part X];

(c) "cognitive abilities" means reasoning, perception, communication, learning, planning, problem solving, abstract thinking or decision making;

(d) "cyber security" means the activities to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(e) "cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(f) "network and information systems" has the same meaning as in regulation 1 of the Network Information Systems Regulations 2018; and

(g) "technology" has the same meaning as in Schedule 2 of the Export Control Order 2008 Order.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

101. Several respondents suggested removing artificial intelligence (AI) as a mandatory sector as AI is an underlying technology rather than a specific sector. Many respondents stated that any security risks arising from AI should be covered by the other mandatory sectors.

102. Most respondents stated that the AI sector definition lacked clarity and was too broad in scope. Respondents suggested that the definition provided in the consultation would require acquirers to notify transactions in areas of the AI sector where there were

potentially no or limited risks to national security. Some respondents provided suggested areas for which the definition could be limited to.

Government response

103. The Government accepts that the development and application of these technologies is an industry in its own right, with AI also transforming business models across sectors.

104. We acknowledge that the definition captures entities that identify as AI companies as well as companies in other industries which develop their own AI applications. However, as AI technologies are inherently dual-use, it is the Government's view that all companies that develop AI technologies should be captured, no matter how they self-classify.

105. It is the Government's view that AI should remain as a sector in scope of the mandatory regime; risks arising from AI technologies will not be covered by the other mandatory sectors in this regime. The opportunity to use AI technologies positively across the UK economy can only be harnessed if sensitive applications of AI are protected from the risk of hostile actors intending to do harm to the UK.

106. Following the consultation, we have narrowed the definition to focus on three applications which the Government has identified to be of higher risk. This includes identification of objects, people and events, advanced robotics and cyber security. Whilst these three applications have been specified, there is also overlap with other sector definitions including the defence sector.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

107. Many respondents stated that the phrase 'complex tasks' was vague and excessively broad and that the risk lies not in the complexity of the task but the sensitivity of the outcome. Some respondents accepted the definition's approach to include 'complex tasks' or proposed updates for clarity.

Government response

108. Following the consultation responses, the definition was redrafted to align with internationally recognised definitions. This maintained 'cognitive tasks' which was broadly accepted by the consultation respondents but removed 'complex' tasks.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

109. Several respondents suggested removing AI as a mandatory sector as AI is an underlying technology rather than a specific sector. Many respondents stated that any security risks arising from AI should be covered by the other mandatory sectors.

Government response

110. The Government's response is provided in response to Question 1.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

111. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

112. The responses to this question and the Government's response has been covered under questions 1, 2 and 3.

Question 8. We have used a two-stage approach to define AI, referring to both cognitive functions and complex tasks. Does this approach work? Is this definition accurate in encompassing the breadth of AI technologies and summarising the complex tasks AI can be used to perform?

113. The majority of respondents commented that the AI sector definition lacked clarity and was too broad in scope. It was expected that the current definition would lead businesses to raise notifications when there was no/minimal risk to national security. 'Cognitive functions' was broadly accepted though additions were suggested around specific wording.

114. Many respondents noted that 'complex tasks' was vague and excessively broad and that the risk lies not in the complexity of the task but the sensitivity of the outcome. Some respondents agreed with the definition's approach to include 'complex tasks' or proposed updates for clarity.

115. A number of respondents proposed aiding clarity by aligning the current NSI definition for AI with AI definitions produced by the OECD or EU.

Government response

116. We have narrowed the definition to focus on three higher risk applications. This includes: the identification of objects; people and events; and advanced robotics and cyber security. These applications were identified following thorough engagement with technical and policy experts. By narrowing the definition, it is hoped that the definition is now clearer for companies as to whether mandatory notification is necessary, reducing the burden on the industry and supporting our ambition to grow the UK AI economy.

117. Outside of these three applications, the Bill makes provision for a power for the Secretary of State to call in acquisitions of control over qualifying entities (including UK companies and non-UK companies operating in the UK) or assets ('trigger events') across the economy for a national security assessment, whether or not they have been notified to the Government.

118. Following the consultation responses, the definition was redrafted to align with existing OECD and EU definitions. This maintained 'cognitive tasks', which was broadly accepted by the consultation respondents, but removed 'complex' tasks. By updating to align with OECD and EU definitions the two-stage approach has been removed.

Question 9. This definition is intended to include companies that develop AI technologies but do not purchase AI products. Is that accurately reflected?

119. Respondents were divided on whether it was sufficiently clear that the consultation definition excluded those who purchase AI technology. Some respondents proposed including a general statement of intent that the definition does not include purchase of products or licenses where no novel application occurs.

120. A small number of respondents emphasised that it was not clear what was meant by 'develop' AI technology.

Government response

121. The Government's view is the updated definition sets out clearly that those who purchase products or licenses in relation to AI (for use but not for further development) are not covered by this definition.

Conclusion

122. Following consultation, the definition has been amended to both improve clarity and to narrow it to specify higher risk applications. The definition has been aligned more closely with existing international definitions; updating the original structure of the definition. This maintained the reference to 'cognitive abilities' but removed the reference to 'complex tasks'.

123. The sector definition will be kept under review and can be updated in the future as needed, for example as the technology evolves.

Civil Nuclear

Revised Draft Definition:

1. A qualifying entity that —

(a) subject to paragraph 2, holds, or has submitted an application which has not yet been determined for, a nuclear site licence granted in accordance with section 3 of the Nuclear Installations Act 1965;

(b) subject to paragraph 2, is a tenant on a site in respect of which a nuclear site licence has been granted in accordance with section 3 of the Nuclear Installations Act 1965;

(c) holds Category I/II and/or Category III nuclear material as defined in section 77(7) of the Anti-Terrorism, Crime and Security Act 2001 and regulation 3(3) and (4) of the Nuclear Industries Security Regulations 2003;

(d) is a class A or B carrier of nuclear material as approved under regulation 14 of the Nuclear Industries Security Regulations 2003;

(e) is in receipt of, or has submitted an application which has not yet been determined for, an order granting development consent to the Secretary of State in accordance with the Planning Act 2008 in relation to a nuclear reactor (as defined in section 26 of the Nuclear Installations Act 1965)

(f) is, or has been, required to pay a fee to the Office for Nuclear Regulation under regulation 16(1) of the Health and Safety and Nuclear (Fees) Regulations 2016, and the outcome of the assessment for which that fee is to be, or has been, paid has not yet been determined;

(g) holds equipment and/or software as defined in regulation 2(3), or holds information defined in regulation 2(4), of the Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004;

(h) is a holder of sensitive nuclear information as defined in section 77(7) of the Anti-Terrorism, Crime and Security Act 2001;

(i) is a named recipient of financial support under section 5 of the Science and Technology Act 1965, or under section 93 of the Higher Education and Research Act 2017, for or in relation to nuclear reactors (as defined in section 26 of the Nuclear Installations Act 1965).

2. [An entity which falls under paragraph 1(a) or (b) will not constitute a qualifying entity where the site to which the nuclear site licence relates is controlled or operated wholly or mainly for defence purposes as defined in section 70(3) of the Energy Act 2013].

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

125. Several responses and roundtable discussions welcomed terms used in this definition which were already defined through existing regulations, and which provided clarity as to whether an entity is in the scope of the definition.

126. A few respondents sought clarification on the precise conditions that would capture a tenant of a civil nuclear site within the scope of this definition, and which entities would be captured under the ‘developers’ provision. It was also recommended the definition of a ‘developer’ of a new nuclear site be clarified.

127. Respondents welcomed clarifications that the legislation applies at the point of investment, i.e. 'active' applications for site licences, and current holders of relevant material.

Government response

128. The wording in subsection (b) has been amended to clarify that this would apply to all tenants of civil nuclear sites, regardless of the type or level of activity undertaken on the site. We have also amended the wording in (e) to specify that the legislation applies to the entity that submits an application for a relevant Development Consent Order, and only after point of application.

129. The Government confirms that the legislation applies at the point of investment and includes only 'active' licence applications. This is in line with our stated policy intent, and we have subsequently amended paragraph (a) to reflect this.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

130. Respondents noted that that the section of the definition regarding categorisation of nuclear material incorrectly referred to a section of legislation that has been repealed.

131. Some respondents expressed that the scope should be wider in relation to entities holding or developing sensitive materials and should clarify whether plutonium is in scope. There was also a suggestion to exclude companies from the definition which handle small amounts of radioactive material for non-nuclear purposes.

132. There was an additional suggestion to amend the wording of the definition to specify applicability to entities holding information or technology related to Uranium Enrichment Technology defined in the Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004.

Government response

133. In subsection (c) we have rectified the legislative reference; this now refers correctly to nuclear material as defined in section 77 (7) of the Anti-Terrorism, Crime and Security Act 2001.

134. After careful consideration, we can confirm that part (c) of the definition will not be changed with respect to the types of material holdings that are included (Category I/II and/or Category III nuclear material only), and that holders of non-nuclear radioactive material are not included.

135. The current drafting is in line with the Nuclear Industries Security Regulations (which are informed by the international classification of materials set by the International Atomic Energy Agency), and this manages potential risk at a level in line with our stated policy intent.

136. We have revised the wording in part (g) to make clear that this applies to entities who hold relevant technology or information defined in the Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

137. No substantive responses were received in relation to this question.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

138. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

139. There were various points raised in response this question. Several responses expressed the view that capturing all entities which have paid a particular fee to the Office for Nuclear Regulation including requesting parties to the Generic Design Assessment (GDA) is too wide and should not include previous applicants who are no longer pursuing nuclear opportunities.

140. There was also a question of whether the inclusion of all entities holding sensitive nuclear information is too wide, and as these entities are regulated for security already, they should not be included.

141. Meanwhile responses on the scope of R&D inclusion in the sector ranged from suggestion that the scope of R&D inclusion in the sector definition should be broader to cover a wider range of activities not limited to reactor development; to advice that it would be more proportionate to only capture direct recipients of relevant funding.

Government response

142. We have revised the wording in (f) to specify that this applies to entities paying the specified fee in relation to an on-going assessment where the outcome has yet to be determined. It is our view that this is proportionate because completion of the GDA does not convey to the requesting party any right to develop a nuclear project. If an entity holds classified nuclear information or has applied for consent to develop a new nuclear site, then this would continue to fall within scope of the sector definition.

143. Equally we have retained section (h), as there is a potential security risk from a hostile change of ownership and control of an entity holding classified Sensitive Nuclear Information. It is Government's view that inclusion in the NSI regime is complementary

to, and not a duplication of, regulation under the Nuclear Industries Security Regulations.

144. We have amended the wording in (i) to specify that this legislation would apply to direct (named) recipients of funding. Where necessary, contractual arrangements may cascade similar responsibilities to subcontractors, but we agree that it is not a proportionate measure to capture all indirect recipients as this could capture smaller pieces of work that have no civil nuclear security implications. We have expanded the scope slightly to also capture the Government's funding under UKRI programmes as this will include relevant programmes, but we have not widened the scope to capture a greater range of R&D activities, as we believe new reactor development presents the greatest potential risk from relevant changes of ownership or control. Other parts of the definition would capture relevant enrichment activities.

Conclusion

145. The consultation responses provided valuable feedback which we have taken into account fully when developing the definition. The changes that have been made are largely for clarificatory purposes, to better reflect the policy intent and to ensure entities are able to readily self-assess whether they fall under the definition.

146. The policy intent of the definition has not changed significantly through the consultation, and we believe that this definition is proportionate to the underlying sensitivities and risks relating to the civil nuclear sector.

Communications

Revised draft definition

Communications

Public communications

1.— (1) A qualifying entity which meets the condition in sub-paragraph (2) and carries on activities in the United Kingdom which consist in or include—

(i) providing a public electronic communications network; or

(ii) providing a public electronic communications service.

(2) The condition in this sub-paragraph is that the turnover of the entity's relevant business for the relevant period is £50,000,000 or more.

(3) For the purposes of this paragraph—

(i) turnover shall be calculated in conformity with accounting practices and principles which are generally accepted in the United Kingdom;

(ii) turnover shall be limited to the amounts derived by that entity from the relevant business after deduction of sales rebates, value added tax and other taxes directly related to turnover; and

(iii) when an entity's relevant business consists of two or more undertakings that each prepare accounts then the turnover shall be calculated by adding together the turnover of each, save that no account shall be taken of any turnover resulting from the supply of goods or the provision of services between them.

(4) In this paragraph—

"relevant business" means so much of any business carried on by the entity as consists in any one or more of the following—

(i) the provision of a public electronic communications network;

(ii) the provision of a public electronic communications service;

"relevant period" means—

(i) the period of one year ending with the 31st March next before the time when notification is given under section 14 of the Act;

(ii) in the case of an entity which at that time has been carrying on that business for a period of less than a year, the period, ending with that time, during which it has been carrying it on; and

(iii) in the case of an entity which at that time has ceased to carry on that business, the period of one year ending with the time when it ceased to carry it on.

Infrastructure critical to public communications

2.—(1) A qualifying entity carrying on activities in the United Kingdom which consist in or include making available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service falling within paragraph 1, except in so far as they are physical infrastructure of a kind specified in sub-paragraph (2).

(2) Physical infrastructure that hosts cables (including strands of optical fibre) is specified for the purposes of sub-paragraph (1).

(3) A qualifying entity carrying on activities, for a purpose mentioned in sub-paragraph (4), which consist in or include—

(i) providing an electronic communications network by means of a submarine cable system;

(ii) providing an electronic communications service by means of a submarine cable system; or

(iii) making available a cable landing station used in connection with such a network or service.

(4) The purpose referred to in sub-paragraph (3) is the provision of connectivity to a public electronic communications network or a public electronic communications service falling within paragraph 1.

(5) A qualifying entity supplying services to persons in the United Kingdom which consist in or include providing a top-level domain name registry servicing 14 billion or more queries from any devices located in the United Kingdom in any consecutive 168-hour period for domains registered within the Internet Corporation for Assigned Names and Numbers.

(6) A qualifying entity supplying services to persons in the United Kingdom which consist in or include—

(i) providing a domain name system resolver service which services 500,000 or more different Internet Protocol addresses used by persons in the United Kingdom in any consecutive 168-hour period; or

(ii) providing a domain name system authoritative hosting service servicing 100,000 or more domains registered to persons with an address in the United Kingdom.

(7) A qualifying entity supplying services to persons in the United Kingdom which consist in or include providing an internet exchange point and which has 30% or more market share for such services in the United Kingdom in terms of interconnected autonomous systems.

(8) In this paragraph—

"domain name system" has the meaning given in paragraph 10(5)(a) of Schedule 2 to the Network and Information Systems Regulations 2018;

"internet exchange point" has the meaning given in paragraph 10(5)(c) of Schedule 2 to the Network and Information Systems Regulations 2018;

"top-level domain name registry" has the meaning given in paragraph 10(5)(d) of Schedule 2 to the Network and Information Systems Regulations 2018.

Supply chain for public communications

3. —(1) An entity carrying on activities in the United Kingdom which consist in or include—

(i) developing or producing; or

(ii) supplying, providing or making available

goods or services used to directly make possible or directly support a purpose mentioned in sub-paragraphs (2) or (3).

(2) The purposes mentioned in this sub-paragraph are—

(i) the provision of a public electronic communications network falling within paragraph 1; or

(ii) the provision of a public electronic communications service falling within paragraph 1.

(3) The purposes mentioned in this sub-paragraph are—

(i) the provision of an electronic communications network by means of a submarine cable system, for the purpose of providing connectivity to a public electronic communications network or a public electronic communications service falling within paragraph 1;

(ii) the provision of an electronic communications service by means of a submarine cable system, for the purpose of providing connectivity to a public electronic communications network or a public electronic communications service falling within paragraph 1; or

(iii) the making available of a cable landing station used in connection with such a network or service.

Interpretation

4. —(1) In this Part—

"associated facility" has the meaning given in section 32(3) of the Communications Act 2003;

"cable landing station" means a network facility which enables the interconnection of one or more public electronic communications networks with an electronic communications network provided by means of a submarine cable system;

"electronic communications network" has the meaning given in section 32(1) of the Communications Act 2003;

"electronic communications service" has the meaning given in section 32(2) of the Communications Act 2003;

"physical infrastructure" has the meaning given in regulation 2 of the Communications (Access to Infrastructure) Regulations 2016;

"public electronic communications network" has the meaning given in section 151(1) of the Communications Act 2003;

"public electronic communications service" has the meaning given in section 151(1) of the Communications Act 2003.

5. In this Part, references to the provision of an electronic communications network include references to its establishment, maintenance or operation.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

147. Most respondents welcomed the use of the existing concepts of electronic communications networks and electronic communications services as used in the Communications Act 2003. It was recognised that the industry was already familiar with these definitions and would understand whether transactions would be caught.

148. Several respondents believed that the definition provided clarity as to whether or not a business was in scope of the definition; however, there were concerns regarding how broad the definition was.

149. Others disagreed and said that it was so broad that it was unclear as to the extent to which some companies, such as those within the supply chain, were caught. For instance, one respondent suggested that the definition include additional, explicit categories for subsea fibre optic cables, the associated supply chain and digital infrastructure companies within the definition.

Government response

150. The Government has maintained the use of concepts from the Communications Act 2003 as the basis of the sector definition following the general consensus that it provides clarity to enable investors and businesses to understand whether they will need to notify.

151. We have narrowed the definition to address respondents' concerns that it was too broad and to focus on public communications networks, services and associated facilities. The Government has also set out specific categories of businesses that are caught by the definition to provide further clarity. These are: providers of submarine cable systems, cable landing stations, and the operators of essential services in the digital infrastructure subsector as set out in the Network and Information Systems Regulations 2018 (as amended) (NIS Regulations) as follows: Top Level Domain Name Registries, Domain Name System Resolver and Authoritative Hosting services, and Internet Exchange Points.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

152. Most respondents were satisfied that the terms used were correct and clear. A few respondents were concerned that it was not clear how the categories of 'associated telecoms supply chain' and 'digital infrastructure companies' referenced in the accompanying rationale would apply. They noted it was unclear whether the list of digital infrastructure companies in the consultation document was exhaustive and unclear regarding the point in time at which a company supplying services or goods would be regarded as belonging to the associated supply chain.

153. Despite the clear and correct use of terminology, it was recognised it could still be difficult in places to determine whether an electronic communications network or service was being provided or an associated facility was being made available. This was demonstrated in an example of a landowner of an agricultural field with cell towers positioned on the fields being inadvertently caught by the definition of an 'associated facility.'

154. Many respondents suggested the definitions should use the concept of an operator of an essential service as defined in the NIS Regulations.

Government response

155. The Government has amended the definition to provide further clarity on telecoms supply chain and what parts are captured. The Government is also actively considering further narrowing the supply chain definition, potentially listing the specific components of the supply chain that should be caught. The definition has also been amended to set out each of the types of digital infrastructure companies that are caught by the definition which, as noted above, uses concepts from the NIS Regulations to ensure there is no ambiguity as to what is caught.

156. The Government agrees with the concerns that the Communications Act definition of 'associated facility' used in the definition could leave some businesses unsure as to whether they were captured in scope. The definition has been amended so that relevant associated facilities are caught only if they are associated facilities by reference to a public electronic communications network or service. In addition, the public electronic communications network or service in question must meet a threshold that has been

introduced. Currently, this relates to the turnover of the network or service provider but the Government is still considering whether to use a user-based or turnover-based threshold. This excludes other associated facilities that fall within the Communications Act 2003's definition where the facility is not used in relation to a significant public network or service.

157. In light of this amendment, those landowners whose land hosts associated facilities (such as masts) or electronic communications networks are not intended to fall within the definition merely because they own the land. However, if landowners also make available associated facilities (such as masts or buildings which house electronic communications apparatus) then the Government considers that they would fall within the definition. We are still, however, considering the application of the definition to landowners and may make further amendments to ensure that the former category of landowners is exempt.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

158. Most respondents used this section to reiterate their concerns that the definition was too broad. They commented that given that the definition encompassed virtually all acquisitions within the sector, it would also inevitably capture the foreign investment that had the potential to cause national security risks.

159. There was also a concern that the definition did not include housing and support infrastructure such as data centres, which were critical to security as they allowed access to the network nodes.

160. One of the responses recommended that the definition should also include the provision of maintenance, repair and upgrade services of companies within the associated supply chain.

Government response

161. We have sought to address the concerns with the breadth of the definition.

162. The Government recognises the importance of data centres to the secure running of the public telecommunications network, and are satisfied that the revised definition does include those who own buildings that host data centres that are part of the core public telecommunications infrastructure (e.g. those which host internet exchange points and the 5G core networks). This is on the basis that buildings which are specifically intended to host active infrastructure would be classified as 'associated facilities'. In addition, the Data Infrastructure sector definition also covers entities that house and support data infrastructure. The Government is still in the process of considering the extent to which the two definitions interplay with one another.

163. We are satisfied that those who provide maintenance, repair and upgrade services to public electronic communications networks are caught by the revised definition. We do

not consider that there is a need to include providers of passive infrastructure such as ducts and poles, and accordingly there is no need to include those who provide maintenance and repair services of such passive infrastructure.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

164. A number of respondents stated that the sector already faced stringent security obligations under a number of different pieces of legislation, most notably the forthcoming Telecommunications (Security) Bill (TS Bill), and therefore questioned whether it was necessary to apply the National Security and Investment Bill to the communications sector. One respondent suggested that the TS Bill covered the same screening objectives as the NSI Bill, giving the government powers to make national security judgements and decisions in relation to potential high-risk vendors, and issuing corresponding orders to communications providers.

165. Several respondents highlighted that the Government still had the call-in power to scrutinise transactions, and therefore the scope of the definition for mandatory notification should be narrowed.

Government response

166. The Government acknowledges that there are many regulatory obligations on the telecommunications industry via a number of different pieces of legislation. Nevertheless, the NSI Bill fills a regulatory gap by providing the Government with new powers to protect the UK's digital infrastructure and supply chain from hostile actors using ownership of, or influence over, businesses and assets to harm the country.

167. The Telecommunications (Security) Bill is intended to create powers to restrict (or impose other requirements on) the use of goods, services or facilities supplied by a high-risk vendor, but it does not extend to investments in the communications providers themselves or investments in other infrastructure used to provide communications. It also cannot prevent the acquisitions of vendors by hostile actors, and accordingly cannot prevent the entirety of a particular segment of the supply chain being acquired by hostile actors, thereby leaving the UK with no secure suppliers.

168. We are therefore satisfied that the NSI Bill fills a regulatory gap and represents an important new strand of the Government's toolkit to address national security threats in the sector. When taken together, the two Bills provide complementary regimes that protect telecommunications critical national infrastructure from national security threats.

169. However, given that the Government will also have the call-in power within the NSI Bill, and in light of the consultation responses from industry on this point, we have significantly narrowed the scope of the mandatory notification regime as outlined below.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

170. Nearly all respondents were concerned that the definition was too broad, with concerns raised that the definition would capture virtually every transaction that occurred in the sector, of which many would pose no national security threat. One respondent suggested that the definition should not be narrowed to avoid opening the way for subjectivity and regulatory uncertainty.

171. Respondents were concerned that the inclusion of 'associated facility' captured almost any supporting activity such as landowners providing the land or building on which any network apparatus is located (e.g. a telecoms mast or power supply) and plastic pipes for lining underground ducts. One respondent suggested that the definition should be limited solely to those associated facilities that are used, or reasonably likely to be used, in association with the use of electronic communication networks or services, rather than those which could have the potential to be used for an electronic communications network or service.

172. Two respondents suggested using the definition of 'electronic communications apparatus' from the Electronic Communications Code in Schedule 3A of the Communications Act 2003.

173. There were suggestions to remove passive infrastructure from the definition, thus removing infrastructure such as antennae, ducts and conduits. The inclusion of material thresholds was also suggested with various figures recommended by respondents.

174. Many respondents suggested that the definition be amended to focus on public electronic communications networks and services, thereby excluding private networks. Alternatively, respondents suggested it could focus on certain private networks that were used in core national infrastructure.

175. There was support for the exclusion of broadcasting content services from the mandatory notification regime. These should continue to be captured by the media public interest regime.

Government response

176. The Government has taken a number of steps to address the concerns raised by respondents that the definition was too broad. We have now added thresholds to the definition to exempt acquisitions of smaller companies to minimise the burden on the industry. The threshold specifically relates to the turnover of the network or service provider, although the Government is also considering an end user threshold.

177. Elsewhere, the Government is considering applying the turnover threshold to qualifying entities in the supply chain such as vendors and service providers. So if a

vendor supplied goods which made possible the provision of any public electronic communications service and the entity providing the public electronic communications service had a turnover higher than £50m, then the vendor would be captured by the definition. We have applied the same thresholds that are found in the Network and Information Systems Regulations 2018 to the operators of essential services in the digital infrastructure sector.

178. We have drawn a distinction between what we consider to be 'active' infrastructure and 'passive' infrastructure, drawing on concepts from the , whereby passive infrastructure such as ducts and poles, and the manufacturers and suppliers of such passive infrastructure, are exempt from the definition. We are still in the process of determining precisely what infrastructure should be classed as passive and active.

179. The definition has been amended so that relevant associated facilities are caught only if they are associated facilities by reference to a public electronic communications network or service that meet the threshold. We are satisfied that this revised definition of associated facilities addresses concerns with the wide scope and unlike the definition of 'electronic communications apparatus' will not catch 'passive' infrastructure as above.

180. Landowners whose land hosts associated facilities (such as masts) or electronic communications networks are not intended to fall within the definition merely because they own the land. The Government is considering further changes to the definition to ensure such landowners are exempt from the definition. However, if landowners also make available associated facilities (such as masts or buildings which house electronic communications apparatus) then the Government considers that they would fall within the definition.

181. The Government is also actively considering further narrowing the supply chain definition, potentially listing the specific components of the supply chain that should be caught.

Question 10. Is the definition sufficient to capture all our interests to enable us to respond to potential and exceptional national security concerns in particular equipment and services suppliers and digital infrastructure?

182. Respondents generally agreed that the definition was sufficient to capture all relevant interests. As previously noted, respondents were concerned that the definition was so broad as to capture nearly all acquisitions within the sector.

Government response

183. The Government has sought to address concerns that the definition is too broad by narrowing it in a number of ways such as, adding thresholds to the definition to exempt acquisitions of smaller companies to minimise the burden on the industry. The Government believes that the revised definition strikes the balance between capturing all of our national security concerns, while minimising the burden on industry.

Question 11. Is the definition clear that the Communications sector definition includes entities that provide public and private electronics communications networks, and their associated facilities?

184. All respondents who answered this question agreed that the definition was clear that the definition included entities that provided public and private electronic communications networks, and their associated facilities.

Government response

185. The Government welcomes the fact that it was clear to respondents that the definition included private networks in addition to public networks and their associated facilities. For the purposes of narrowing the scope of the definition, the definition has now been amended to specifically reference 'public' electronic communication networks and services, with private networks now excluded.

12. How can the definition be narrowed to exclude private communications networks that do not pose a risk to national security?

186. Many respondents suggested introducing materiality thresholds to exclude small private networks. In particular, it was suggested that the definition should be narrowed to exclude private communication networks that do not supply networks or services to the UK defence sector or to operators of an essential service as defined in the Network and Information System Regulations 2018 because other private networks do not pose a risk to national security. Other respondents recommended that the definition was limited to those which are provided to UK defence or critical national infrastructure sectors. A de-minimis threshold of 500,000 end users was suggested, whereby private networks which serve less end users were exempt.

187. Other suggestions included narrowing the definition to exclude private networks by specifying the definition with reference to public electronic communications networks and public electronic communications services. However, it was recognised that it can sometimes be difficult to ascertain whether various types of infrastructure are wholly or mainly for the purpose of making electronic communication services available to members of the public. Therefore, it was suggested that the government considered limiting the definition to networks and services that are designated by Ofcom under section 33 of the Communications Act 2003.

Government response

188. The Government recognises that the original definition was too broad and was likely to capture many private networks that posed no national security risk, such as private networks used by taxi firms.

189. We have therefore removed private networks from the Communications definition. Certain other private networks such as those used by the emergency services are captured within other sector definitions of this Bill. We are still in the process of

considering whether further critical sector private networks should be added to other respective sector definitions.

190. This narrows the definition in line with the views of most respondents, and in many instances, exceeds expectations.

191. We consider that capturing relevant private networks and services in each sector definition is a more appropriate way of targeting them than requiring certain providers to notify Ofcom under section 33 of the Communications Act 2003.

Conclusion

192. Following consultation, we have narrowed the definition to exclude as far as possible the components of the national telecoms infrastructure that do not pose a national security risk to reduce the burden on businesses and investors.

193. The definition is now divided into three sections (public communications, infrastructure critical to public communications, and the associated supply chain) and sets out certain specific activities that are included, such as the provision of submarine cable systems and cable landing stations, to provide greater certainty. The Government acknowledges that different elements of the definition may overlap to some extent or a particular entity may fall under several different elements, but this approach has been adopted to provide certainty.

194. As consultation responses supported the government approach to the treatment of media enterprises, the definition continues to cover providers of broadcast transmission infrastructure which are providers of public electronic communication networks or services and meet the newly specified turnover threshold.

195. Furthermore, broadcasting content services (television and radio) remain excluded from the definition of an electronic communication network or service and therefore do not fall within this sector definition. Other news media (e.g. newspapers) are not electronic communication networks or services and also do not fall within this sector definition.

196. Enterprises who provide both broadcasting infrastructure and content services will be covered by this sector definition in relation to their broadcast infrastructure.

Computing Hardware

Revised Draft Definition

Computing hardware

1. A qualifying entity whose activities consist of or include the activities set out in paragraph (2).

2. The activities referred to in paragraph (1) are —

(a) the ownership, creation or supply of intellectual property relating to-

(i) computer processing units;

(ii) architectural, logical and physical designs for such units;

(iii) the instruction set architecture for such units;

(iv) code, written in a low level language, that can control how such units operate;

(v) integrated circuits with the principal purpose of providing memory;

(b) the design, maintenance, or delivery of a service for the secure provisioning or management of—

(i) roots of trust of computer processing units;

(ii) code, written in a low level language, that can control how such units operate;

(c) the fabrication or packaging of—

(i) computer processing units;

(ii) integrated circuits with the principal purpose of providing memory.

3. In this part —

“computer processing unit" means-

(a) a central processing unit (CPU);

(b) a field programmable gate array (FPGA);

(c) a microcontroller;

(d) a system on chip;

(e) a graphics processor unit;

(f) a specialist processor for artificial intelligence applications;

“fabrication” means the process of producing a microelectronic circuit on a semiconductor substrate or using other advanced materials, for example, from raw silicon to circuits on silicon;

“packaging” means the process of turning a microelectronic circuit on an appropriate substrate into a package suitable for use in an electronic circuit, for example, from a circuit on silicon to a microchip to be installed on a circuit board.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

197. Respondents noted some terms used in the definition could benefit from further information on what they cover, for example ‘functional capability’ and ‘provides support’.

198. It was also noted the definition's rationale made reference to 'ownership', but this was not captured in the definition. It was therefore possible to interpret that an entity that acquired, but did not create, intellectual property was not covered by the definition.

199. Furthermore, the respondents sought clarity on whether the definition covers entities which create or supply intellectual property relating to: the end-product hardware itself; central processing unit (CPU) wafers; or architectural designs for CPUs.

Government response

200. The definition has been updated to remove terms that were unclear, including the terms 'functional capability' and 'provides support'. References to ownership have also now been included to ensure it is captured within the definition.

201. The focus of the Computing Hardware definition remains preventing the loss of intellectual property within the supply chain to hostile actors. The definition has therefore not been updated to make reference to the end-product hardware itself or CPU wafers. We have now included reference to 'architectural, logical and physical designs' into the definition as clarification. We will continue to review technical references to ensure that they are well-understood across the sector.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

202. Respondents noted that the term 'computer processing unit' was less well recognised than the more commonplace 'central processing unit'. There was therefore a risk that the terms could be confused by businesses.

Government response

203. We recognise the potential for confusion between 'computer processing unit' and 'central processing unit'. A list of six sub-terms has been included within the definition to determine what 'computing processing unit' includes. 'Central processing unit' is listed as one of the six sub-terms.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

204. Respondents noted that the definition covers computing hardware products that are used in consumer products or are part of the wider supply chain for consumer products. It was therefore suggested that the definition may capture a number of products that would be deemed low risk. Some respondents also suggested that fabrication and packaging would not give rise to national security concerns.

205. Respondents recognised that there may be security risks regarding business activities relating to 'roots of trust'.

Government response

206. While we recognise comments raised by industry, there remains the possibility of unforeseen, ‘dual-use’ applications of computing hardware products. This remains, even within the supply chain of products for consumer use. An exclusion on consumer products has therefore not been applied. We will continue to speak with industry as the definition iterates and welcome any further discussions going forward.

207. While the majority of the definition looks at intellectual property, we recognise too that the UK’s strengths are in novel, advanced computing hardware manufacturing techniques. An acquisition of these manufacturing techniques, knowledge or expertise, relating to computing hardware, could be used to undermine our national security. References to fabrication and packaging have therefore not been removed.

208. Advances in technology related to computing hardware occur throughout the supply chain and if a hostile actor obtains access or control, they could use a part of the supply chain to identify vulnerabilities in them or cause harm.

209. We can confirm there were no changes regarding ‘roots of trust’ within the definition.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

210. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

211. Respondents noted that the definition would cover computing hardware products that are used in consumer products or are part of the wider supply chain for consumer products. It was therefore suggested that computing hardware products that are ultimately for consumer use be excluded.

Government response

212. While we recognise the comments raised by industry, there remains the possibility of unforeseen, ‘dual-use’ applications of computing hardware products. This remains, even within the supply chain of products for consumer use. An exclusion on consumer products has therefore not been applied. We will continue to speak with industry as the definition is iterated and welcome any further discussions going forward.

Question 13: The definition covers computer processing units: we interpret this to cover central processing units, field programmable gate array devices, a microcontroller for general purpose application and a System on Chip. Is this clear?

213. Respondents noted that the term ‘computer processing unit’ was less well recognised than the more commonplace ‘central processing unit’. There was therefore a risk that the terms could be confused by acquirers.

214. It was queried whether the definition covers entities which create or supply intellectual property relating to the end-product hardware itself; central processing unit (CPU) wafers; or architectural designs for CPUs.

Government response

215. We recognise the potential for confusion between ‘computer processing unit’ and ‘central processing unit’. A list of six sub-terms has been provided within the definition to specify what ‘computing processing unit’ includes. ‘Central processing unit’ is listed as one of the six sub-terms.

216. The focus of the Computing Hardware definition remains preventing the loss of intellectual property within the supply chain to hostile actors. The definition has therefore not been updated to make reference to the end-product hardware itself or CPU wafers.

217. We have now included reference to 'architectural, logical and physical designs' into the definition as clarification. We will continue to review technical references to ensure that they are well-understood across the sector.

Question 14. We consider that integrated circuits with the principal purpose of providing memory should be covered here. Is it clear what products this would cover?

218. Respondents generally noted that it was unclear whether integrated circuits with the principal purpose of providing memory were covered by the definition, although some respondents interpreted this as being captured implicitly. Some respondents did note it would be beneficial for the term to be captured within the definition.

Government response

219. The reference to ‘integrated circuits with the principal purpose of providing memory’ has now been specifically referenced within the definition.

<u>Conclusion</u>

220. Technological advances have changed the way in which people interact and businesses develop and grow. New products and services offer the potential to transform the way we live. Much of this depends on continuing advances in computing power and in connectivity, in and out of the home.

221. These changes have also brought challenges that will impact products across the computing hardware sector.

222. Responses from the consultation helped to signal where more clarity would be beneficial. The definition now provides additional detail on what is covered by the term ‘computer processing unit’. It also adds additional terms into the full definition, including ‘integrated circuits providing memory’ and ‘architectural, logical and physical designs'.

223. Exclusions have not been provided for certain types of products - such as consumer products - or their supply chains. The definition looks to prevent hostile actors from obtaining access or control to computing hardware products, to cause harm or to identify vulnerabilities in them. There exists the possibility of unforeseen, ‘dual-use’ applications of computing hardware products, even within the supply chain of products for consumer use. This in turn could still give hostile actors knowledge or expertise that could be used to undermine our national security.

224. We will continue to review technical references to ensure that they are well-understood across the sector.

Critical Suppliers to Government

Revised Draft Definition

Critical suppliers to government

1. A qualifying entity holding a public contract with government where the performance of the contract involves one or more of the activities set out in paragraph (2).

2. The activities are—

(a) the processing or storage of material to which a security classification of SECRET or TOP SECRET has been applied in accordance with guidance published by the Cabinet Office: Government Security Classification 2018 (1) ;

(b) a requirement for List X accreditation to fulfil the contract (2) ;

(c) a requirement for employees of the qualifying entity to be vetted at or above 'Security Check' level (3) ;

(d) the provision of services to facilitate the security of network and information systems;

(e) the guarding of premises to ensure against unauthorised access or occupation, against outbreaks of disorder or against damage.

3. In this Part—

"government" has the same meaning as "contracting authority" in the Public Contracts Regulations 2015;

"public contract" means a contract for pecuniary interest between one or more persons or other bodies that offer the execution of works, supply of goods or provision of services and government, where the contract has as its primary object the execution of works, the supply of products or the provision of services;

"network and information systems" has the meaning as set out in regulation 1 of the Network and Information Systems Regulations 2018.

(1) https://www.gov.uk/government/publications/government-security-classifications

(2) https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors

(3)https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

225. Many respondents stated that the definition was too broad and would capture too many fail-safe transactions.

226. A concern raised by respondents was that subcontractors may not know they are part of a government supply chain and should be excluded from the scope.

Government response

227. The Government has narrowed the critical suppliers to government definition and has made it clearer for investors to understand whether they fall under the mandatory notification regime. Having carefully considered the points raised around sub-contractors, we have removed subcontractors from scope to ensure that the definition is proportionate.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

228. No substantive responses were received in relation to this question.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

229. No sector specific elements outlined in responses we reviewed.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

230. Several respondents suggested that stringent change of control clauses in contracts would provide the greatest clarity to suppliers. There were other suggestions of controlling the supply chain through the tender process.

Government response

231. We agree that the tender process could be utilised to control the supply chain. Change of control provisions on contracts can also give suppliers greater clarity and are used in certain instances. Nonetheless, we wish to retain the definition whilst narrowing down the scope to balance the needs of national security with those of proportionality for investors.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

232. This has been covered in the sector specific questions below.

Question 15. Is the definition provided sufficient to capture suppliers of critical goods and services, both nationally and locally procured, that are necessary to the delivery of core Government functions?

233. Most respondents noted the definition was too broad and that many sub-contractors may not be aware of they are captured within a government supply chain. The threshold of 5000 PII was regarded to be too low a threshold, especially when we have UK GDPR legislation. Suggestions included raising the PII threshold to 1 million or aligning with

the US FIRRMA regulations and raising the threshold to 200k or 0.3% of the UK population.

234. Further clarity was also sought on how energy and fuel suppliers constitute critical suppliers to government.

235. There were concerns that including government property in the definition would bring landlords into scope. There was a suggestion of publishing a list of critical suppliers that would be subject to mandatory notification.

Government response

236. The Government agrees with many of the proposals and we have taken steps to modify the definition in a manner which balances national security with proportionality.

237. We removed reference to the 'functioning of the state' in an effort to clarify the intent as being specifically for national security grounds.

238. We have removed a number of limbs from the definition where they were already adequately covered by other sectoral definitions, or where voluntary notification, marketing monitoring or other remedies are judged to be sufficient for the level of national security risks expected to arise. In particular, we have removed reference to government property, fuel and energy supplies, and personal identifiable information. In order to align with other sectoral definitions, we have also removed subcontractors from scope.

239. We have not applied material thresholds to the definition as security risk does not necessarily align with contract value. We cannot publish a list of critical suppliers as that would itself represent a risk to national security and would change on a frequent basis.

240. Our revised definition is largely focussed on the protection of classified material, estates, and the people who work with such materials as their compromise represents the greatest risk to national security. It also brings us into closer alignment with the screening regimes of our closest allies.

Question 16. Are there alternative ways to ensure notification of relevant transactions, for example through contracts?

241. Respondents suggested alternative methods may be to control the supply chain through the supplier qualification bid process, use control provisions in contracts and controlling the supply chain through tenders and contracts.

Government response

242. We agree that the tender process could be utilised to control the supply chain. Change of control provisions in contracts can also give suppliers greater clarity - and are used in certain instances. Nonetheless, we wish to retain the definition whilst

narrowing down the scope to balance the needs of national security with those of proportionality for investors.

Conclusion

243. We have revised our definition in light of the consultation responses. Our aim remains to protect national security without creating an unnecessary burden on business.

244. Our definition now focuses on contracts which relate to the handling of classified information or estates and their protection. We also want to ensure that contracts relating to the security of government networks and information systems, and the provision of manned guarding services, remain in scope. Our aim is to protect our most sensitive assets as unauthorised access to sensitive or classified information could undermine critical security work.

Critical Suppliers to the Emergency Services

Revised Draft Definition:

Critical suppliers to the emergency services

1. A qualifying entity that is contracted by an emergency service, to provide to one or more emergency service goods or services that are critical to the operational delivery of that emergency service.

2. In this Part—

(a) "critical" means those goods and services that are essential to continued operational activities, have no alternatives and/ or the compromise or interruption of which would prevent or significantly restrict the ability of one or more emergency service to continue performing their roles, thereby impacting on national security.

(b) "operational" means being directly related to duties, responsibilities and activities undertaken by one or more emergency service including—

emergency response and recovery;

national safety and security;

preserving law and order;

prosecuting criminals;

securing critical national infrastructure; and

protecting the public.

(c) "emergency service" means—

(i) a fire and rescue authority;

(ii) a police body;

(iii) British Transport Police;

(iv) Ministry of Defence Police;

(v) Civil Nuclear Constabulary;

(vi) Ambulance Services;

(vii) Border Force;

(d) "a fire and rescue authority" in England is—

(i) constituted by a scheme under section 2 of the Fire and Rescue Services Act 2004 (a combined fire and rescue authority);

(ii) constituted by a scheme to which section 4 of the Fire and Rescue Services Act 2004 applies (a combined fire and rescue authority constituted under the Fire Services Act 1947);

(iii) created by an order under section 4A of the Fire and Rescue Services Act 2004 (a police and crime commissioner as fire and rescue authority);

(iv) a metropolitan county fire and rescue authority;

(v) the London Fire Commissioner;

(vi) a combined authority established under section 103 of the Local Democracy, Economic Development and Construction Act 2009 [];

(e) "a fire and rescue authority" in Wales is—

(i) a county council is the fire and rescue authority for the county;

(ii) a county borough council is the fire and rescue authority for the county borough;

(f) "a fire and rescue authority" in Northern Ireland is the Northern Ireland Fire and Rescue Service Board defined in article 3 of the Fire and Rescue Services (Northern Ireland) Order 2006;

(g) "a fire and rescue authority" in Scotland is the Scottish Fire and Rescue Service as defined in section 1A and Schedule 1A of the Fire (Scotland) Act 2005 as amended;

(h) "police body" means—

(i) a local policing body as defined in section 101 of the Police Act 1996;

(ii) a chief officer of police as defined in section 101 of the Police Act 1996;

(i) "British Transport Police" means the police force established by Part 3 of the Railways and Transport Safety Act 2003;

(j) "Ministry of Defence Police" means the police force established under the Ministry of Defence Police Act 1987;

(k) "Civil Nuclear Constabulary" means the constabulary established under section 52 (1) of the Energy Act 2004.

Goods and services critical to operational delivery

3. Goods and services that are critical to the operational delivery of one or more emergency service are—

(i) non-PPE equipment used operationally, including but not limited to: uniforms, body worn video, lethal and non-lethal weapons, ammunition, drones, covert policing operations equipment, radios, handheld devices and associated software, control room and telephony hardware, and tasers;

(ii) vehicles, vehicle software and vehicle hardware;

(iii) forensic services, including forensic consumables, chemicals and digital forensics;

(iv) IT and communications infrastructure, to cover software, systems and infrastructure such as radio towers, that are used operationally in respect of emergency service; and

(v) contractual services (those that are outsourced or provided by the private sector) that directly impact upon, or are essential to maintain, operational effectiveness and capability of emergency services, as defined in this section.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

245. Respondents stated the definition was largely clear but captured a broad range of suppliers. It was suggested that the scope for non-PPE hardware was very wide and would include both relatively straightforward pieces of hardware, such as stretchers, through to very sophisticated monitoring devices dependent on both power and software.

246. There was request for guidance as to what constitutes 'hardware used operationally' or 'vehicle hardware', as these were not entirely clear. The respondents suggested that these should be limited to hardware that is specialised to specific emergency services and not include, for example, items such as standard vehicles and vehicle parts that are

commonly used outside the emergency services sector. Further clarifications were also requested for terms such a 'IT and communications infrastructure'.

247. There were suggestions to narrow the definition by using material thresholds and the use of proactive notices to relevant contractors identifying the goods or services being provided as critical to the delivery of a relevant emergency service. Respondents stated that the strict control change of control provisions in service contracts would grant the Government the right to approve the identity of any party seeking to acquire a relevant level of control over the contractor should also be considered in this context.

248. One respondent suggested that HM Coastguard should be included as a separate emergency service.

249. One respondent suggested there was quite an overlap between the sector definitions in relation to where services would fall.

Government response

250. The Government seeks to capture the goods and services that are critical to the operational delivery of the emergency services that would pose risks to national security. We recognise that further refinement of the definition is required and will continue to engage closely with our operational partners and stakeholders, with a view to producing a definition with a narrower scope.

251. We have sought to provide further clarity by providing definitions for terms such as ‘operational’, ‘critical’ and IT infrastructure. We have also incorporated suggestions on specific items that should be included to help refine and clarify each category of goods.

252. We have also removed the inclusion of PPE in this definition, subject to further engagement with key operational partners. This brings the definition in line with current government policy following the amendment to Section 58 of the Enterprise Act 2002 to add a new public interest of ‘public health emergency’ to the existing public interests of national security, media plurality and financial stability so that action could be taken if necessary, in relation to PPE supply concerns.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

253. Most respondents commented that the technical and scientific terms within the definition were sufficiently clear and easy to understand. However, there were some clarifications were sought regarding what constitutes ‘hardware used operationally’, ‘vehicle hardware’ and 'IT and communications infrastructure' as these were not entirely clear.

Government response

254. We have sought to provide further clarity by providing definitions for terms such as ‘operational’, ‘critical’ and IT infrastructure. We have also incorporated suggestions on

specific items that should be included to help refine and clarify each category of goods. We will continue to clarify the terms used within the definition as we further develop the definition.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

255. One respondent suggested the availability of PPE and non-PPE hardware is a supply chain and resilience issue rather than one of national security.

256. The limbs in paragraph 3 were seen to be quite broad as they could potentially capture suppliers of non-specialist vehicles and parts thereof, as well as other non-specialist materials. For example, 'IT and Communications Infrastructure' could conceivably include standard computer equipment that is not specialised, in addition to bespoke or specialist equipment. Respondents suggest that while the emergency services sector as a whole is clearly of importance to national security, it is not clear that a disruption to a single supplier of standard computer equipment has significant potential to cause a national security risk. Respondents stated that the limbs should be clarified to apply to those areas that are truly critical to the emergency services, rather than non-specialist equipment.

257. Additionally, the breadth of the definition could at present capture a business that provides only a small quantity of goods to the emergency services.

Government response

258. The Government seeks to capture the goods and services that are critical to the operational delivery of the emergency services, where the disruption or acquisition of such goods and services poses a risk to national security. We understand the concerns by raised respondents in relation to categories of goods that could include standard equipment that are not relevant to the operational delivery of emergency services and and as a result work on this definition is ongoing with the aim of refining the definition.

259. We will continue to engage closely with our operational partners and stakeholders to refine terms used and further develop the definition to ensure the scope is clear and proportionate. 'IT and Communications Infrastructure' will be refined further in order to provide further clarity to potential acquirers in alignment with the communications sector definition.

260. We have also removed the inclusion of PPE in this definition, subject to further engagement with key operational partners. This will bring the definition in line with current government policy, as referenced in response to Question 1.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

261. There were suggestions to use change of control and assignment clauses to deal with national security issues similar to the approach currently being used by the Government defence procurement contracts, which are perceived to be effective. It was also suggested proactive engagement and monitoring of suppliers should be considered for those companies perceived to be critical and at a risk of takeover. In certain circumstances, Government could choose to adopt a controlling or influencing stake in these organisations.

262. Further clarification was sought by respondents whether the definition intended to address key healthcare supplies.

Government response

263. The Government recognises the value of change of control and assignment clauses but considers it essential that the critical suppliers to the emergency sector is included within the National Security and Investment Bill as one of the most sensitive sectors for which the mandatory notification requirement should apply.

264. It is the Government's intention to capture specific activities in relation to critical suppliers to the emergency services, which does include the ambulance services, but does not cover wider healthcare supplies.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

265. Respondents suggested it was difficult for investors to determine whether the supplier is 'critical' or not. They stated the lack of a materiality threshold is challenging given that products caught in paragraph 3 likely include those that are easily replaceable or not inherently critical. The acquisition of an entity that supplies a de minimis amount of facemasks ('PPE') or car tyres ('vehicle hardware'), for example, could not give rise to any plausible national security concern.

266. Respondents provided suggestions to include materiality thresholds within the definition to narrow the scope. There was a suggestion to amend the definition to ensure that there is a clear materiality threshold in each sub-paragraph. This could be carried out for contracts dependent on the value of the contract.

267. Respondents also suggested this concern could also be addressed in future by the relevant emergency service issuing a notice to certain contractors that the service they provide amounts to critical supply to the relevant emergency service.

268. For businesses that operate both as suppliers to the emergency services sector and to other sectors, the breadth of the definitions relating to non-PPE hardware, vehicle hardware, and IT infrastructure mean that businesses supplying non-sensitive equipment would be required to make mandatory filings if they make even de minimis supplies to the emergency services. The definitions could be narrowed without significant impact on national security by: (i) limiting the relevant sectors to items that are specialised to the emergency services sector (and not of general use); and/or (ii) introducing a de minimis threshold so that businesses that make only incidental supplies to the emergency services are not caught.

Government response

269. We have sought to provide further clarity by providing definitions for terms such as 'operational', 'critical' and IT infrastructure. We have also incorporated suggestions on specific items that should be included to help refine and clarify each category of goods.

270. The Government seeks to capture the goods and services that are critical to the operational delivery of the emergency services where the disruption or acquisition of such goods and services poses a risk to national security. We understand the concerns by raised respondents in relation to categories of goods that could include standard equipment that are not relevant to the operational delivery of emergency services. We have considered the suggestions by respondents and will continue to engage closely with our operational partners and stakeholders to further develop the definition to ensure the scope is proportionate. This includes exploring the suggestion of including materiality thresholds.

Question 17. Is the broad definition provided sufficient to capture all the goods and services, both nationally and locally procured, that are necessary to the delivery of the core emergency service functions?

271. Respondents recognised the definition captured all the goods and services necessary but stated that it was too broad in scope. It was noted a PPE shortage was a bigger challenge in these sectors in 2020, but some respondents suggested that this should be considered a national resilience issue.

272. One respondent suggested that the sector definition could also be broadened to include the Air Ambulance Charity sector.

273. One respondent provided a list of additional goods and services which are necessary to the delivery of the core functions of the Ambulance Service and should be captured in the definition.

Government response

274. It is not the Government's intention to broaden the scope of the Critical Suppliers to the Emergency Services definition to include the Air Ambulance Charity.

275. The Government welcomes the suggestions for additional goods and services that are necessary to the core functions of the Ambulance Service and will take these responses into consideration in refining the definition further.

Question 18. Are there aspects of the broader supply chain to direct suppliers that should also be captured within this regime?

276. Most respondents stated the approach of direct suppliers being captured was proportionate. There was a suggestion for the Government to issue a notice to its contractors (which could be provided in turn to subcontractors) that a certain service provided amounts to a critical service. Furthermore, monitoring the key suppliers to the emergency services could be better managed by putting in place stringent change of control provisions in the service contracts that grant the Government the right to approve the identity of the buyer.

Government response

277. The Government recognises the value of change of control and assignment clauses but considers it essential that the critical suppliers to the emergency sector is included within the National Security and Investment Bill as one of the most sensitive sectors for which the mandatory notification requirement should apply.

Conclusion

278. The Government seeks to capture the goods and services that are critical to the operational delivery of the emergency services where the disruption or acquisition of such goods and services poses a risk to national security. We recognise that further refinement of the definition is required and will continue to engage closely with our operational partners and stakeholders, with a view to producing a definition with a narrower scope.

Cryptographic Authentication

Revised draft definition:

Cryptographic authentication

1. A qualifying entity carrying out activities consisting of or including research into, developing or producing, any product which—

(a) has authentication as a primary function;

(b) employs cryptography in performing that function; and

(c) is not ordinarily supplied to or made available for acquisition by consumers.

2. In this Part—

"consumer" means an individual acting for purposes that are wholly or mainly outside that individual's trade, business, craft or profession;

"authentication" means verifying—

(i) the identity of a user, process or device; or

(ii) the origin or content of a message or other information.

"cryptography" means the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorised use and is limited to the transformation of information using one or more secret parameters or associated key management.

"secret parameter" means a variable, constant or key kept from the knowledge of others or shared only within a group.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

279. The main concern raised was that the definition was too broad. Two responses suggested Cryptographic Authentication should be removed from the mandatory notification regime as it is a widely available and used technology and that its inclusion could inhibit investment in this sector.

280. One of these responses stated 'the current sector would appear to cover a wide range of companies which use cryptographic authentication technology for their consumer and commercial devices, software and services. This scope hinders the ability of investors and businesses to determine whether a transaction is intended to be (or is inadvertently) caught by the sector definition.'

281. Another suggestion was to explicitly define the key harms the sector definition is seeking to prevent. A further response stated that the definition was sufficiently clear and suggested the inclusion of an entity who applies the technology could be applicable.

Government response

282. We have sought to narrow the scope of the definition on the grounds of proportionality in response to the consultation, to reduce impact to the most critical National Security-relevant entities. We accept the consulted definition was too wide and covered a range of companies which use cryptographic authentication technology for their consumer and commercial devices, software and services, which should not be in scope. The revised definition will ensure that only products posing a national security risk are captured.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

283. We received one response to this question stating, 'the terms are succinct and concise to determine relevant activities.'

Government response

284. As we only received one response regarding this specific question, we have not changed the technical or scientific terms. However, we have provided explanations of technical words to ensure a common understanding of the meaning of the words: 'cryptographic', and 'authentication'.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

285. We received two responses to this question. One suggested the sector should not be included in the mandatory regime as it is not sensitive. The more sensitive cryptographic authentication technologies for military and government applications will already be covered by other sector definitions. The second response noted that overall the definition does capture the key areas of the economy where foreign investment may cause national security risks.

Government response

286. We have sought to narrow the scope of the definition on the grounds of proportionality in response to the consultation, to reduce impact to the most critical National Security-relevant entities. We accept the consulted definition was too wide and covered a range of companies which use cryptographic authentication technology for their consumer and commercial devices, software and services, who should not be in scope. The Government recognises, the consulted definition would have included a range of products that do not necessarily give rise to national security risks. The revised definition will ensure that only products posing a national security risk are captured.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

287. There were no sector specific responses in response to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

288. There were suggestions to narrow the scope of the definition by excluding areas which are particularly low risk. Possible suggestions to narrow the scope were to:

- Clarify that the development and production of consumer products that employ cryptographic authentication should not be caught.
- Internal (e.g. in-company) use of cryptographic authentication technology does not have the potential to give rise to any national security threat (other than in the case of companies that are already covered by other mandatory notification sectors). Only companies that develop or produce cryptographic authentication technologies and supply this to third parties (in the UK) should be covered.
- Cryptographic authentication techniques can be excluded where national security interests are already well-protected by functioning of the information security industry.

289. On the other hand, another respondent believed the definition struck the right balance and did not need to be narrowed.

Government response

290. We have sought to narrow the scope of the definition on the grounds of proportionality in response to the consultation, to reduce impact to the most critical national security-relevant entities. We accept the consulted definition was too wide and covered a range of companies which use cryptographic authentication technology for their consumer and commercial devices, software and services, who should not be in scope. The revised definition will ensure that only products posing a national security risk are captured.

<u>Conclusion</u>

291. Cryptographic technology enables information to be protected whilst in storage or in transit by making it inaccessible or unreadable by everyone except those who have the information needed to access or read it. The technology is integral to a well-functioning economy. The Government recognises the importance of these technologies to the UK and promotes research and innovation in cyber security through research grants and supporting the development of new cyber innovation centres.

292. Categorisation of cryptographic authentication technologies falls within the broader industry of information security. Cryptographic authentication can take a variety of forms and is in use in a wide variety of economic sectors as a means of access control, identity, management, network and endpoint security.

293. With this definition, we aim to only capture entities that research, develop or produce products whose primary function is authentication using cryptographic means, where

these products are to be used in systems critical for national security (i.e. the company provides the technology to UK third parties, such as government, CNI or strategic industries); and where products and systems that are generally available to the public, and intended for use by the consumer, are not within scope.

Data Infrastructure

Revised Draft Definition:

Data Infrastructure

1. A qualifying entity whose activities consist in or include any of the activities set out in paragraph (2)

2. The activities referred to in paragraph (1) are—

(a) owning or operating relevant data infrastructure;

(b) managing relevant data infrastructure on behalf of other entities;

(c) managing facilities where relevant data infrastructure is located;

(d) providing specialist or technical services to entities in (a), (b) or (c) which gives the entity providing those specialist or technical services physical access to relevant data infrastructure;

(e) providing services where the provision of such services gives the entity providing those services administrative access to relevant data infrastructure;

(f) producing or developing software designed for use in the services in (e) which configures or manages the provision of administrative access.

3. In this part—

"relevant data infrastructure" is physical or virtualised infrastructure, which:

a) stores, processes or transmits relevant data in respect of which the qualifying entity has a direct contractual relationship with a critical sector entity;

b) is used by public communications providers (as defined in section 151 of the Communications Act 2003) for peering, interconnection or exchange of digital data; or

c) connects any international cabling routes;

"relevant data" are data in digital form which are used for the operation of one or more critical sector entities;

"critical sector entity" means

(a) A public sector authority, where "public sector authority" has the same meaning as "contracting authority" in the Public Contracts Regulations 2015;

(b) A qualifying entity described in the Civil Nuclear definition [x];

(c) A qualifying entity described in the Communication definition [x];

(d) A qualifying entity described in the Critical Suppliers to Government definition [x];

(e) A qualifying entity described in the Critical Suppliers to the Emergency Services definition [x];

(f) A qualifying entity described in the Defence definition [x];

(g) A qualifying entity described in the Energy definition [x];

(h) A qualifying entity described in the Transport definition [x];

"international cabling routes" means an electronic communications network provided by means of a submarine cable system which interconnects with a public electronic communications network in the UK;

"specialist or technical services" means:

a) equipment installation services, installing the relevant data infrastructure; or

b) equipment repair and maintenance services in respect of the relevant data infrastructure;

"administrative access" refers to authorisation or access granted via logical and/or administrative access controls by virtue of which an entity may access relevant data infrastructure or control access to relevant data infrastructure where such access would otherwise be restricted or compartmented without such administrative access and where such access would permit the modification of the relevant data infrastructure in a way that was not authorised.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

294. Many respondents opined that the definition was too broad in scope. They also raised the potential for confusion for businesses due to cross-over between the Data Infrastructure definition and other sectors and warned that some businesses might not read every sector definition if they expect to fall under a specific definition.

Government response

295. The Government has refined the scope of the Data Infrastructure definition in response to concerns about its breadth. We have also endeavoured to improve consistency and reduce overlap between Data Infrastructure and other sector definitions.

296. Regarding the potential cross-over between definitions, we have advised stakeholders that there will be no consequential difference for reporting if an entity is captured by more than one definition. The stakeholder engagement that we have conducted and ongoing relationship with the sector will form a basis for the implementation phase of the NSI.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

297. Respondents did not provide specific answers to this question. Some noted that many terms used in the definitions were broad and generic and so inclusion of the context of the perceived risk that they represent would be helpful.

Government response

298. We have refined the definitions of key terms within the Data Infrastructure definition to ensure that they are sufficiently clear and understood.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

299. It was suggested the definitions would capture a very wide segment of the economy, including some entities that they perceive to present low risks to national security.

Government response

300. We have refined the scope of the Data Infrastructure definition to ensure that entities that pose potential risk are captured, while those that do not pose such risks are excluded by the regime. For example, we revised the scope of relevant data so that entities are only captured if they have a direct contractual relationship with a critical sector entity to store, process or exchange that critical sector entity's data. We have also narrowed the number of mandatory sectors that are cross-referenced as critical sector entities, from 17 to seven. These mandatory sectors are undergoing continued policy development and are subject to change. The definition of relevant data will be reviewed in light of any changes that impact our policy intent.

301. We also revised our description of access and separated physical and logical access with more clearly defined terms. This included removing landowners and leaseholders as categories of entities captured by the definition.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

302. Several respondents suggested that a new definition was not necessary because existing screening legislation, such as the Enterprise Act 2002, already consider issues of national security.

Government response

303. Data infrastructure has not previously been defined in law, including within the Enterprise Act 2002. It is a sector of growing importance and emergent risks that the Government is considering holistically for the first time. Moreover, the powers set out in the Enterprise Act 2002 are outdated and in need of reform and modernisation to ensure that we are keeping pace with new technology and evolving risks to data.

304. The Government believes that it is no longer appropriate for the UK's national security investment screening to be intertwined with our competition regime. The NSI will separate these issues. In addition, the Enterprise Act 2002 is solely focussed on relevant merger situations. The new regime will widen the range of investment activity in scope and introduce a mandatory notification regime.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

305. Respondents commented that the scope of the definition was quite broad. They also stated that there were multiple regimes such as the Enterprise Act 2002 and Network and Information Security (NIS) regulations that potentially apply to these sectors, and so the Government should consider the interplay to ensure a unified approach. This would minimise the burden on businesses.

Government response

306. We have refined the scope of the Data Infrastructure definition in response to the concerns raised by respondents. For example, landowners and leaseholders were removed as categories of entities with access to data infrastructure that present a national security risk. We believe such changes help to ensure an appropriate balance between safeguarding national security risk and minimising the burden on businesses.

307. In relation to the interplay with existing legislation, the laws mentioned by respondents each have separate functions. The Enterprise Act 2002 is principally a voluntary notification merger regime, while the National Security and Investment Bill focuses on national security risks. The NIS is a cybersecurity regulation and does not involve investment screening.

Question 19. Does the data infrastructure definition capture all entities whose operations give it potential access to relevant data or relevant data infrastructure, and exclude those without such access?

308. Many respondents advised that landowners, property investors and leaseholders of land on which relevant data infrastructure was housed, who were not involved in its ownership, operation or management, would not have access to those facilities or the data stored within them. Also relating to access, some industry stakeholders noted that there were service providers with physical access to data infrastructure that would not have access to data itself.

309. We received significant feedback on the complexity of entities in the data infrastructure sector being able to determine the nature of the data stored within their facilities. Consequently, the requirement for entities captured by the definition to know whether they held 'relevant data' would place an unreasonable and commercially damaging burden on the sector. There was further concern that linking 'relevant data'

to entities caught by all other sectors subject to mandatory notification would be very wide and difficult for businesses to assess.

310. Other respondents noted that the reference to Software Defined Networks without any further threshold or caveat would capture many entities operating in the digital space and not necessarily those with access to relevant data infrastructure.

Government response

311. In response to the consultation and direct industry engagement we have revised our understanding of relevant data infrastructure and narrowed the qualifying entities to only those whose business activities yield such access. For example, landowners and leaseholders have been omitted as categories of entities captured by the definition. We also revised our understanding of access, separating physical and logical access with more clearly defined terms. This included removing the illustrative reference to Software Defined Networking and providing a precise definition of 'administrative access'.

312. We have taken onboard the advice around the infeasibility of entities always knowing what type of data they store. An entity is now captured only if it knows by virtue of a direct contractual relationship with a critical sector entity it stores, processes or transmits relevant data. We have also narrowed the number of sectors considered to hold relevant data in the draft definition. These changes will make it easier for businesses to self-assess whether they are subject to mandatory notification.

313. Other consultation responses were considered but did not lead to changes. For example, respondents suggested that managers of colocation data centres - who are responsible for the facility but do not have access to client data - should not be captured. While we accept the distinction managers of colocation data centres, we have continued to capture them in the revised definition due to the national security risks associated with facility management.

***Question 20. If you are a data infrastructure owner or operator, we are interested in more details about your current ways of working. How do you manage technical services wi*thin your facility? To what extent are these provided by in-house staff or outsourced and how is security of data ensured?**

314. There were no detailed responses to this question. One respondent advised that operational duties are done internally, security services are sometimes outsourced and that infrastructure maintenance is performed by manufacturers. Another noted that business models vary.

Government response

315. No changes were made in response to this question due to the lack of evidence provided in consultation responses.

Question 21. How many businesses provide the following services to relevant data centres, and what proportion of their overall business is the sector likely to constitute: security services; installation/maintenance/repair services; and virtualised services?

316. There were no substantive responses in relation to this question.

Government response

317. The Government has removed the provision of security services to relevant data infrastructure from the revised definition. We recognise that we need to build our understanding of the data infrastructure-specific security services sector to ensure that we are not having a disproportionate impact on businesses. Currently, there is a degree of coverage of security firms in the data infrastructure space in the Critical Suppliers to Government mandatory sector, which captures entities providing physical security services to government bodies. Other options for mitigating risk include procurement guidance to data infrastructure operators or the Secretary of State to using the call-in power where necessary.

Question 22. We would like to understand existing approaches to managing the national security risks to relevant data and relevant data infrastructure. In particular, how are the following risks currently managed: a landlord/site owner's access to a data infrastructure facility that is owned or operated by a different entity; a third party service provider (such as security, installation, maintenance) having access to data infrastructure facilities and sensitive data; a third party virtualised service provider having access to data infrastructure or sensitive data?

318. Respondents provided an overview of the physical and cyber security measures enforced at their facilities. Several noted that protections were also contractually required, in accordance with internationally recognised and peer reviewed standards. Similarly, existing approaches to managing security risks include implementing appropriate technical and organisational measures to comply with regulatory obligations (Network and Information Security regulation, UK General Data Protection Regulation, the Telecommunications (Security) Bill) and adhering to security best practice. Finally, some respondents noted that conducting due diligence and risk assessments of third-party providers was a further way to mitigate risk in the sector.

Government response

319. The Government welcomes the information provided by respondents to the consultation. None of the responses contradicted the rationale for our inclusion of data infrastructure nor the scope of activities captured by the definition. We made no direct changes in response to the answers to this question as a result.

Conclusion

320. Data is now a key driving force of the world's modern economies. It fuels innovation in organisations large and small, across the private, public and third sectors. Data Infrastructure is the infrastructure that underpins our modern use of data. It provides the ability to store, process and transfer data. The Government has a responsibility to ensure that data and its supporting infrastructure is resilient, secure and trustworthy in the face of established, new and emerging risks, protecting the economy as it grows.

321. National security risks can arise where an entity's normal business activities give it access to data infrastructure that is used to store, process and/or exchange relevant data and/or to facilitate interconnection. Such access could be achieved by entities that own or manage key data infrastructure, or by entities that provide certain services to such infrastructure, virtual or physical.

322. The consultation responses provided useful insight, including from industry, on the data infrastructure sector. This informed our revision of the sector definition. Changes made include refined definitions of administrative access, relevant data and data infrastructure, amending the qualifying entities to those whose business activities yield such access. For example, landowners and leaseholders have been omitted as categories of entities captured by the definition.

323. The revised data infrastructure definition will provide the Government with a strong lever to mitigate national security risks while minimising the impact on businesses in the sector.

Defence

Revised Draft Definition:

Defence

1. A qualifying entity that carries out activities that comprise or include the research, development, design, production, creation or application of goods or services which are used or provided for defence or national security purposes where that entity meets the conditions in paragraph (2).

2. The conditions referred to in paragraph (1) are that the entity—

(a) is a government contractor or any sub-contractor in a chain of sub-contractors which begins with the government contractor who provides goods or services; or

(b) has been notified by or on behalf of the Secretary of State of information, documents or other articles of a classified nature which the entity or an employee of his may hold or receive relating to the activities within the scope of paragraph (1).

3. In this Part—

"defence" has the meaning given to it by section 2(4) of the Official Secrets Act 1989; and

"government contractor" has the meaning given to it by section 12 of the Official Secrets Act 1989.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

324. Respondents were generally of the view that the definition is clear and comprehensive.

325. Several respondents indicated that 'national security' (which appears within the Defence definition) should be clearly defined.

326. Several respondents advised that the Government should consider introducing a 'safe harbour' for businesses that are not aware that they are making supplies for a defence-related use. Another respondent stated that including all sub-contractors in lengthy or complex supply chains will put an obligation on a small supplier to understand elements of a supply chain far removed from their own role.

327. Some respondents stated the definition could capture contractors or subcontractors who are providing goods or services unrelated to defence (e.g. cleaning or hospitality services).

Government response

328. The Government recognises that the draft definition could capture contractors or sub-contractors who are providing services such as catering or cleaning to defence or national security facilities. This is consistent with the policy intent since contracts that provide access to such facilities may still give rise to potential national security risks.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

329. Most respondents offered no substantive response to this question. Those who did suggested that the terms used in the definition are concise, correct and sufficiently clear for the purposes of determining relevant activities.

Government response

330. The Government acknowledges the responses received.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

331. Respondents agreed that the definition covers an area of significant potential national security risks, particularly with regard to the safeguarding of classified information and securing vital inputs for Defence within the supply chain.

Government response

332. The Defence sector is acknowledged as one of the most sensitive areas of the economy with clear links to national security.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

333. Most respondents had no related suggestions. Two respondents suggested that inserting change of control clauses and clauses that require contractors to seek consent before sub-contracting services would be a better way to address the national security risk posed by changes of ownership in such entities.

334. One respondent noted that the Ministry of Defence (MOD) has a contractual requirement for providers to notify a change of control of contractors/sub-contractors (DEFCON 566 - Change of Control of Contractor) and stated that it must be aligned with the NSI regime.

Government response

335. DEFCON 566 (Change of Control of Contractor) currently encapsulates the MOD requirement that contractors should notify MOD of a change of control and communicate this requirement to sub-contractors. MOD is working to ensure alignment with the NSI regime.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

336. Respondents generally agreed that the definition strikes a balance between national security and investor needs, noting that investors are generally aware that defence-related activities carry additional responsibilities and requirements for government approval due to their sensitive nature.

Government response

337. The Government acknowledges the responses received.

Conclusion

338. A robust defence sector is vital to our national security. It is essential for the development of innovative and first-class military capabilities that enable us to protect our people, territories, values and interests at home and overseas. The defence sector provides advanced capabilities for our Armed Forces and those of our allies.

339. The importance of companies with a direct contractual or sub-contractual relationship with Defence is clear. These companies hold information and capability that is critical to the defence of the United Kingdom. It is therefore imperative that the Defence supply chain is protected from threats, including hostile investment, which may provide adversaries with access to sensitive information or capabilities.

340. This definition focuses on UK Defence and the Defence supply chain and is designed to include companies at all tiers, including sub-contractors and those in the chain of sub-contractors, where the goods or service that they research, develop, design, produce, create or apply are provided or used for defence or national security purposes. The mandatory notification requirement applies to entities whose UK activities include the provision of goods or service for defence or national security purposes where they satisfy either one of the two conditions.

341. The first condition in the definition is that the entity is a government contractor or any subcontractor in a chain of sub-contractors which begins with the government contractor. The Government expects that most suppliers who are providing goods and services for defence and national security purposes will to be aware of the nature of their contractual arrangements. The Ministry of Defence has a standing contractual requirement for providers to notify the Ministry of Defence of a change of control of the Contractor, including any sub-contractors. It is expected that the mandatory notification requirement will reinforce this standing requirement and the entities with a statutory obligation to notify will be clearly identifiable by virtue of their contractual arrangements.

342. The second condition is that the entity has been notified by the Government that they hold, or may come into possession of, classified material. The Government has an established Security Policy Framework and entities who are subject to that framework are notified that they are involved in the handling of classified material.

This notification is issued in one of several ways, depending on the nature of the activity concerned, but most commonly through the issuing of a Security Aspects Letter or the designation of a facility as a List X.

343. Consultation responses generally recognised the importance of ensuring HMG has visibility of changes of ownership of the Defence and national security suppliers to ensure that national security risks can be properly assessed.

344. Some respondents noted that the definition would include contractors/sub-contractors providing goods or services without clear 'Defence' applications, such as catering or cleaning. But contracts which provide access to defence and facilities may still give rise to potential security risks - and are included for this reason.

Energy

Revised Draft Definition:

Energy

1. A qualifying entity that carries out any of the activities set out in paragraph (2).

2. The activities referred to in paragraph (1) are the ownership or operation of—

(a) terminals, upstream petroleum pipelines or infrastructure which is or will be necessary to a petroleum production project, with (i) a throughput of greater than 3,000,000 tonnes of oil equivalent over the last 12 months or (ii) for prospective terminals, upstream petroleum pipelines or infrastructure, greater than 3,000,000 tonnes of oil equivalent is expected to flow in its first year of operation;

(b) licensed "transmission" or "distribution" operators as defined in section 6 of the Electricity Act 1989 or section 7 of the Gas Act 1986;

(c) gas or electricity interconnectors, long range gas storage and gas reception terminals, including Liquefied Natural Gas;

(d) Authorised Electricity Operators in Great Britain that provide load via:

(i) individual assets that would have a total installed capacity, greater than or equal to 100 megawatts; or

(ii) assets that, when cumulated with those of the affiliated undertakings of the acquiring entity, would have a total installed capacity, greater than or equal to one gigawatt;.

(e) aggregators that control assets in Great Britain, that when cumulated have a total capacity greater or equal to one gigawatt;

(f) entities that supply petroleum-based road, aviation or heating fuels (including liquefied petroleum gas) to the United Kingdom market, via

(i) a company that provides or handles more than 500,000 tonnes per annum; or,

(ii) a downstream facility owner if the owned facility has capacity in excess of 50,000 tonnes;

where either carry out any of the following activities:

(aa) the import of any of crude oil, intermediates, components and finished fuels;

(bb) the storage of any of crude oil, intermediates, components and finished fuels;

(cc) the production of intermediates, components and finished fuels through a range of refining or blending processes;

(dd) the distribution of petroleum-based fuels to other storage sites throughout the UK by road, pipeline, rail or ship;

(ee) the delivery of petroleum-based fuels to retail sites, airports or end users.

3. In paragraph (2)—

"aggregator" is a natural or legal person who combines multiple customer loads or generated electricity for sale, purchase or auction in the GB electricity market;

"Authorised Electricity Operators" means any person (other than the licensee) who is authorised to generate, participate in the transmission of, distribute or supply electricity or participate in the operation of an interconnector;

"gas" has the meaning set out in section 2 of the Energy Act 2008;

"gas importation and storage project" means a project carried out by virtue of a licence granted under section 4 of the Energy Act 2008;

"load" is defined pursuant to the Grid Code as "the Active, Reactive or Apparent Power, as the context requires, generated, transmitted or distributed";

"petroleum", has the meaning set out in section 90 of the Energy Act 2011;

"petroleum production project" has the meaning set out in section 90 of the Energy Act 2011;

“terminal" has the meaning given to it by Section 90 of the Energy Act 2011;

"upstream petroleum pipeline" has the meaning given to it by Section 90 of the Energy Act 2011;

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

345. The majority of respondents sought further clarity on the scope of the definition. Much of the feedback focused on the potential for different interpretations of the terms used. Particular concern was expressed over what constitutes a ‘Petroleum Production Project’ as well as language used such as ‘form part of’ or ‘involved in’ that could be interpreted in different ways. There was some concern over the varying use of ‘and / or’ where it was unclear whether a company had to perform both functions to fall within scope.

346. Respondents also believed that the thresholds should be clarified further, including how they were assessed (actual production/capacity, timeframes). Further clarity was also requested on whether infrastructure needed to be operational or if projects in construction would be included.

Government response

347. The Government has taken account of the consultation responses. The updated definitions will provide significantly more detailed breakdown of exactly what is and is not captured. We will set out how thresholds will be measured and over what period, and we will aim to reference as many existing legislative definitions as possible.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

348. Respondents noted that that any technical or scientific terms were generally well understood but requests were made for all wording to be fully defined where possible.

349. There were suggestions on the use of MegaWatts (MW) in the generation thresholds and the difference between Alternating Current and Direct Current values. Questions were also raised on the use of tonnes as a form of measure of oil instead of barrels.

Government response

350. The Government supports providing definitions for all technical and scientific terms where required. The Government will ensure specific points around MWs is clarified but believes the use of tonnes for oil thresholds is correct as it is widely recognised and commonly used in existing regulation (such as the Network and Information Systems Regulations) and publication of Government energy statistics.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

351. There was widespread consensus that Energy is a critical part of the economy and there are clear national security risks.

Government response

352. The Government welcomes industry's agreement that Energy is a critical component of national security, demonstrating its need for inclusion in the mandatory notification regime.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

353. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

354. There was widespread agreement that the definitions covered areas that may pose a national security concern. Some specific areas within the definition were questioned, such as the inclusion of Electricity Suppliers (retail), concerns over lack of future proofing for the electricity sector and that thresholds were too low across oil infrastructure.

Government response

355. Electricity suppliers (retail) are not in scope of the legislation. This has been the policy intent from the outset as this would likely have a detrimental and burdensome impact on retail energy suppliers, entities that do not own any infrastructure. All reference to 'supply' or 'suppliers' has been removed and the full legal definitions will not include this language.

356. As we develop the final definition, we will continue to review the thresholds for oil infrastructure. The threshold for the capacity of a downstream facility will be revised from 20,000 tonnes to 50,000 tonnes.

357. We will also review the electricity definitions to cover entities with a key role in overseeing or operating any part of the GB electricity and gas markets.

Conclusion

358. Energy underpins every aspect of modern life and a secure and reliable energy supply is vital to enable a thriving country. We are keen that we are able to ensure a safe, secure and reliable supply of energy.

359. The increasing digitalisation and globalisation of the energy system means we must be extra vigilant in identifying investment in novel energy technologies and services. While the definitions focus on established technologies and services, these will be continuously reviewed and updated to ensure they reflect the rapid development taking place within the sector as the UK strives to meet its net zero target. The consultation feedback has been broadly very positive and the full detailed legal definitions that will be included in the legislation should provide companies the additional level of detail they have asked for in the consultation.

360. The Government has broadly adopted many of the changes recommended by participants in developing the detailed definitions.

Military and Dual-Use

Revised Draft Definition:

Military and Dual Use

1. A qualifying entity whose activities consist of or include researching, developing or producing restricted goods or restricted technology.

2. In this Part—

"restricted goods" and "restricted technology" are goods and technology, including software or information, other than information in the public domain, the export or transfer of which is controlled by virtue of their being specified in the relevant export control legislation;

"relevant export control legislation" means—

(i) Schedules 2 and 3 to the Export Control Order 2008;

(ii) the Schedule to the Export of Radioactive Sources (Control) Order 2006;

(iii) Annex I to Council Regulation (EC) No. 428/2009.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

361. Respondents were generally of the view that the consultation definition was clear and comprehensive, but rather broad.

362. It was also suggested that the reference to 'holding information' was overly broad and should be narrowed, suggesting that businesses may not be aware they hold information that meets the conditions set out in the consultation draft definition.

363. Some respondents suggested that the draft definition should be amended to provide further clarity and Section 1b of the consultation definition, which referred to the holding of information capable of use in connection with the development or production of restricted goods could be removed. Section 1b of the consultation definition concerned an entity whose activities consist in or include "holding information (including but not limited to information comprised in software and documents such as blueprints, manuals, diagrams and designs) that:

i. is capable of use in connection with the development or production of restricted goods; and
ii. is responsible for achieving or exceeding the performance levels, characteristics or functions of the restricted goods that are specified in the relevant export control legislation."

364. One respondent commented that reference to the Dual-Use list in its entirety will result in the notification of transactions which do not pose any national security risk - and that only the most sensitive items should be subject to mandatory notification.

365. Another respondent mentioned that the inclusion of the 'military and dual-use sector' only serves to bring within scope investments in businesses that are less sensitive from a national security perspective, in light of the existing export control regime. It was suggested the Government remove military, defence and dual-use from scope so there is no contradiction or duplication with existing laws. A further respondent suggested explicit reference to items in scope rather than the inclusion of Export Control orders.

Government response

366. The draft definition has been amended to take account of respondent views. This sector has been identified across government as one of the most sensitive, so will be subject to mandatory notification of proposed transactions. We must ensure that the Export Control Criteria cannot be circumvented by allowing the acquisition of companies that produce such goods, rather than buying the goods themselves, without effective screening.

367. The issue of scope of the requirement, in particular, concerning the holding of information, has been addressed by focusing the requirement on restricted technology that is captured under the relevant Strategic Export Lists.

368. The revised definition now further clarifies that information within the public domain would not, on its own, trigger the notification obligation. It also removes the exclusion for controls that only concern a single country. This exemption raised a consistency point in principle as a single country control would not raise the obligation, but two or more countries would - thus adding to the complexity for entities seeking to establish whether the obligation applied.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

369. There were limited responses to this question. Those who did in general suggested that the terms used in the definition are clear, with only one respondent suggesting they were too broad.

370. One respondent suggested it is not entirely clear as to the extent to which items falling within Schedule 3 of the Export Control Order 2008/3231 (the UK Dual-Use List) fall within scope, as some entries are controlled only for export to particular destinations.

371. One respondent suggested where a business only deals in dual-use items within the UK and does not make exports, there is limited risk to national security. Therefore, they should not be covered in scope of the mandatory notification regime especially, in light of the existing export regime.

Government response

372. The Government has shortened and further clarified the definition.

373. We disagree that dual-use items made for UK markets alone should not come within the mandatory notification regime. Certain acquisitions, particularly where the acquirer is under the control of an adversary state, may result in the loss of core dual-use capability, even if the target did not export ahead of the transaction. This point highlights how the NSI regime sits alongside export controls to provide a comprehensive regime protecting our national security capability.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

374. Respondents agreed that the definition covers an area of potential national security risk.

Government response

375. The military and dual-use sector is acknowledged as one of the most sensitive areas of the economy with clear links to national security.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

376. One respondent suggested that the pre-existing export control licensing regime is appropriate, for which a number of businesses have robust and sophisticated compliance programmes - noting a ‘significant overlap’ between the lists and a number of the other proposed mandatory sectors.

Government response

377. The Government recognises the value of the existing export control regime but considers it essential that the military and dual-use sector is included within the National Security and Investment Bill as one of the most sensitive sectors for which the mandatory notification requirement should apply.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

378. There was a mixed response, with several respondents suggesting a reduction in scope of the definition.

379. One respondent suggested that the scope of the definition should be narrowed to ensure a clear focus on only the most sensitive businesses - possibly by limiting the list of relevant control entries under the lists that are within scope; removing section 1(b) of the draft consultation definition (a suggestion supported by an additional respondent); or removing references to elements of the control lists that duplicate sectors that are already proposed to be subject to mandatory notification.

Government response

380. The scope of the definition has been narrowed in response to the suggestions made by respondents.

Conclusion

381. Military and dual-use technologies cover the design and production of military items (such as arms, military and paramilitary equipment) and dual-use items which can be used for both military and civil purposes. Military and dual-use items can, in the wrong hands, pose clear and immediate risks to the UK, our people and society. There are also indirect national security interests – for example, innovative UK businesses help to ensure that our Armed Forces maintain a clear operational advantage over others. The acquisition of such companies - with their expertise and intellectual property - by a potentially hostile actor is highly likely to raise national security concerns.

382. Military and dual-use goods appear on the Strategic Export Control lists, which place restrictions on exporting them overseas, because their transfer must be carefully controlled for national security reasons. We must ensure that the Export Control Criteria cannot be circumvented by allowing the acquisition of companies that produce such goods, rather than buying the goods themselves, without effective screening. This does not, however, include goods on the Human Rights Strategic Export Control Lists unless they appear on the Military and Dual-Use Lists, as while human rights are of great importance to the Government, this is beyond the scope of this legislation and is best addressed through other means.

383. This definition covers entities that develop or produce restricted goods or technology. Restricted goods or technology are goods, software or information, not including information in the public domain, which are controlled by the export control legislation set out below:

- Schedules 2 and 3 to the Export Control Order 2008;
- the Schedule to the Export of Radioactive Sources (Control) Order 2006; or
- Annex I to Council Regulation (EC) 428/2009

384. Most consultation responses recognised the rationale behind including military and dual-use production capabilities in the mandatory notification category. The need to protect these capabilities is clear.

385. Some respondents highlighted the scope of the dual-use controls and noted that the mandatory notification requirement would attach to entities even where those entities were not exporting their products. We recognise that the obligation may capture entities producing for civilian use and entities which are not exporting. The object of this requirement is to protect against the transfer or loss of capability, particularly advanced capability, which has military use, even where that isn’t the development or production focus of the entity concerned. The export control legislation listed, provides a

comprehensive and consolidated list of dual-use controls and reference to these lists is more appropriate and less burdensome than the devising of a separate list.

386. A number of respondents expressed concerns about the inclusion of entities who hold information capable of use with or improvement of restricted goods. This requirement could include a potentially large range of information, and entities may not be aware that the information that they hold is able to be used in that way. We have reviewed this requirement and agree that it is possible to interpret the previous drafting in an open-ended way. We have therefore looked at how to clarify the application of the obligation. There is clearly a national security concern in ensuring that information and technology concerning restricted goods is not lost, misused or does not fall into the hands of hostile parties. We have therefore focused the requirement on the technology controls already set out in the export control lists.

Quantum Technologies

Revised Draft Definition:

Quantum technology

1. A qualifying entity carrying on activities that consists of developing or producing quantum technology.

2. In this Part—

"quantum technology" means—

(i) quantum communications;

(ii) quantum connectivity;

(iii) quantum imaging, sensing, timing or navigation;

(iv) quantum information processing, computing or simulation; or

(v) quantum resistant cryptography;

"quantum communications" means—

(i) the transmission of information, utilising the properties of quantum mechanics, specifically superposition, entanglement, single photon technology or the use of conjugate variable technologies;

(ii) the use of a communication network (quantum or otherwise) to distribute quantum states or quantum state information; or

(iii) the establishment of cryptographic keys or the generation of provably random numbers using a quantum physical process;

"quantum connectivity" means the ways in which quantum coherence, during processes such as transmission, propagation or amplification, is preserved;

"quantum imaging" means utilising the phase or amplitude properties of quantum mechanics, specifically superposition, entanglement or the use of sub-Poissonian sources or detectors of photons, to create images of objects;

"quantum information processing, computing or simulation" means the simulation or realisation of systems that utilise certain properties of quantum mechanics, in particular superposition or entanglement, to acquire, encode, manipulate or process information, run algorithms or perform operations or measurements on data, including—

(i) algorithms, applications, software, error correction, noise reduction and operating systems that enable the functionality of the system;

(ii) the use of a classical computer to represent the internal state and operations of a quantum computer ("Quantum Emulation");

(iii) the hosting or provision of third party access of a quantum information processing, computing or simulation cloud-based service;

"quantum navigation" means utilising phase properties of quantum mechanics, specifically measurements of atoms or ions, or atom-ion interferometry, to establish the location, inertia of, and to guide, objects;

"quantum resistant cryptography" means methods of securing information or data being transmitted or stored, with a view to resisting attack by a quantum computing or simulation device;

"quantum sensing" means utilising the phase properties of quantum mechanics, specifically measurements of atoms or ions or atomic spin systems, to determine a property or rate of change in the property of an object, or the effect of an object on a measurable quantity;

"quantum timing" means utilising the phase properties of quantum mechanics, specifically measurements of atoms or ions or atomic gases, and the application of associated hardware including stable frequency mixers, optical or microwave sources, crystal oscillators and frequency combs, to provide a timing or synchronisation signal, or frequency reference.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

387. Most respondents stated that the sector definition was clear and well understood. However, several respondents suggested that the definition would cover the majority of transactions relating to the sector, including the academic research community and associated supply chain sectors. Multiple responses noted that the phrase 'develops or produces anything designed, modified or adapted for use or application in…' was too broad and could capture a wide range of components that are also used in non-quantum systems.

388. One response proposed that research entities should be narrowed to only those that hold and control transferable research outcomes including IP rights and know-how. Another response suggested tightening the scope of qualifying entities for each technology group by identifying certain threshold performance levels above which mandatory notification would be required.

389. It was also suggested that more could be done to pre-empt the development of new quantum technologies that are likely to emerge in the next 5-10 years, particularly where new materials are being explored.

Government response

390. The Government intends to tighten the scope of entities subject to mandatory notification, so that it only captures entities that develop or produce a quantum technology product (as defined in the technical descriptions). We have excluded entities that only undertake research in quantum from mandatory notification, as well as entities that use quantum technologies to enable them to supply a service, and the broad range of supply chain companies.

391. We are continuing to work with experts in the sector to explore the potential for more detailed work to refine the technology definitions further for inclusion in the final regulations, for example the development of a limited list of essential supply chain components for quantum technologies or the use of performance thresholds.

392. We recognise that the field of quantum technologies is developing rapidly, and we will keep the definitions under review and update them as needed.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

393. The technical terms used in the consultation definition were generally considered to be accurate, well defined and clear in the view of the respondents.

394. Through written and direct engagement, respondents suggested alternative technical terms or descriptions that could help to clarify the definitions of all of the sub-categories

of quantum technologies (other than quantum-resistant cryptography). One response recommended wording to make it explicit that conventional digital computers (that also make use of quantum mechanics) are not in scope of the regulations. There was a suggestion to consider the hybrid classical/quantum devices that could emerge over the decade.

395. One response noted that the quantum connectivity definition could refer to any component in a system, and therefore was too broad in its drafting.

Government response

396. We have worked closely with technical experts to refine the technical definitions of each sub-category of technology based on consultation with the sector.

397. Through testing consultation responses with experts in the quantum technologies field, we have taken on board technical suggestions from respondents where it has helped to improve scientific accuracy, better define the underpinning physical effects and associated hardware that enable a quantum technology's functionality, or to greater clarify the intended focus on second-generation quantum technologies.

398. Where helpful we have further defined technical terms to ensure that the meaning is well understood and unambiguous for the purposes of these regulations. We have removed the phrase 'suspensions of atoms or ions' from the definitions of quantum navigation, sensing and imaging as this was technically inaccurate. We have also re-framed the definition of connectivity to take on board feedback that the previous definition was too broad.

399. We intend to review and update the technical definitions in the future as quantum technologies develop.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

400. Several responses noted that the definition covers all areas of potential national security interest, but in doing so bring the majority of the sector, academic community and associated supply chain sectors into scope of mandatory notification.

401. Some responses noted that the definitions could better differentiate between quantum technologies that are of the most interest to national security, and those that are of less interest and could be exempted from mandatory notification requirements. It was suggested that elements of quantum information processing that could be of national security interest other than hardware should be added to the definition, such as quantum software.

402. Extending the definition of quantum communications to cover the use of a communication network that distributes quantum state information was also proposed.

Government response

403. We have considered feedback on differentiating between the security risks of different quantum technologies. The Government's position remains that all areas of second-generation quantum technology development are of potential importance for national security. This is predicated on the dual-use potential that all quantum technologies hold, which in the wrong hands would pose clear risks to the UK. Whilst many quantum technologies are developed for civil purposes, it is the application of the technology product that gives rise to national security concerns.

404. For instance, quantum-secured communications, computing and cryptography are all anticipated to have a significant impact on how Government, industrial and personal information is stored, shared and analysed in the future. Quantum imaging, gravity sensing (such as for detection of hostile activity), precision timing or sophisticated navigation technologies (such as underwater) all present the opportunity for significantly enhanced military capabilities.

405. Quantum computers are expected to pose a significant threat to the cryptographic systems which underpin much of our existing cyber security. We have amended the definition of 'quantum computing or simulation' to explicitly capture other areas of quantum information processing that enable the hardware to perform its function, including algorithms, applications, software, error correction, noise reduction and operating systems.

406. The use of a communication network to distribute quantum state information has been added to the revised definition.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

407. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

408. It was noted by several respondents that, whilst the definition would cover all transactions of potential national security interest, it would cover majority of transactions in the sector, including the academic research community, associated supply chain and end users of the technology. This could pose a burden on businesses and have an adverse effect on inward investment into the sector if transactions were delayed.

409. Multiple respondents expressed concern that the early stage of quantum technology development would mean that start-ups do not receive the necessary early investment where investors are concerned about future issues in exiting the investment.

410. Multiple responses recommended an exemption for academic entities from mandatory notification where fundamental research is taking place.

411. Some responses noted that the definitions could better differentiate between quantum technologies that are of the most interest to national security, and those that are of less interest and could be exempted from mandatory notification requirements.

412. There was a concern around requiring entities supplying services employing technologies to mandatorily notify the Government of transactions, even if they have not contributed to the quantum technology's development or production. Another response recommended the addition of quantum software and quantum cloud computing as a service.

Government response

413. We are tightening the scope of entities subject to mandatory notification to only captures entities that develop or produce a quantum technology product. We are working with experts in the sector to explore the potential for the development of a limited list of essential supply chain components for quantum technologies, for inclusion in the final regulations.

414. We have excluded entities that only undertake research in quantum from mandatory notification, as well as entities that use quantum technologies to enable them to supply a service, and the broad range of supply chain companies.

415. The Government's position remains that all areas of second-generation quantum technology development are of potential importance for national security. This is predicated on the dual-use potential that all quantum technologies hold, which in the wrong hands would pose clear risks to the UK. Whilst many quantum technologies are developed for civil purposes, it is the application of the technology product that gives rise to national security concerns.

Conclusion

416. We have considered all responses to the consultation relating to the quantum technologies sector definition.

417. Based on feedback to the consultation, we have sought to reduce the scope of qualifying entities to only those that develop or produce a specified quantum technology. We have removed provisions that extended the scope of mandatory notification across the supply chain and are working with experts in the sector to explore the potential for a limited list of essential components that are of national security interest, for inclusion in the final regulations. The revised definition excludes entities that solely undertake research in quantum, and entities that use quantum technologies to supply a service.

418. We have closely considered all the feedback on the technical definition for each quantum technology in consultation with technical experts. We have incorporated recommendations where it adds to the technical accuracy or clarity of a particular definition.

Satellite and Space Technologies

Revised Draft Definition:

Satellite and Space technology

1. A qualifying entity carrying out activities that consist of or include operating, designing, producing, creating or utilising facilities for any of the activities set out in paragraph (2).

2. The activities referred to in paragraph (1) are—

(a) space debris management, including sending an object into space to remove or manage existing space debris;

(b) the provision of:

(i) in-orbit servicing and robotics capabilities including life extension services (refuelling, repairs, relocation) or inspection services;

(ii) in-orbit maintenance and manoeuvring, including any technology or system that performs any of the services set out in paragraphs (a) or (b) or which through design could have a use in disrupting, modifying or interfering with satellites;

(c) the provision of inter-satellite communications links including radio frequency and optical links—

(i) between satellites in orbit;

(ii) between space craft and satellites in orbit;

(iii) between satellites in orbit and celestial bodies;

(iv) from Earth to space, and from space to Earth;

(d) operating and maintaining the capability of secure ground infrastructure and associated secure facilities and systems related to space activity or sub-orbital activity or to services derived from space activity to ensure the safe and secure access to capabilities derived from space-based services;

(e) the manufacture and testing of spacecraft and launch vehicles, satellites, planetary probes, orbital stations, manned space vehicles, ground segment equipment, and component parts of, and materials used in, any equipment set out in this sub-paragraph;

(f) the use of space-derived data for any military or national security purpose;

(g) the provision of space infrastructure operational control facilities;

(h) the provision and processing of space situational awareness data by activity on earth or by space activity or by means of infrastructure for any of the following—

(i) orbital and sub-orbital activity;

(ii) near-earth and space weather events;

(iii) national security purposes;

(iv) military purposes.

3. In this Part—

"infrastructure" includes the following listed items for the operation, maintenance, provision, processing or use in relation to any of the facilities set out in paragraphs (2) (d), (g) and (h):

(i) command and control stations;

(ii) ground stations, ground sites and ground segment equipment;

(iii) software (including analysis software);

(iv) information technology and telecommunications networks (including fibre cables);

(v) uplink and downlink terminals;

(vi) data processing and storage facilities (including databases);

(vii) satellites; and

(viii) technological systems and equipment deployed in space or on earth;

"space activity" and "sub-orbital activity" have the meaning given to them by section 1(4) of the Space Industry Act 2018;

"testing" includes any service that provides quality assurance assessment of—

(i) equipment or systems for services derived from space activity, including engines, component parts, radio frequency, software and systems;

(ii) facilities that manufacture, design or create any of the materials set out in paragraph 2(e);

(iii) launch site equipment and facilities; and

(iv) equipment and facilities for transport of satellites, launch vehicles or their major components between sites;

"spacecraft" has the meaning given to it by section 2(6) of the Space Industry Act 2018;

"space derived data" includes data—

(i) obtained from space activity or from ground stations receiving data from outer space or from both space activity and ground stations receiving data from outer space, and

(ii) which relate to—

(aa) position, navigation and timing;

(bb) earth observation;

(cc) space situational awareness;

(dd) telecommunications;

(ee) signal intelligence;

(ff) remote sensing; and

(gg) research and development;

"space situational awareness" includes space surveillance tracking, space weather monitoring and forecasting, near earth objects, and space debris.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

419. The majority of respondents stated that the consultation definition was too broad, and not proportionate to the national security risk. Several responses pointed out that under the consultation definition, almost all transactions in the UK space market would be covered. There were suggestions that we narrow the definition as much as possible.

Government response

420. We have worked to narrow the definition as much as possible, focusing only on those transactions that pose the greatest risk to national security. Several limbs of the original definition have been removed, such as, specialised telecommunications applications, provision of Internet access by satellite infrastructure, space science and exploration activities. We believe that this narrowing will allow the regime to focus on the areas that could pose a risk to national security. Although narrowed the definition is still broader

than those of some other sectors – this is because satellite and space technologies cover a huge range of capabilities, many of which can be used for both a civil and military purpose. It is therefore essential that we include any areas that could potentially pose a risk.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

421. It was generally agreed that the technical and scientific terms were correct and sufficiently clear and commonly understood. However, a few respondents suggested that the definition did not clearly distinguish the parts of the sector that are and are not relevant to national security.

Government response

422. We have worked to narrow the definition as much as possible, focusing only on those transactions that pose the greatest risk to national security. We recognise that the original definition was too broad and did not adequately distinguish between areas of concern to national security and areas not of concern. We have therefore removed several limbs from the original draft definition. We have also made certain references more explicit to increase the focus on national security – for example 'the use of space-derived data for any military or national security purpose'. This narrows the definition further and focusses on the issue of security rather than the general use of space-derived data.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

423. Respondents identified some overlap between other definitions within the mandatory notification regime such as the communications or military and dual-use definitions. Some responses highlighted that space technologies do underpin the functioning of other sectors, which may be the justification for the slight overlap. Several responses stated that the definition was reasonable and did include areas of the economy where foreign investment has the greatest potential to cause national security risks.

Government response

424. We recognise that there is overlap between the satellite and space technologies definition and some of the other mandatory notification sector definitions. Due to the nature of the sector, some overlap is inevitable, as pointed out in some of the consultation responses. We have tried to reduce the amount of explicit overlap with other sectors, for example by removing 'provision of specialised telecommunications applications' which clearly overlapped with the communications definition.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

425. No substantive responses were received in relation to this question.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

426. There was a general concern that the definition was too broad and did not adequately identify areas of national security concern, which could place a burden on commercially focussed businesses, especially start-ups and SMEs as a result. In contrast, some responses suggested that there was no need to narrow the definition further as it already struck the right balance.

Government response

427. We have taken steps to narrow the definition as much as possible so that it only focusses on areas that could be of concern to national security. This should reduce the burden on businesses.

Conclusion

428. The UK is a world leader in small satellite technology, telecommunications, robotics and Earth observation and UK universities are some of the best in the world for space science. Space is a rapidly developing sector that delivers a broad range of services and capabilities. All space-based services by nature have crossover and impact other CNI sectors, and the range of products and technologies available can vary hugely depending on the service (for example, earth observation, PNT, etc.).

429. Risks to the sector include, but are not limited to, hostile state actors, serious organised crime and cyber criminals. The ease with which satellite and space technology can be used for both civilian and military purposes – either in the UK or internationally – is a growing concern and is something that the Government will continue to monitor closely. This concern is nuanced, and the main issue is the potential for adversaries to use what seem to be predominantly civil capabilities to meet military objectives.

430. The Government believes that there are certain assets and entities within the sector that are sufficiently sensitive that they should be included in the mandatory notification regime. The definition covers a range of rapidly changing technologies that are covered by the sector, including but not limited to, aspects such as manufacturing, launch, and operations. Also covered are entities that use space-derived data for national security or military purposes, which may be of particular interest and would merit notification.

431. Several changes have been made post-consultation in line with feedback received. Respondents pointed out that the definition was very broad; we have narrowed the

scope down significantly to focus on only those areas that may pose a significant risk to national security.

Synthetic Biology

Revised draft definition:

Synthetic biology

1. Subject to paragraph 4, a qualifying entity carrying out activities that consist of or include—

(a) carrying out basic scientific research into synthetic biology;

(b) the development of synthetic biology;

(c) the production of goods using synthetic biology;

(d) the formulation of synthetic biology to enable the degradation of materials;

(e) the provision of services that enable the activities in paragraphs (a) to (d).

2. "Synthetic biology" means the process of applying engineering principles to biology to design, redesign or make biological components or systems that do not exist in the natural world.

3. Synthetic biology includes—

(a) the design and engineering of biological-based parts of

(i) enzymes;

(ii) genetic circuits and cells;

(iii) novel devices and systems;

(b) redesigning existing natural biological systems;

(c) using microbes to template materials;

(d) cell-free systems;

(e) gene editing and gene therapy;

(f) the use of DNA for data storage, encryption and bio-enabled computing.

4. A qualifying entity is not required to notify synthetic biology matters that include—

(a) general services and servicing not related to core synthetic biology, where 'core' means those activities without which experiments cannot be conducted, such as DNA synthesis, and cloning;

(b) the use of microorganisms to remove harmful contaminants, pollutants, and toxins from the environment (known as bioremediation), including bio-based reagents that allow for testing for contaminants;

(c) any approach used to gather clinical information for the purpose of making a clinical decision or making a diagnosis (known as diagnostics) but not the storage or ownership of sensitive human genetic information that enables the identification of an individual;

(d) industrial biotechnology research, development and production using enzymes or organisms that have not been modified through the application of systematic biodesign techniques, including the approaches described in paragraph (3);

(e) the production of substances ordinarily consumed as food or used as feed, including any ingredient or component thereof;

(f) gene therapy where it is used solely for the purpose of replacing missing or defective genes to restore phenotypes to achieve a therapeutic effect;

(g) cell therapy where cells are modified by genetic engineering and then introduced into a patient to treat disease.

5. In this Part, "services" means routine synthetic biology processes that are outsourced to specialist providers for completion before being re-integrated into the original work stream to assemble into an experiment or product, including making a specific strand of DNA or running a proprietary algorithm on a dataset.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

432. A common concern raised by respondents was the broad nature of the consulted engineering biology definition, which could make it difficult for businesses to self-assess whether they are in scope. Respondents raised concerns that the scope of the definition would capture all foreign investment in this sector.

433. One response noted that the 'broadly accepted definitions of synthetic/engineering biology do not use differentiated definitions and it is odd that the UK would diverge from the rest of the world on this'. Several respondents suggested areas which could be excluded from the mandatory notification regime because they do not pose a risk to national security. Some suggested that the definition should be updated to explicitly mention activities which are included and excluded.

Government response

434. We are grateful for the response to the formal consultation process and the subsequent engagement. The wide range of views has prompted us to reconsider our approach and helped narrow the definition. The sector now focuses on synthetic biology, and the revised definition makes it clear which activities are included and excluded.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

435. There was a mixture of views about the terminology of the original definition of engineering biology.

436. Respondents suggested the definition of synthetic biology that was included within the wider engineering biology definition differed slightly from established definitions. However, they agreed that the meaning was comprehensible. All feedback was critical of the very broad scope of the definition. A few respondents provided revised versions of the definition, suggesting ways to narrow it.

437. Respondents suggested areas for exclusion, including but not limited to, biologics, cell therapy, gene therapy, diagnostics, vaccines, and bioremediation. One response queried whether technologies that may not have any biological component at all, would be covered by the definition. Another suggestion made by respondents was to exclude early-stage companies.

Government response

438. We recognise that the scope of the engineering biology consultation definition was very broad. As a direct consequence of the feedback, the definition has been comprehensively revised to narrow the focus to synthetic biology. The definition reflects

the technical and scientific advice from stakeholders and is clearer as a result. Activities that are in and out of scope are now clearly articulated.

439. Additional assistance was received from some of the respondents on refining the definition and helping to clarify the wording of some of the exclusions. The revised definition has been through numerous iterations reflecting input from our stakeholders and internal government experts.

440. Some of the suggestions were considered and discounted owing to national security concerns.

441. The technical and scientific terms in the definition reflect the feedback we received, have been checked by our experts, and are deemed to be commonly understood for the purposes of determining relevant activities in the synthetic biology sector.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

442. Many respondents questioned the breadth of the consultation definition as it encompassed all areas of engineering biology. Respondents generally agreed the broad definition would cover areas of national security concern, however some also noted there could be unintended consequences because the definition was over-inclusive.

Government response

443. We have revised the definition after careful consideration of all responses and feedback. Some of the suggested changes have been implemented but owing to the potential for dual-use and national security concerns, there are activities that remain within scope of the reporting regime. Respondents broadly agreed that synthetic biology can pose a national security risk.

444. We have consulted stakeholders and our experts to develop a definition of synthetic biology that captures the main areas of concern whilst trying to minimise any unnecessary burden on businesses. Each of the excluded activities has been developed by experts and covers clearly defined areas such as: diagnostics, industrial biotechnology, food related, gene therapy, general services, and cell therapy.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

445. There were limited responses to this question. A few respondents questioned the inclusion of the original definition of engineering biology under the mandatory notification regime. They suggested the voluntary notification regime and the call-in powers would be sufficient.

Government response

446. The narrowing of the definition will help to minimise the impact on businesses. Whilst the voluntary and call-in powers are useful, monitoring a rapidly developing and changing sector such as synthetic biology is almost impossible without the use of a mandatory notification regime.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

447. A consistent concern throughout the responses related to the broad nature of the definition and its potential impact on companies innovating within this and other sectors.

Government response

448. The definition has been narrowed to reflect the responses from stakeholders. After consultation with stakeholders and experts, we are confident the revised definition strikes the right balance between safeguarding national security and minimising the burden on UK businesses and foreign investors.

449. It is important in a sector such as synthetic biology that all sizes of company are in scope. This is consistent across all sectors.

Conclusion

450. A continuing theme throughout the consultation phase was that the definition of engineering biology was too broad. In direct response to this, the definition has been narrowed to 'synthetic biology' and comprehensively revised to reflect stakeholder suggestions about activities that could be excluded. By changing the sector name to synthetic biology, it now focuses on the areas of most concern and is instantly recognisable by businesses and investors.

451. The policy intent continues to be ensuring the UK has appropriate safeguards in place to protect our national security and make the UK a global biotechnology partner of choice. We want to encourage research and development that will be crucial to combating current and future risks, and which makes an important contribution to UK economic prosperity and security.

452. Synthetic biology is, by its very nature, rapidly evolving and technically complicated. Many of the tools or enabling technologies are dual-use, and difficult for the Government to comprehensively monitor well enough to proactively 'call-in' transactions that are not routinely notified. The dual-use issue makes it difficult to identify organisations involved in defence and security related work or whose work could be used or repurposed for nefarious means.

Transport

Revised Draft Definition:

Transport

Ports and Harbours

1. A qualifying entity carrying on activities that consist of —

(a) owning or operating a port or harbour situated in the United Kingdom that handled 1 million tonnes or more of cargo in the year preceding the year in which notification is given under section 14 (Mandatory notification procedure) of the Act, as recorded in the Port Freight Annual Statistics published by the Department for Transport; or

(b) owning and operating terminals, wharves or other infrastructure situated in a port or harbour described in sub-paragraph (a).

2. In paragraph 1—

"harbour" has the same meaning as in set out in section 313 (1) of the Merchant Shipping Act 1995;

"infrastructure" means the infrastructure, facilities and equipment within a port or harbour which enable the effective operations directly related to the movement of freight, passengers or seafarers;

"operating" means controlling the functioning of the port, harbour, terminal, wharf or other infrastructure situated in a port or harbour; and

"port" means an area of land and water made up of such infrastructure, facilities and equipment so as to permit—

(i) the receiving and departing of ships;

(ii) the loading and unloading of ships;

(iii) the storage of cargo;

(iv) the receipt and delivery of cargo; or

(v) the embarkation and disembarkation of passengers, crew and other persons; and

"ship" has the meaning set out in section 313 (1) of the Merchant Shipping Act 1995.

Airports

3. Qualifying entities carrying on activities that consist of—

(a) owning or operating an airport situated in the United Kingdom that handled at least six million passenger movements or 100 000 tonnes of freight in 2018, as recorded in the UK Airports Annual Statements of Movements, Passengers and Cargo published by the Civil Aviation Authority;

(b) providing en route air traffic control services in the United Kingdom;

(c) owning a provider of en route air traffic services in the United Kingdom.

4. In paragraph 3 —

"airport" has the meaning set out in section 66 (1) of the Civil Aviation Act 2012;

"en route air traffic control services" mean services provided pursuant to a licence under section 6 of the Transport Act 2000;

qualifying entities owning a provider of an en route air services traffic provider include—

(i) a company which owns such a provider (C);
(ii) any parent undertaking of C (P1); and
(iii) any parent undertaking of P1 (P2);

qualifying entities owning an airport include—
(i) a company which owns the airport ("C");
(ii) any parent undertaking of C ("P1"); and
(iii) any parent undertaking of P1 ("P2");

"operating an airport" means having overall responsibility for its management; and

"parent undertaking" has the same meaning as set out in section 1162 of the Companies Act 2006.

Question 1: Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?

Maritime

453. Many respondents sought to understand the intention for including the 12 passengers wording in the consultation definition as it was unclear what it was designed to capture and seemed to broaden the scope of definition.

454. One respondent sought clarity on whether we aim to capture only those companies that own and operate assets within a port or harbour. Another respondent requested clarification on ownership and another on 'relevant year'.

Airports

455. Respondents sought clarity on the definition of an airport and of a 'holding' and 'parent company'. There was a concern that some activities or operations at airports such as ground handling, which do not involve overall control of the airport, might be inadvertently caught by the definition. There was also some confusion around the reference to the relevant year. One respondent also asked if we could align the thresholds with those listed in the Network and Information Systems (NIS) directive.

456. One respondent noted there was uncertainty as to whether other air navigation service providers (other than the sole licence holder under section 6 of the Transport Act 2000) were caught by the definition and whether there was a need to specifically exclude service providers which deliver communication, navigation and surveillance (CNS) services at airports. It was also suggested to include 'in the UK' after 'en route air traffic control services' in the definition of 'en route service provider'.

Government response

Maritime

457. We have removed references to '12 passengers' to ensure this legislation is properly aligned with national security interests and in response to industry feedback. We have also removed the inclusion of the Category 1 goods wording to narrow the scope of the definition further. Acquisitions within smaller ports will now be considered using the call-in power where appropriate.

458. We reviewed the use of owns and operates when referring to infrastructure with a port or harbour. We intend the wording to capture only those companies that own and operate terminals, wharves or other port related infrastructure, not those that have parent companies across various sites.

459. We have also provided further detail on 'operates' to clarify we intend this to mean controlling the functioning of the port, harbour, terminal, wharf, or other infrastructure. We have also defined the time period for which we set cargo thresholds under the Port Freight Annual Statistics.

Airports

460. We can confirm that the definition outlines that the operator of an airport is the entity with overall responsibility for its management. This excludes ground handling operations and other operations which carry out some activities at airports but do not have overall control or management of them.

461. We have revised the definition to refer to 'parent undertaking' rather than 'holding company'. This term is used in section 1162 of the Companies Act. It covers a slightly wider range of company interrelationships. For example, an undertaking is a parent undertaking in relation to another entity if it has the right to exercise a dominant influence over it by provisions contained in the company's articles.

462. As the consultation paper noted, initially the definition will work by reference to the published figures for 2018 because of the reduced demand due to the Covid pandemic in 2020, but it will be possible to make further regulations to change this to a later year once demand recovers. Therefore, we have updated the drafting to reflect this.

463. The Government does not agree that the thresholds need to be the same for this definition and the NIS Regulations. Both regulations address separate aspects of national security as NIS Regulations are only concerned with network and system security.

Question 2: To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

Maritime

464. Respondents sought clarity around some of the terms used such as ‘operates’, ‘relevant year’ and ‘port’.

Government response

465. We have specified that relevant ports are those that are within the UK and further defined the terms raised by respondents which required further clarity. We have defined a port as ‘an area of land and water made up of such infrastructure, facilities and equipment so as to permit, principally, receiving and departing of vessels, their loading and unloading, the storage of goods, the receipt and delivery of those goods and the embarkation and disembarkation of passengers, crew and other persons’. This avoids doubt as to the nature of ports we intend to capture.

466. We have also defined ‘infrastructure’ as part of this definition to clarify that it only applies to infrastructure, facilities and equipment within a port or harbour which enable effective operations directly related to the movement of freight, passengers or seafarers.

Question 3: To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

467. Respondents expressed some concern regarding the scope of the maritime definition as it captures all 51 major ports.

Government response

468. The Government remains committed to capturing all 51 major ports. This is due to the ability of these ports to handle a variety of goods. The scope therefore remains expansive to reflect the flexibility of usage and choice within this sector. We would not wish to list ‘key’ ports, as it would be simple to circumnavigate this requirement.

Question 4: How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?

469. Whilst there was no specific response to this question, we have taken steps to reduce the breadth of the definition, reducing the burden on those small ports potentially captured by the Category 1 and 12 passengers wording.

Question 5: Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

470. A respondent suggested the ‘1 million tonnes of cargo’ threshold was too low and would capture too many ports.

Government response

471. We have retained the threshold of 1 million tonnes of cargo as this is used by Department for Transport's Port Statistics to determine a major port, and therefore is the correct threshold for this legislation. We would like to capture transactions associated with major ports.

Conclusion

472. The transport sector is essential to keeping the country moving, and many essential services rely on it to function.

473. Only certain entities in the transport sector are sensitive enough to be subject to mandatory notification, and so we do not seek to include all transport related entities. Instead, the revised definition in this response focuses on areas that have the highest potential to give rise to national security risks from certain types of investment, and do not currently have sufficient alternative controls in place.

474. The transport sector definition, where possible, broadly seeks to avoid duplication where Government notification is already a requirement or unavoidable – although in some cases, however, the Bill's provisions will supplement what exists in the current regulatory regime, recognising the value of increased intervention powers in limited areas.

475. Emerging technology within the transport sector, such as AI or autonomous vehicles, is captured under other sector definitions and so is not included here.

476. As a result of the consultation phase, we have made some changes. The majority do not have any material impact on the definition, with the exception of the 12 passengers and Category 1 wording. These changes draw clearer boundaries as to the parts of the two chosen sectors where we feel it is important to understand ownership and influence to ensure national security is protected.

Annex A: Draft revised definition for Advanced Materials

Advanced materials

Advanced materials

1. A qualifying entity whose activities consist of or include the activities set out in paragraph 2 in relation to the matters described in paragraph 4 or the sectors set out in paragraph 5.

2. The activities referred to in paragraph (1) are—

(a) research into;

(b) developing or producing;

(c) developing or producing anything designed as an enabler for use in;

(d) developing or producing anything designed to be used to make;

(e) providing qualified or certified designs, materials, parts or products for use in;

(f) owning, creating, supplying or exploiting intellectual property relating to ;

(g) providing know-how or services of enablers; and

(h) recycling or re-using.

3. In this Part—

"advanced composites" relates to structural composite materials with either metallic or ceramic matrices and includes 3D reinforcing architectures for any matrix (polymer, metal or ceramic);

"advanced materials" means materials that provide targeted properties and include both completely new materials and those that are developments on traditional materials, such materials show advantageous and either or both outstanding structural or functional properties;

"enabler" means any material or process which is not a material described in paragraphs 4 or 5 but is used in the manufacture or application of such materials;

"graphene and related 2D" are those with attributes as defined within ISO TS 80004-13:2017;

"metamaterial" means a composite material in which the constituents are designed and spatially arranged through a rational design-led approach to change the manner in which electromagnetic, acoustic or vibrational energy interacts with the material, in order to achieve a property or performance that is not possible naturally and includes a metasurface and for this purpose "composite material" means a solid material formed from two or more constituents and "constituent" includes a region containing a vacuum, gas or liquid. (Types of composite materials that are not metamaterials are the advanced composites described in paragraph 5 and composites or coatings containing pigments or fillers that are mixed in or blended into a binder material where both of these types of composite materials can be a constituent from which a metamaterial may be formed.);

"metasurface" means a two-dimensional form of metamaterial which includes one or more layers of material that are intentionally patterned or textured (irrespective of whether they are periodic or not) through a rational design-led approach;

"nanotechnology" means the manipulation and control of matter predominantly in the nanoscale to make use of size-and-structure-dependent properties and phenomena distinct from those associated with individual atoms or molecules, or extrapolation from larger sizes of the same material (where "manipulation and control" includes material synthesis in relation to nanotechnology) with current or potential utility for defence, including nanomaterials, nanodevices, nanocomponents and nanosystems (including nanomachines) in accordance with ISO/TS 80004-1:2015.

'nanomaterials' means materials with any external dimension in the nanoscale or having internal structure or surface structure in the nanoscale and include nano-objects, dispersions or mixtures containing nano-objects, and nanostructured material (including structuring at an interface between materials, including air, and within a material) in accordance with ISO/TS 80004-1:2015;

"photonic and optoelectronic materials and devices" relate to high power lasers that are characterised by a combination of power at the output apertures (values of 1 kilowatt (kW) and above), beam quality (M^2 of less than 1.2), intended operating ranges (greater than 1 kilometre (km)) and at wavelengths

compatible with propagation over those distances (typically 1 micrometre (µm) to 2 micrometres (µm) wavelengths);

"semiconductor" relates to—

(i) semiconductors used to form radio frequency (RF) and microwave devices;

(ii) semiconductors used to realise imaging sensor arrays;

(iii) the accessibility of design and production for semiconductor devices and chips where 'chips' include Field Programmable Gate Array (FPGA) devices, System on Chip, Application Specific Integrated Circuits (ASIC) and Readout Integrated Circuits (ROIC) and where "devices" includes radio and microwave frequency control circuitry, power amplifiers, low noise amplifiers and monolithic microwave integrated circuits and detectors;

"technical textiles" relates to textiles (and their processes and enablers) specifically developed for their functional performance including additional functionality (such as integrated computing, processing or data transmission), 3-D architectures, protection against blast and ballistic events but does not include sportswear or clothing that is ordinarily available to consumers or household goods;

4. The matters referred to in paragraph 2 are materials, the export or transfer of which is controlled by virtue of their being specified in:

(a) Schedule 2 to the Export Control Order 2008(**1**); and

(b) Annex I and Annex IV to Council Regulation (EC) No 428/2009(**2**).

Sectors

5. The sectors and matters within each sector are—

(1) *Advanced composites*

(a) *Systems, equipment and components*

none

(b) *Test, inspection and production equipment*

(i) production technologies and capabilities for the manufacture of metal matrix composites;

(ii) production technologies and capabilities for the manufacture of ceramic matrix composites.

(iii) manufacture of 3-D fibre architectures (that is with interlaminar reinforcement) for all composite types.

(c) *Materials*

(i) metal matrix composites: powder-based metal matrix composites and continuous fibre reinforced metal matrix composites;

(ii) fibre reinforced ceramic matrix composites;

(iii) continuous silicon carbide fibres with diameters at and below 140 micrometres (µm);

(iv) continuous oxide-based ceramic fibres with diameters at and below 20 micrometres (µm);

(v) coatings for the protection of ceramic matrix composites from degradation in the environment, for example ytterbium mono- and di-silicates.

(d) *Software and data*

(i) capabilities for the design and design for manufacturing of metal matrix composites and fibre reinforced ceramic matrix composites.

(**1**) S.I. 2008/3231. Schedule 2 was substituted by S.I. 2017/85 and subsequently amended by S.I. 2017/697, S.I. 2018/165, S.I. 2018/939 and S.I. 2019/989. CHECK

(**2**) OJ No L 134.5.2009, p.1, as amended by Commission Delegated Regulation (EU) 2017/2268 (OJ No L 334, 15.12.2017, p.1), Commission Delegated Regulation (EU) 2018/1922 (OJ No L 319, 14.12.2018, p.1) and Commission Delegated Regulation (EU) 2019/2199 (OJ No L 338, 30.12.2019, p.1).CHECK

(ii) Software and computer-aided design for 3-D fibre architectures and 3D preforms (i.e. with interlaminar reinforcement) for all composite types.

(e) *Technology*

none

(2) Metals and alloys

(a) *Systems, equipment and components*

(i) magnets utilising rare earth element-lean or element- free permanent magnetic materials with remanent magnetism, $B_{r,}$ greater than 1.0 Tesla (T) and all rare-earth magnetic materials;

(b) *Test, inspection and production equipment*

(i) any processes that are involved in the reduction of either pure or mixed oxides in the solid state into either metals or alloys in or into crude or semi-fabricated forms, including powders, in batches of at least 1 kilogram (kg);

(ii) hot isostatic pressing (HIP);

(iii) spark plasma sintering (SPS) / field assisted sintering technology (FAST);

(iv) diffusion and friction-based joining processes for steel for power transmission shafts described in paragraph (c)(v), titanium alloys, nickel alloys or cobalt alloys;

(v) friction-based processes to join metallic material layer by layer to create a structure;

(vi) superplastic forming of titanium and aluminium alloys;

(vii) electron beam, laser and weld arc-based metal additive manufacturing capabilities;

(c) Materials

(i) any alloys that are formed by chemical or electrochemical reduction of feedstocks in the solid state directly from their oxides;

(ii) titanium alloys with continuous temperature-of-use capabilities above 350°C;

(iii) powder metallurgy alloys;

(iv) nickel and cobalt based superalloys with continuous temperature-of-use capabilities above 700°C;

(v) steels for power transmission shafts with yield strengths of at least 1030 megapascals (MPa) at 20°C and 760 MPa at 450°C, ultimate tensile strengths of at least 1240 MPa at 20°C and 950 MPa at 450°C and fracture toughnesses of at least 40 MPa square root metres ($MPa.m^{½}$) at 20°C;

(vi) high strength high toughness weldable marine grade steels (toughness levels D, E and F);

(vii) armour grade steels;

(viii) armour grade aluminium alloys;

(ix) high entropy alloys and compositionally complex alloys (alloys that are formed by five or more elements where the composition is not dominated by one or two elements);

(x) rare earth element-lean or element-free permanent magnetic materials with remanent magnetisation, B_r, greater than 1.0 Tesla (T), and all rare-earth magnetic materials;

(xi) magnetically materials with high total saturation flux densities greater than 2.0 Tesla (T), which may include monolithic and laminate forms, and particulate and fibre reinforced composite materials.

(d) Software and data

(i) computer models of complex metallic components, formed by powder-based additive manufacture, that embody a fluid and heat transfer function within their structure;

(ii) data on the performance of complex metallic components, formed by powder-based additive manufacture, that embody a fluid and heat transfer function within their structure.

(e) *Technology*

none

(3) Engineering and technical polymers

(a) Systems, equipment and components

none

(b) Test, inspection and production equipment

(i) machines for additively manufacturing the materials listed in sub-paragraph (c), including loaded polymer filaments to enable electrically insulating and electrically conducting, thermally conducting and insulating, or magnetic and non-magnetic materials (or further combination thereof).

(c) Materials

(i) engineering polymer materials and formulations with a glass transition temperature (T_g) >190°C;

(ii) polymers responsive to external stimuli such as electromagnetic, load, chemical and biological stimuli (for example electroactive polymers, thermoactive polymers self-healing systems) but not hydrogels in applications such as nappies.

(iii) high temperature, high pressure and chemically resistant elastomeric seals and systems;

(iv) polymer electrical insulation materials with high temperature (greater than 200°C) and high voltage (above 1kilovolt (kV)) capabilities for application in aviation electrical power management systems;

(v) filaments and feedstocks for additive manufacturing or 3-D printing with bespoke and elevated electrical, magnetic, or electromagnetic properties (typically formed from filled polymer compositions);

(vi) adhesives capable of retaining performance at high temperatures (above 190°C);

(vii) adhesives with underwater curing capabilities;

(viii) void-filling viscoeleastic polymers, created using at least a thermoplastic polyester and curing agent, intended for use to damp vibrations in metallic structures.

(d) Software and data

none

(e) Technology

none

(4) Engineering and technical ceramics

(a) Systems, equipment and components

none

(b) Test, inspection and production equipment

(i) spark plasma sintering (SPS) or field assisted sintering technology (FAST);

(c) Materials

(i) boron carbide and silicon carbide ceramics for the manufacture of hard armour plates;

(ii) ultra-high temperature ceramics (with melting temperatures of at least 3000 °C) including transition metal diborides, either as monolithic or composite forms, including other ceramic monoliths or composites where ultra-high temperature ceramics have been added to their bulk or into surfaces;

(iii) magnetic materials, including fibres and particulates, for electromagnetic applications at frequencies above 500 megahertz (MHz);

(iv) functional ceramics (including ferroelectrics, magneto-dielectrics, or multi-ferroics) for acoustic applications, or electromagnetic applications above 100 megahertz (MHz);

(v) dielectric and ferroelectric materials for use in the generation of, and manipulation of, high energy or high power radio frequency (RF) radiation, including functioning under high voltage conditions.

(d) Software and data

none

(e) Technology

none

(5) Technical textiles

(a) Systems, equipment and components

(i) textile materials and products manufactured primarily for technical performance and functional properties rather than aesthetic or decorative characteristics but not sportswear or clothing ordinarily available to consumers or household goods;

(b) Test, inspection and production equipment

(i) knitting, weaving, nonwoven or hybrid manufacturing processes related to sub-paragraph (a)(i);

(ii) fibre manufacturing processes related to sub-paragraph (a)(i);

(iii) yarn manufacturing and texturing, dry fabric coating and laminating;

(iv) manufacture of 3-D textiles;

(v) closed loop recycling processes associated with sub-paragraph (a)(i).

(c) Materials

(i) smart fabrics with fibres or yarns equipped with embedded sensors that respond to stimuli and perform a specific function;

(ii) fabrics made of smart polymers and textiles to protect and prevent injury or damage from blast and ballistic events;

(iii) energy harvesting fabrics;

(iv) textiles or fibres incorporating activated carbon;

(v) fabrics with embedded devices for data storage and communication.

(d) Software and data

(i) software and computer-aided design for 3-D textiles and preforms;

(ii) machine learning software systems for smart textile manufacturing facilities, or for data-driven design and manufacturing of textile materials and systems;

(e) Technology

(i) textile-based wearable electronics with potential to enable subtle integration of electronics with the human body for human-machine interfacing;

(ii) integration technologies to enable functionalities such as energy harvesting, data storage and communication, camouflage, structural and personnel health monitoring and protection.

(6) Metamaterials

(a) *Systems, equipment and components*

(i) metamaterials used in-

(aa) electromagnetic components (including antennas, arrays, lens, devices);

(ba) electromagnetic applications including radio frequencies (RF) and microwave through to ultraviolet wavelengths

(ca) nano-photonics or quantum technology as an enabler

(da) thermal control or protection;

(ea) airborne or underwater acoustics; or

(fa) structural applications.

(b) *Test, inspection and production equipment*

(i) test, inspection and production equipment associated with the fabrication of 2-dimensional and 3-dimensional arrangements of one or more material and/or device constituents to form a metamaterial (including but not limited to additive manufacturing, printed electronics methods, nano-fabrication, chemical self-assembly or engineering biology);

(ii) equipment associated with the non-destructive test and assurance of assembled or produced metamaterial including—

(aa) composition;

(bb) spatially varying composition;

(cc) spatial arrangement parameters.

(c) *Materials*

(i) a metamaterial

(ii) tailored or bespoke feedstocks used in fabricating metamaterials (including blended or formulated filaments (referred to in paragraph 3(c)(v)), inks or dispersions used for additive manufacturing or printing) but excluding inks or dispersions commercialised for forming electrically conducting pathways ("wires") in printed electronics.

(d) *Software and data*

(i) Accumulations of metamaterial designs, or of elements comprising metamaterials, any of which that enable artificial intelligence, machine learning design or optimisation of metamaterials.

(e) *Technology*

(i) The inclusion with a metamaterial of technology in the form of systems or components, as well as material constituents, as part of the means and methods that enable metamaterials to alter their function and behaviour once installed or produced.

(7) *Semiconductors*

(a) *Systems, equipment and components*

(i) high performance thermal imaging systems, equipment and components providing system sensitivity less than 30 milli-Kelvin (mK) for large format systems with more than 1megapixels (Mpixels);

(ii) integrated systems having multiple operating wavebands on a single camera including mid-wavelength and long-wavelength infrared;

(iii) imaging systems with on-chip (smart) processing;

(iv) research, development and production of type II superlattice detectors;

(v) research, development and production of single photon counting detector arrays operating at wavelengths longer than the visible band (wavelength greater than 750 nanometres (nm)), and with a size of at least 32x32 elements, or linear arrays with a size of at least 1x256 elements;

(vi) research, development and production of low noise CMOS (complementary metal-oxide-semiconductor) and EMCCD (electron multiplying charge coupled device) cameras where low noise would be less than 1 photoelectron/pixel/second;

(vii) research, development and production of technology and components for non-Von Neumann computing architectures, including but not limited to neuromorphic computing systems.

(b) Test, inspection and production equipment

(i) the production of radio and microwave frequency systems, equipment and components incorporating compound semiconductors; example components include but are not limited to control circuitry, power amplifiers, low noise amplifiers and monolithic microwave integrated circuits and detectors;

(ii) facilities operating as a compound semiconductor foundry or providing compound semiconductor processing capability;

(iii) chip and device fabrication;

(iv) ceramic and polymeric packaging of processed semiconductor chips;

(v) the production and integration capabilities for the high-performance imaging systems described in sub-paragraph (7)(a)(i) to (vii).

(c) Materials

(i) all compound semiconductors for radio frequency (RF) and microwave application including gallium nitride (GaN), gallium arsenide (GaAs), gallium oxide (GaO), silicon germanium (SiGe) and indium phosphide (InP);

(ii) imaging camera detector materials including cadmium mercury telluride (CMT), aluminium gallium arsenide (AlGaAs), indium gallium arsenide (InGaAs) and germanium silicon (GeS).

(d) Software and data

(i) Chip and Device design.

(e) Technology

none

(8) Photonic and Optoelectronic materials and devices

(a) Systems, equipment and components

(i) polarisation control components including materials (solid and liquid) especially for high power applications (>100 watts (W));

(ii) optical fibre designs mitigating nonlinear effects and enabling polarisation control of the output light for high power applications in both transverse single-mode and multimode optical fibre formats;

(iii) optical Fibre based components such as light diodes, tap couplers and fibre Bragg gratings;

(iv) nonlinear components for nonlinear frequency conversion such as optical fibre geometries, crystal materials and optical patterning techniques;

(v) low loss, high bandwidth optical fibre technologies and manufacturing techniques for telecommunications applications;

(vi) phase modulators, where the spectral linewidth of fibre laser amplifiers is limited to no more than 16 gigahertz (GHz).

(b) Test, inspection and production equipment

(i) optical fibre designs and production techniques, including coating techniques and test methodologies;

(ii) laser materials manufacturing techniques, host material doping techniques and characterisation techniques;

(c) Materials

(i) materials that enable increased amplification, improved quality, improved robustness, improved increased electro-optical efficiency or reduced size or volume;

(ii) materials and or coatings or treatments that reduce optical losses of lenses or mirrors;

(iii) materials and or coatings or treatments that improve increase the physical stability or robustness of lenses or mirrors;

(iv) materials enabling non-mechanical beam steering for detectors, sensors and imaging systems;

(v) materials that reduce the size, weight and power requirements of optical detection, sensing and imaging systems;

(vi) materials suitable for aberration correction of high-power lasers (>1 kilowatt (kW)) in the atmosphere.

(d) Software and data

(i) algorithms, and their implementation in firmware, that compensate for the adverse atmospheric effects on laser beam propagation at distances >1 kilometre (km);

(ii) software, hardware and algorithm developments that improve phase control/coherent beam combination and efficiency;

(e) Technology

(i) any approaches that enable high average optical power (>3 kilowatts (kW)) combined with high quality (M^2 <1.2) amplifiers;

(ii) any aspects that enable the propagation of light over significant distances (>1 kilometre (km)), including aberration correction devices.

(9) Graphene and related two-dimensional materials

(a) Systems, equipment and components

(i) Developing and operating equipment to synthesise single to few layer graphene and related 2D materials, including—

(aa) controlling the desired structure of the materials or their properties for application;

(bb) using processes including chemical exfoliation, electrochemical exfoliation, atom or molecule intercalation, surface growth, solution phase growth, vapour deposition and large area chemical vapour deposition;

(b) Test, inspection and production equipment

(i) synthesis and manufacturing routes to—

(aa) graphene and related 2D; or

(bb) graphene and related 2D materials (or combination thereof) with bespokely tailored or optimised functional properties, including but not limited to functioning as semi-conductors**;**

(ii) research, development and production of materials at scale for use as a filler or pigment including forming or using graphene and related two-dimensional materials in dispersions or mixed with other binders;

(iii) research, development and production to integrate the use of materials in devices and systems;

(iv) conversion of graphene and other 2D materials into intermediaries using processes including to surface treatment and functionalisation, dispersion in matrices, mechanical and laser shaping, coating and ink printing processes;

(c) Materials

(i) all graphene and related 2D materials, including—

(aa) graphene, hexagonal boron nitride and transition metal dichalcogenides (such as MoS_2 and WS_2);

(bb) graphene and related 2D materials as thin films or coatings, powder form or mixtures with other materials; or

(cc) energetic materials (such as propellants or explosives);

(d) Software and data

none

(e) Technology

(i) stacking of different 2D crystals resulting in either or both a charge redistribution between neighbouring crystals or causing structural changes;

(ii) components with finely tuned properties made by combining different 2D materials, including but not limited to stacking different two-dimensional materials;

(10) Nanotechnology

(a) Systems, equipment and components

(i) sensors or detectors including quantum dots with very high sensitivity to—

(aa) chemical, biological or nuclear materials (where the threshold is close to and including single molecule levels); or

(bb) light or other forms of radiation (where the threshold is close to and including single photon levels);

(ii) autonomous remote or remotely activated sensing and reporting systems that are enabled by nanotechnology including Smart Dust;

(iii) nanomachines or nanoscale robots either with physically moving parts or capable of physical movement;

(b) Test, inspection and production equipment

(i) test, inspection or production of nanotechnology or nanomaterials but not including services only offering test and inspection requiring the prior destruction of the produced nanotechnology or nanomaterials to form a test artefact (such as using Scanning Electron Microscopy or Atomic Force Microscopy).

(ii) methods to create or integrate nanotechnology for use in—

(aa) computer processing or memory devices (excluding commoditised silicon microelectronics technologies);

(ba) communications or electronic warfare devices or components;

(ca) precision navigation and timing systems;

(da) detectors, sensing or imaging systems;

(ea) counter-measure devices, systems;

(fa) moving parts or soft robotics;

(c) Materials

(i) high-density nanoceramics and carbon nanotubes to reinforce ceramics for ballistic and blast protection;

(d) Software and data

none

(c) Technology

(i) technology that exploits nanoscale phenomena or technology that is nano-enhanced or nanoscience that further enhances nanoscale phenomena;
(ii) materials possessing exploitable magnetic, quantum or atomic spin states, or in combination for spinwave effects or technologies (including defect centres in nanomaterials or utilising skyrmions;
(iii) electro-optic, magneto-optic, photonic or nanophotonic effects or devices (including vertical cavity emitting lasers) and circuits;
(iv) micromechanical, nanomechanical, electromechanical, optomechanical, or electro-opto-mechanical effects or systems;
(v) metamaterials or metasurfaces;

(11) Critical materials

(a) Systems, equipment and components

none

(b) Test, inspection and production equipment

none

(c) Materials

The extraction, refinement, processing, production and end of life recovery (in single element, compound or product form) of—

(i) activated carbon;
(ii) antimony;
(iii) arsenic;
(iv) beryllium;
(v) bismuth;
(vi) boron;
(vii) cadmium;
(viii) cerium;
(ix) chromium;
(x) cobalt;
(xi) dysprosium;
(xii) erbium;
(xiii) europium;
(xiv) fluorspar;
(xv) gadolinium;
(xvi) gallium;
(xvii) germanium;
(xviii) graphite;
(xix) holmium;
(xx) indium;
(xxi) iridium;
(xxii) lead;
(xxiii) lithium;
(xxiv) lutetium;
(xxv) mercury;
(xxvi) molybdenum;
(xxvii) neodymium;
(xxviii) niobium;
(xxix) osmium;
(xxx) palladium;
(xxxi) platinum;
(xxxii) praseodymium;
(xxxiii) rhenium;
(xxxiv) ruthenium;

(xxxv) samarium;
(xxxvi) scandium;
(xxxvii) selenium;
(xxxviii) tantalum;
(xxxix) tellurium;
(xl) terbium;
(xli) thulium;
(xlii) tungsten;
(xliii) vanadium;
(xliv) ytterbium;
(xlv) yttrium.

(12) Other materials

(a) Systems, equipment and components

(i) capacitors based on tantalum;

(b) Test, inspection and production equipment

(i) machines for additively manufacturing fully-assembled robotic, soft-robotic, sub-systems and systems or autonomous robotic sub-systems, systems and vehicles but not including machines for additively manufacturing individual components for such sub-systems systems and vehicles;
(ii) circuit board manufacturing of pitch, track or gap dimensions less than 30 micrometres;
(iii) new component placement technologies, including multi-axis component placement;
(iv) additive manufacturing or printing of moving parts, components and machines (known as '4D printing');
(v) battery pack assembly specifically for defence and security applications (at the stage of integration, not isolated battery cell construction);

(b) Materials

(i) any materials (including paints or other forms of coating or surface) that are capable of modifying (including in real time) the appearance, detectability, traceability or identification of any object to a human or to sensors within the range of 15 terahertz (THz) up to and including ultraviolet;
(ii) foams with designed electrical, electromagnetic or thermal protection properties;
(iii) honeycombs with designed electrical or electromagnetic properties;
(iv) smart materials (including micro-fluidic systems) whose properties can be repeatably altered once installed at rates exceeding 1 megahertz (MHz);
(v) materials enabling extreme size, weight and power reduction for energy, power and propulsion sources, or sensing or communications devices and systems for use in micro or smaller unmanned systems;

(c) Software and data

(i) creative artificial intelligence algorithms for material discovery and optimisation;
(ii) quantum simulation for material discovery and optimisation.

(d) Technology

(i) neuromorphic or quantum technologies enabling creative artificial intelligence or quantum simulation for materials discovery.

This publication is available from: www.gov.uk/beis

If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.