Department for
Business, Energy
& Industrial Strategy

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

Consultation on secondary legislation to define the sectors subject to mandatory notification in the National Security and Investment Bill 2020

Closing date: 6 January 2021

November 2020

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

Contents

General information

Why we are consulting

The Government has introduced legislation to update its powers to scrutinise and intervene in acquisitions of control of entities and assets to protect national security. The new powers will mandate notification for certain transactions in a list of sectors. This means that the Government is automatically informed of potential transactions in these crucial areas, and able to take action accordingly to investigate and mitigate any national security risks. This approach brings us in line with many of our allies including the USA, France and Germany. Responses to this consultation will inform and refine the sectors of the economy that will be subject to mandatory notification under that regime.

The National Security and Investment Bill introduced to Parliament on 11 November 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 updated powers needed to comprehensively scrutinise and, if necessary, intervene in certain types of transactions across the economy if they give rise to national security concerns.

Mandatory notification of certain types of transactions in 17 key sectors will ensure that the Government is informed of potential acquisitions of control or ownership in these particularly sensitive areas, and can take action accordingly to investigate and mitigate any national security risks. The sectors are:

1. Advanced Materials
2. Advanced Robotics
3. Artificial Intelligence
4. Civil Nuclear
5. Communications
6. Computing Hardware
7. Critical Suppliers to Government
8. Critical Suppliers to the Emergency Services
9. Cryptographic Authentication
10. Data Infrastructure
11. Defence
12. Energy
13. Engineering Biology
14. Military and Dual Use
15. Quantum Technologies
16. Satellite and Space Technologies
17. Transport

The vast majority of the transactions will not be called in, and this process can therefore provide more certainty and confidence for businesses and investors that the Government will not intervene in their investment.

This consultation document sets out the Government's proposed definitions for the types of entity within each sector that could come under the Bill's mandatory regime. Responses to this consultation will be used to refine the definitions so they provide enough clarity to allow parties to self-assess whether they need to notify. The final definitions will be put into secondary legislation, which the Government intends to introduce in time for commencement of the Bill in 2021. For many sectors, this represents a starting point with respect to the definition and our proposals should not be seen as definitive. We therefore expect some definitions to change following this consultation.

The National Security and Investment Bill is currently before Parliament and all aspects of the regime are subject to Parliamentary approval.

Consultation details

Issued: 11 November 2020

Respond by: 6 January 2021

Enquiries to: nsisectorconsultation@beis.gov.uk

Respond online at: https://beisgovuk.citizenspace.com/ccp/nsi-mandatory-notification-sectors

or

Email to: nsisectorconsultation@beis.gov.uk

Consultation reference: National Security and Investment: sectors in scope of the mandatory regime

Audiences:

We are seeking views from entities operating in the sectors specified in this consultation, from sectoral experts from the private sector and academia, and from investors and their legal advisers.

Territorial extent:

The proposed reforms will extend to the whole of the UK. National security is a reserved matter in Scotland and Wales and an excepted matter in Northern Ireland.

For general enquires about the Bill interested parties should email nsiireview@beis.gov.uk

How to respond

Respond online at: https://beisgovuk.citizenspace.com/ccp/nsi-mandatory-notification-sectors

or

Email to: nsisectorconsultation@beis.gov.uk

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: beis.bru@beis.gov.uk.

Executive summary

The UK economy thrives from Foreign Direct Investment, and 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, such as new investment from overseas investors in UK businesses, expansions of existing investments by overseas investors, or mergers and acquisitions involving foreign acquirers. In the past 10 years, $750 billion has flowed into the UK as a result of Foreign Direct Investment. However, an open approach to Foreign Direct Investment must include appropriate safeguards to protect our national security against the small minority of investments that could do it harm. Through the National Security and Investment (NSI) Bill, published 11 November, the Government is updating its powers to screen investments and mitigate any security risks they may present, bringing them in line with our Five Eyes allies.

The Bill makes provision for a mandatory notification and pre-approval requirement for the most sensitive parts of a number of sectors of the economy, backed up by a voluntary notification option for the rest of the economy and a call in power for transactions that have not been notified. The scope of this requirement, referred to as the ‘mandatory regime’, will be set out in secondary legislation before commencement of the NSI powers.

We are consulting on drafts of the definitions that set out which areas of the economy require notification and pre-approval. The rationale for the sectors which fall within the mandatory regime and the proposed definitions of those sectors are set out in this consultation document. The proposed sectors cover a mixture of traditional Critical National Infrastructure and advanced technology. The Government is aware that there is a great wealth of expertise outside of Government on these areas and welcomes the opportunity to refine these definitions with experts over the course of this consultation.

The proposed definitions in this consultation follow the guiding principles that have underpinned our policy development from the outset – including certainty, transparency and predictability of the regime to businesses and investors and ensuring that the UK is the best place to invest in a business.

Introduction

Background

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. Of course, an open approach to international investment must include appropriate safeguards to protect our national security and the safety of our citizens. 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 transactions on national security grounds are required. The Government welcomes Foreign Direct Investment and is clear that the UK is open for business.

We have seen that at times investors have found novel means to try to obfuscate our current regime; for example by structuring a deal in such a way that it is difficult to identify the ultimate owner of the investment by funnelling investment through a UK or ally investment fund or by buying or licencing certain intellectual property, rather than investing in or acquiring the whole company directly. This is why the Government has taken a careful and considered approach to updating its investment screening powers.

The Government first announced its intention to update the investment screening powers in 2016 and consulted via a Green and White Paper. While the proposals put forward in the 2018 White Paper would achieve longer-term reforms, they do not go far enough in addressing the national security risks arising from a small number of transactions in particularly sensitive sectors, nor reflect the full gravity of the current situation. In particular, they do not do enough to prevent the few determined hostile actors from evading scrutiny and acquiring critical businesses or assets under the radar.

The Government introduced the National Security and Investment Bill on 11 November. The Bill makes provision for a mandatory notification requirement for key sectors of the economy, backed up by a voluntary notification option for other sectors in the economy and a call-in power.

The regime is in line with many of those administered by our Five Eyes allies (USA, Canada, Australia, New Zealand), so investors will be familiar with the notification requirements. Other regimes around the world, including the United States, France, Italy and Japan also have certain notification requirements for certain sectors.

The Government has already made some changes to the existing regime under the Enterprise Act 2002 in July 2020 which will apply until the National Security and Investment Bill is commenced, providing for a lower threshold for intervention in three sensitive sectors of the economy: artificial intelligence, cryptographic authentication technology and advanced materials. The Government made similar changes in 2018 in relation to three other sectors: military/dual-use technologies, quantum technology, and computing hardware.

The definitions set out in the following chapters further develop those definitions and so differ from those in the 2018 and 2020 Enterprise Act amendments. The 2018 and 2020 amendments were only ever intended as short-term measures before more comprehensive reforms were brought forward via primary legislation.

The Government is now consulting on the content and definitions of the sectors which will fall in scope of the mandatory regime.

The proposed definitions in this consultation follow the guiding principles that have underpinned our policy development from the outset – including certainty, transparency and predictability of the regime to businesses and investors and ensuring that the UK is a good place to invest in a business.

The definitions for the sectors contained in this consultation are draft. The consultation process will draw on feedback from respondents in order to inform the ultimate definitions and policy decisions that the Government will bring forward into secondary legislation.

This consultation document should be read in conjunction with the National Security and Investment Bill as presented to Parliament, its explanatory notes, and the White Paper Response published on 11 November – see GOV.UK National Security and Investment Bill.

Mandatory notification in specific sectors

Definitions of key sectors subject to mandatory notification

The sector definitions have been drafted to give clarity to business about which legal entities are subject to the requirement to notify the Secretary of State about relevant notifiable acquisitions.

The Government is keen to hear views from all relevant parties as to whether the definitions provide sufficiently clear parameters to inform businesses of the need to notify, and whether they are proportionate in scope.

Mandatory notification of notifiable acquisitions

The National Security and Investment legislation will introduce mandatory notification of some transactions in specified sectors where risks are most likely to arise, referred to here as the ‘mandatory regime’.

This means that the Government will be informed of proposed acquisition of control or ownership in these crucial areas, and able to take action accordingly to investigate and address any national security risks.

Acquisitions covered by mandatory notification must be notified and receive approval from the Secretary of State before they can take place. These acquisitions are known as ‘notifiable acquisitions’ for the purposes of the Bill.

For the first time investors and business will be able to seek clearance on national security grounds from the Government on their transaction in a statutory timeline set out in law. More information about the functioning of the regime is available in the Bill as presented to Parliament, its explanatory notes, and the White Paper Response published on 11 November.

Consultation questions

Questions applying to all sectors

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?**

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

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?**

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?**

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?**

Questions applying to specific sectors

Please note that not all sectors have sector-specific questions.

Advanced Robotics

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?**

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?**

Artificial Intelligence

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?**

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

Communications

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?

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

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

Computing Hardware

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?

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?

Critical Suppliers to Government

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?

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

Critical Suppliers to the Emergency Services

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?

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

Data Infrastructure

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? In your response, we are particularly interested in

whether we have accurately covered the various operating and ownership models within the data infrastructure sector; the provision of technical services to relevant data infrastructure; and the provision of virtualised services to relevant data infrastructure.

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 within your facility? To what extent are these provided by in-house staff or outsourced and how is security of data ensured?

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?

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 are 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?

Proposed sector definitions

Advanced Materials

Proposed definition

1. An entity whose activities consist of or include –
    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, or
    g. providing know-how or services of enablers, where “enabler” means any material or process which is not an advanced material but is used in the manufacture of an advanced material

for use in the sub-sectors set out in paragraph (2), where the entity is carrying out the functions set out in paragraph (3).

2. The sub-sectors are:
    a. Advanced composites;
    b. Novel or complex metal alloys;
    c. Engineering and technical polymers and ceramics;
    d. Technical textiles;
    e. Metamaterials;
    f. Semiconductors;
    g. Photonic and optoelectronic materials;
    h. Graphene and other two-dimensional (2D) materials;
    i. Nanotechnology;
    j. Critical materials, niche materials and materials related products.
3. The functions described in subparagraphs (2.a) to (2.j) are:

a. Advanced Composites

    i. Test, inspection and production equipment

        1. Production technologies and capabilities for the manufacture of metal matrix composites and fibre reinforced ceramic matrix composites, including Hot Isostatic Pressing (HIP), electron beam and laser based metal additive manufacturing capabilities, Spark Plasma Sintering / Field Assisted Sintering Technology.

        2. Production technologies and capabilities for the manufacture of ceramic matrix composites, including chemical vapour deposition / infiltration, and melt infiltration

    ii. Materials

        1. Metal matrix composites: powder-based metal matrix composites and continuous fibre reinforced metal matrix composites

    iii. Software and data

        1. Capabilities for the design and design for manufacturing of fibre-reinforced metal matrix composites and ceramic matrix composites

b. Novel or complex metal alloys

    i. Test, inspection and production equipment

        1. any manufacturing processes that are involved in the solid state formation of alloys in or into crude or semi-fabricated forms, or powders for additive manufacturing, where “additive manufacturing” means a process of joining materials to make parts from three-dimensional model data;

        2. Single crystal and directionally solidified metallic casting

        3. Hot Isostatic Pressing (HIP)

        4. Spark Plasma Sintering / Field Assisted Sintering Technology

        5. Diffusion and friction-based joining processes for titanium, nickel and cobalt alloys and high performance specialist steels

        6. Friction-based processes to join metallic material layer by layer to create a structure

        7. Superplastic forming of titanium and aluminium alloys

8. Electron beam, laser and weld arc-based metal additive manufacturing capabilities (including wire arc additive manufacturing, MELD manufacturing)

ii. Materials

1. any alloys that are formed by chemical or electrochemical reduction of feedstocks in the solid state
2. Titanium alloys with continuous temperature-of-use capabilities above 350°C
3. Beryllium and its alloys
4. Powder metallurgy alloys
5. Titanium or nickel aluminides
6. Nickel and cobalt based superalloys with continuous temperature-of-use capabilities above 700°C
7. Steels for aero engine shaft applications
8. High strength high toughness weldable marine grade steels (Toughness levels D, E and F)
9. Armour grade steels
10. Armour grade aluminium alloys
11. High Entropy Alloys / Compositionally Complex Alloys (alloys that are formed by relatively large proportions of five or more elements)
12. Rare earth element-lean / free permanent magnetic materials
13. Soft magnetic materials with high total saturation flux densities greater than 2.0 Telsa, which may include monolithic and laminate forms, and particulate and fibre reinforced composite materials, intended for operation for long durations in high temperature environments (at and above 200°C) under mechanical loading.

iii. Software and data

1. Computer models of complex metallic components that embody a fluid and heat transfer function within their structure that have been formed by powder-based additive manufacture

2. Data on the performance of complex metallic components that embody a fluid and heat transfer function within their structure that have been formed by powder-based additive manufacture

c. Engineering and technical polymers and ceramics

i. Systems, equipment and components

1. Machines for additive manufacturing bulk materials combining electrically insulating and electrically conducting, or thermally conducting and insulating, or magnetic and non-magnetic materials (or further combination thereof) (not including mass-produced printed electronics)

2. Machines for additively manufacturing robotic or soft-robotic or autonomous vehicle or robotic systems

ii. Test, inspection and production equipment

1. Spark Plasma Sintering / Field Assisted Sintering Technology

2. Electron Beam Physical Vapour Deposition

iii. Materials (Feedstocks and constituents)

1. Armour-grade boron carbide and silicon carbide ceramics

2. Continuous silicon carbide fibres with diameters at and below 140 micrometres

3. Continuous carbon fibres with diameters at and below 10 micrometres

4. Continuous oxide-based ceramic fibres with diameters at and below 20 micrometres

5. Ultra-high temperature ceramics e.g. transition metal diborides

6. Engineering polymer materials and formulations with high structural rigidity, high Tg >190°C and / or non-flammable

7. Electroactive polymer (EAP) systems

8. Damage tolerant, self-healing polymer systems

9. High temperature, high pressure and chemically resistant elastomeric seals and systems

10. Magnetic materials, including fibres and particulates, for electromagnetic applications at frequencies above 500 MHz

11. Functional ceramics (including ferroelectrics, magneto-dielectrics, or multi-ferroics) for acoustic applications, or electromagnetic applications above 100 MHz

12. Dielectric and ferroelectric materials for use in the generation of, and manipulation of, high energy or high power radio frequency (RF) radiation; which may include functioning under high voltage conditions.

13. Dielectric or superconducting materials for use in detectors, sensors and imaging systems, especially reducing the need for cooling systems

14. Polymer electrical insulation materials with high temperature (greater than 200°C) and high voltage (in the kV range) capabilities for application in aviation electrical power management systems.

15. Filaments and feedstocks for additive manufacturing or 3D printing with bespoke and elevated electrical, magnetic, or electromagnetic properties (typically formed from filled polymer or mixed ceramic compositions).

d. Technical textiles

   i. Systems, equipment and components

      1. Textile materials and products manufactured primarily for their technical performance and functional properties rather than their aesthetic or decorative characteristics.

   ii. Test, inspection and production equipment

      1. State-of-the-art knitting and weaving processes

      2. Yarn manufacturing and texturing, dry fabric coating and laminating

      3. Manufacture of 3D textiles

   iii. Materials (Feedstocks and constituents)

      1. Smart fabrics with threads equipped with tiny sensors that respond to stimuli and perform a specific function

      2. Fabrics embedded with devices to enhance muscle recovery and to help with physical rehabilitation

      3. Fabrics made of smart polymers to protect and prevent injury

      4. Fabrics impregnated or coated for smart wound healing

5. Energy harvesting fabrics
6. Breathable fabrics that have a range of qualities including having a good stretch, lightweight and weather resistant.

iv. Software and data
1. Software and Computer-Aided Design for 3D printing of 3D shaped fabrics

v. Technology

1. Textile-based wearable electronics is an emerging technology with potential to enable subtle integration of electronics with the human body for human-machine interfacing.
2. Integration of functionalities such as energy harvesting, camouflage, structural and personnel health monitoring and protection.

e. Metamaterials

i. Systems, equipment and components

1. Metamaterials used in electromagnetic (including antennas, arrays, lens, devices), components; including but not limited to RF and microwave through to ultraviolet wavelengths, or for nano-photonics or quantum technology), thermal control and protection, airborne and underwater acoustics or in structural light-weighting applications.

ii. Test, inspection and production equipment

1. Means to fabricate 2- and 3- dimensional arrangements of one or more material and / or device constituents to form a metamaterial (including additive manufacturing, printed electronics methods, nano-fabrication, chemical self-assembly or engineering biology).
2. Means to non-destructively assure the 3-dimensional arrangement of the materials forming a produced metamaterial.

iii. Materials

1. Any metamaterial that does not include fibre-reinforced plastics in structural components, products or coatings with completely random dispersion of pigment or other filler; or any packaged device components that are designed for civil application
2. Tailored or bespoke feedstocks used in fabricating metamaterials (e.g. including blended filaments for fused deposition additive manufacturing)

iv. Software and data

1. Large accumulations of metamaterial designs, and elements comprising metamaterials that enable AI or machine learning design or optimisation of metamaterials.

v. Technology

1. Means and methods that enable metamaterials to alter their function and behaviour once installed or produced.

vi. Where:

1. “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;

2. “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.

f. Semiconductors

i. Systems, equipment and components

1. Key components enabled by compound semiconductors including control circuitry, power amplifiers, low noise amplifiers and monolithic microwave integrated circuits and detectors

ii. Test, inspection and production equipment

1. Compound semiconductor foundry and processing capability

2. Chip and Device fabrication

3. Ceramic and polymeric packaging of processed semiconductor chips

iii. Materials

1. Including gallium nitride, gallium arsenide and silicon germanium

2. With performance exceeding cadmium mercury telluride for thermal or electro-optical detectors or imaging devices or systems

iv. Software

1. Chip and Device design

g. Photonic and Optoelectronic materials

i. Materials

1. Materials that enable increased amplification, improved quality, improved robustness, improved electro-optical efficiency or reduced size or volume.
2. Materials and or coatings that reduce optical losses in lenses or mirrors.
3. Materials and or coatings that improve the physical stability or robustness of lenses or mirrors.
4. Materials enabling non-mechanical beam steering for detectors, sensors and imaging systems
5. Materials enabling wide fields of view for detector, sensing and imaging systems.

ii. Software and data

1. Algorithms, and their implementation in firmware, that compensate for the adverse atmospheric effects on laser beam propagation

iii. Technology

1. Any approaches that enable high power (>3kW) combined with high quality (M2 <1.2) amplifiers
2. Any aspects that enable the propagation of light over significant distances

h. Graphene and other two-dimensional materials

i. Systems, equipment and components

1. Developing equipment to synthesise single to few layer 2D materials controlling the desired structure of the materials and their application, including chemical exfoliation, atom/molecule intercalation, surface growth, solution phase growth, vapour deposition and large area chemical vapour deposition

ii. Test, inspection and production equipment

1. Production of high-quality materials at scale for use as a filler or pigment.

2. Means to integrate the use of materials in devices and systems
3. Conversion of graphene and other 2D materials into intermediaries using processes such as surface treatment and functionalisation, dispersion in matrices, mechanical and laser shaping, coating and ink printing processes.

iii. Materials

1. Graphene for lightweight, thermal and electrical conductivity, ballistic properties, electromagnetic, electronics and optoelectronics.
2. Graphene for graded multifunctional coatings, camouflage and signature management coatings.
3. Graphene for sensors for night vision, security, medical imaging and gas sensing
4. Graphene for wearable electronics, energy harvesting and energy storage
5. Other 2D Materials such as hexagon boron nitride and transition metal dichalcogenides (e.g. MoS2 and WS2) exhibiting excellent thermal conductivity and a wide range of photonic and electronic properties ranging from semiconductor, metallic and superconducting properties

iv. Technology

1. Synthesis of a new group of semiconductor 2D materials made up of single elements such as silicene, phosphorene and germanene nanosheets.
2. Stacking of different 2D crystals resulting in a charge redistribution between neighbouring crystals and/or causing structural changes.
3. Combining components made of different 2D materials or stack different 2D materials to make a component with finely tuned properties

i. Nanotechnology

i. Test, inspection and production equipment

1. Methods and means to fabricate, test and characterise nanoscale materials, devices and systems;
2. Methods to create or integrate for use in

a. Computer processing or memory devices;

b. Communications or electronic warfare devices or components;

c. Precision navigation and timing systems;

d. Detectors, sensing or imaging systems;

e. Counter-measure devices, systems;

f. Materials:

i. Magnetic or spinwave effects or technologies (including utilising skyrmions)

ii. Electro-optic, magneto-optic, photonic or nanophotonic effects or devices (including vertical cavity emitting lasers) and circuits, or

iii. Quantum effects or devices

iv. Micro- or nano- electro-mechanical, opto-mechanical, or electro-opto-mechanical effects or systems or

v. Metamaterials, metasurfaces, or

vi. Additive manufacturing or printing of moving parts or soft robotics

ii. Materials

1. High density nanoceramics and carbon nanotubes to reinforce ceramics for ballistic protection for vehicle and body armour

2. Carbon Quantum Dots, where used as sensors for detection of chemical, biological, nuclear warfare agents and/or used for photodetectors / luminescence security ink.

3. Smart Dust, where used to (1) enable wireless monitoring of people and products for security purposes (2) as sensor nets for underwater security - detecting sound emitted or magnetic disturbances from underwater threats (3) Monitoring activities in inaccessible areas

j. Critical materials, niche materials and materials related products

i. Systems, equipment and components

1. Industry grade production facility that has the potential or intent to be operated outside of a factory setting and/or as a temporary

facility including within a military forward operating base, on board a ship, or as part of a disaster relief endeavourbut not 3D printers generally available to the public

ii. Test, inspection and production equipment

1. Critical Materials: engagement in the extraction, refinement, processing, production and end of life recovery of materials identified in the British Geological Survey Critical Raw Materials Risk List (https://www2.bgs.ac.uk/mineralsuk/statistics/riskList.html) and EU critical materials list (https://rmis.jrc.ec.europa.eu/?page=crm-list-2020-e294f6);

2. Advanced circuit board manufacturing, including pitch/track or gaps dimensions less than 30 micrometres.

3. New component placement technologies, including multi-axis component placement.

4. Additive manufacturing or printing of moving parts, components and machines (known as '4D printing')

iii. Materials

1. Critical Materials: engagement in the extraction, refinement, processing, production and end of life recovery of materials identified in the British Geological Survey Critical Raw Materials Risk List (https://www2.bgs.ac.uk/mineralsuk/statistics/riskList.html) and EU critical materials list (https://rmis.jrc.ec.europa.eu/?page=crm-list-2020-e294f6);

2. 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 1.5e13 Hz up to and including ultraviolet;

3. Foams with designed electrical, electromagnetic and/or thermal protection properties.

4. Honeycombs with designed electrical or electromagnetic properties.

5. Smart materials (including micro-fluidic systems) whose properties can be repeatable altered once installed at rates exceeding 1 MHz.

6. 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.

iv. Software and data

1. Creative AI for material discovery and optimisation
2. Quantum simulation for material discovery and optimisation

v. Technology

1. Platform technologies enabling creative AI or Quantum Simulation for materials discovery

Rationale

Advanced materials are critical drivers of innovation across a range of technologies and sectors relevant to defence. Advanced materials, and their methods of manufacture and incorporation into either structural, functional or multifunctional components and systems, are essential for the performance of defence platforms and effectors. Since advanced materials technologies may offer performance advantage to defence capabilities it is necessary to control appropriately their proliferation to prevent their transfer to competitor states and to secure UK defence sector access to on-shore, strategically important advanced materials technologies.

Advanced materials offer significant benefits to military capability, for example through increased functionality, improved survivability, enhanced maintainability and reduced through-life cost. New lightweight materials could reduce the weight of weapons, armour and even whole vehicle platforms. Novel materials that can withstand high MACH numbers could be used in high-speed applications on aircraft. Low observable materials, including meta-materials, also provide future opportunities for advanced camouflage for soldiers, vehicles, aircraft and naval platforms. Military platforms across all operating domains (land, sea and air) need to incorporate an increasingly diverse range of materials to meet the complex and demanding requirements of the Armed Forces.

Materials are at the start of most manufacturing supply chains and feed into every stage of the production process. The UK has capabilities across the full spectrum of the materials supply chain, from the chemicals sector supplying feedstock, through research into new materials development, intermediate and final material production, to use of the materials to make parts.

Through this definition we aim to strike a balance between the need to protect critical UK technology advantage and the need to allow companies and their innovations to flourish and deliver non-defence products and services. It is crucial 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, which would risk adverse defence, security and economic impacts on the UK.

This definition specifies relevant materials and also materials manufacturing and process methods (for example chemical vapour infiltration), in order to safeguard products and their individual components. Materials cannot be separated from their manufacturing methods, as it is the manufacturing that gives them their specific properties and uses.

The definition intends to capture early-stage development through to the finished product, and the entire supply chain. It is crucial that we secure access to critical materials (maintaining both availability and affordability) to mitigate the risk presented by supply disruption (for whatever reason, from conflict to protectionist interventions). It is important that the UK supplier base is sufficiently robust, and that we mitigate the risks of foreign ownership and/or control by competitor countries.

The definition describes materials or material types and provides specific inclusions relating to their use, which are intended to refine the scope of the Bill's powers to specific circumstances. It was developed using recent amendments to the Enterprise Act 2002 as a starting point and following the structure set out in the Strategic Export Control Lists (SECL). The latter sets out in detail the materials and their applications that are subject to export controls.

The approach we have taken is to exclude from this definition, as far as practicable, the materials related technologies and capabilities already covered by the Defence, Military and Dual Use definition of the Bill and solely focus on those that are not covered elsewhere. We recognise that due to the vast range of advanced materials and their applications the definition is complex and that users will need to consider where advanced materials are covered within other parts of the Bill such as the Defence, and Military and Dual Use sections.

Nanotechnology has been incorporated into the advanced materials definition because it is a type of advanced material. The nanotechnology definition is broader than just nanomaterials as it needs to cover nanoscale processes to make features on nanometre scale including nanosystems and nanomachines. Semiconductors are included here as they are not being covered elsewhere in the Bill.

We are aware that some parts of these definitions are wider – for example, on breathable fabrics. We are keen to engage with the sector during the consultation process and welcome views on how to refine this to focus purely on areas that could cause security concerns.

Questions

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

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?
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?
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?

Advanced Robotics

Proposed definition

1. An entity carrying on activities in the United Kingdom which consist in or include developing or producing advanced robotics (or underpinning components or capabilities) that use artificial intelligence to perform a complex task.
2. In paragraph (1):
    a. “artificial intelligence” means technology designed to approximate cognitive abilities including reasoning, perception, communication, learning, planning, problem solving, abstract thinking or decision making
    b. “complex task” means image recognition, object identification, natural language understanding, statistical prediction based on uncertain or incomplete information

Rationale

Developments in advanced robotics, and in particular, capabilities such as being able to act with some degree of autonomy and to work independently and safely alongside humans, have the potential to unlock important defence and security applications, and similarly have the potential to present national security risks if acquired by hostile actors. Examples include unmanned land, air (commonly called drones), surface (or boats) and underwater vehicles and space satellites that could play a role in activities such as reconnaissance and intelligence gathering as well as warfare.

The draft definition therefore emphasises autonomy through some form of artificial intelligence as the principal defining characteristic of advanced robotics. This seeks to exclude traditional industrial robotics performing pre-programmed, repetitive tasks, such as the machining, lifting or pressing operations of a manufacturing process or assembly line. Such capabilities are widely available globally, and do not confer any particular strategic advantage to UK national security or present any threats if acquired by hostile actors.

We acknowledge that the draft definition could be refined to avoid capturing domestic applications and other less sophisticated applications. It is not our intent, for example, to capture technologies such as robot vacuum cleaners etc. We are keen to test how such applications can be readily differentiated from more sophisticated applications in a legally unambiguous way. There may also be other technological capabilities or characteristics beyond sophisticated autonomy/artificial intelligence that could underpin future UK national security capabilities, which require further evidence gathering and input. We are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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?
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?

Artificial Intelligence

Proposed definition

1. An entity carrying on activities in the United Kingdom which include developing or producing goods, software or information that use artificial intelligence to perform a complex task.
2. In paragraph 1:
    a. “artificial intelligence” means technology designed to approximate cognitive abilities including reasoning, perception, communication, learning, planning, problem solving, abstract thinking or decision making
    b. “complex task” includes image recognition, object identification, natural language understanding, statistical prediction based on uncertain or incomplete information

Rationale

Artificial intelligence (AI) technologies are transforming the global economy. The development and application of these technologies is an industry in its own right, but AI is also transforming business models across many sectors. They deploy vast datasets to identify better ways of doing complex tasks.

AI refers to the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence. The methods used to approach such tasks are often automatically formulated and/or adapted, based on pre-existing training data, or learned from interactions with an environment. Such tasks might include image recognition or natural language understanding. AI systems can employ, for example, machine learning, to develop, adapt or refine a set of instructions based on data collected during operation, in order to generate automated decision-making models for complex tasks. In some cases there may be interactions with both digital and physical environments.

AI can optimise the efficiency, precision, and performance of a range of existing technologies in a range of sectors. Its increasing deployment in military and social control scenarios has made the inherent dual-use of AI clear, raising concerns over security, data, and human rights. We must identify and mitigate the risks as specifically as possible in order to ensure that investment into our AI sector does not cause national security concerns.

The opportunity to use AI positively across the UK economy can only be harnessed if sensitive and critical applications of AI can be protected from the risk of hostile actors intending to do harm to the UK and its interests. AI is a rapidly developing technology and there is not currently an accepted legal definition. For the purposes of this legislation we have proposed

defining AI by referencing approximate cognitive functions as well as referring to complex tasks (including examples) that AI is used to perform.

Whilst AI has multiple uses and is used across sectors, we expect only a small number of notifications in AI to be taken forward for a full assessment under this regime. A wide definition ensures the Government is able to act in the minority of cases where national security concerns arise, accounting for future development of the sector and the wide range of possible risk factors, and we are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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

Civil Nuclear

Proposed definition

1. An entity that:

    a. holds or applies for nuclear site licences granted in accordance with section 3 of the Nuclear Installations Act 1965, except where the site to which the licence relates is controlled or operated wholly or mainly for defence purposes as defined in section 70(3) of the Energy Act 2013

    b. is a tenant operating 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, except where the site to which the licence relates is controlled or operated wholly or mainly for defence purposes as defined in section 70(3) of the Energy Act 2013

    c. holds Category I/II and/or Category III 'nuclear material' as defined in section 76(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 and B carrier of nuclear material as approved under regulation 14 of the Nuclear Industries Security Regulations 2003

    e. is a developer of a civil nuclear construction site as defined in section 70(3) of the Energy Act 2013

    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

    g. is subject to the prohibition on disclosure of uranium enrichment technology as defined in regulation 2 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 in receipt of financial support under section 5 of the Science and Technology Act 1965 for or in relation to nuclear reactors (as defined in section 26 of the Nuclear Installations Act 1965)

Rationale

The UK's civil nuclear sector is among the most advanced in the world, from fuel production, generation, new build, research through to decommissioning, waste management and transportation and our world class regulatory system.

The civil nuclear sector is also part of the UK's Critical National Infrastructure (CNI). It generates essential baseload, low carbon electricity critical to families and businesses, providing around 17 per cent of the UK's current electricity needs. Nuclear power is a key part of the UK energy mix, and the drive to move to a clean, low carbon generation that meets the binding targets set out in the Climate Change Act 2008, the Paris agreements, and the UK's Net Zero target; all while protecting consumers' bills.

As well as generating electricity, the civil nuclear sector also stores, processes and transports some of the most dangerous radioactive material and nuclear safety and nuclear security are essential to any nuclear operation.

The UK has a robust, independent civil nuclear regulator (the Office for Nuclear Regulation, ONR) and strong security regulations. This includes existing requirements on certain types of entities in the civil nuclear sector to notify the regulator of a relevant change in ownership, under the 2017 Memorandum of Understanding between BEIS and ONR.

The mandatory NSI regime is designed to complement the regulatory framework, by minimising any residual risks that could occur from a significant change in ownership of potentially sensitive assets within the sector.

The definition of the civil nuclear sector that is under consultation includes entities that would be expected to have access to civil nuclear material (e.g. licensed nuclear sites), sensitive nuclear information (e.g. Nuclear Industries Security Regulations Regulation 22 dutyholders), sensitive knowledge about the nuclear fuel cycle, and/or the ability to influence the protections that will be put around one of those things (e.g. developers of nuclear sites).

The definition is based on that set out in the 2017 Memorandum of Understanding between BEIS and ONR, but has been expanded to capture entities who may hold information or critical roles within the sector, including:

- Applicants for and holders of nuclear site licences, from point of submitting application
- Tenants of licenced nuclear sites
- Other nuclear premises who are holders of Category I/II and/or Category III nuclear material
- Licenced class A or B carriers of nuclear material
- Developers of nuclear construction sites
- Requesting parties who have submitted a design to ONR for the purposes of the Generic Design Assessment
- Entities involved in uranium enrichment
- Key contractors in the civil nuclear supply chain who hold classified sensitive nuclear information (i.e. NISR regulation 22 dutyholders)
- Organisations in receipt of HMG funding for research into civil nuclear technologies (including Small Modular Reactors and Advanced Modular Reactors)

Many of these organisations are already subject to nuclear regulation, but we are cognisant that the NSI Bill's mandatory reporting requirements will have new implications for different parts of the sector and its supply chain. We are keen to engage with the sector during the consultation process.

Questions

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

Communications

Proposed definition

1. An entity carrying on activities in the United Kingdom which consists in or include:
    a. providing an electronic communications network;
    b. providing an electronic communications service;
    c. making available facilities that are associated facilities by reference to an electronic communications network or an electronic communications service.
2. For the purposes of this regulation, “associated facility”, “electronic communications network” and “electronic communications service” have the same meanings as given in section 32 of the Communications Act 2003.

Rationale

The communications sector comprises the telecommunications, internet infrastructure and broadcast infrastructure sectors. It is diverse, technologically advanced and constantly evolving. It is integral to national security, the economy and society as it underlies the operations of all businesses, public safety organisations, Government, and citizens. We are keen to engage with the sector during the consultation process to develop and refine this further. In particular, the definition currently captures a very wide range of private communications networks, many of which will not present national security concerns, and so we are particularly keen to work with industry to reduce this scope.

Telecommunications and internet infrastructure

The telecoms and digital infrastructure sectors provide the infrastructure and services that support the backbone of our digital economy – together these sectors support our society and economy and are a vital part of the UK’s critical national infrastructure. The telecoms and digital infrastructure sectors are already key parts of life in the UK, and as technology develops both in these sectors and the wider sectors they support, our dependence on fast, reliable and secure communications networks is only likely to grow.

As a regulated sector the definition is rooted in existing legislation – the Communications Act 2003 – in order to provide clarity and consistency across the regulatory frameworks.

The definition explicitly includes “associated facilities” to avoid any doubt about the vital inclusion of sub-sea fibre optic cables and services, including cable landing stations, which together form the backbone to the internet.

The inclusion of “associated facilities” is also intended to capture two further areas vital to the provision of the telecoms network and services and internet infrastructure in the UK:

1. The associated telecoms supply chain. As the telecoms network is simply made up of different components, equipment and services supplied by different companies, the supply chain for the telecoms and internet infrastructure equipment and services that the companies rely on is as important as the network itself.

2. Digital infrastructure companies. Internet infrastructure comprises Internet Exchange Points, Domain Name Services, and Top Level Domain. The companies that provide these are therefore integral to the provision and functioning of the internet and internet services in the UK.

In both cases national security risks can arise from these companies with implications for the UK's communications networks in the same way as for telecoms providers.

Media and broadcasting

This sector definition ensures that providers of broadcast infrastructure for the BBC, national commercial radio (analogue or digital) or television services for the UK's public service broadcasters (holders of C3 licenses, Channel 4, Channel 5 and S4C) are covered as they are providers of electronic communication networks or services.

The definition of an electronic communication service (see section 32 of the Communications Act 2003) excludes services that are content services. Therefore, providers of broadcasting services (including television and radio) are not included and therefore not subject to the mandatory notification regime. Enterprises who provide both broadcasting infrastructure and content will be covered by this sector definition.

These organisations will also continue to fall within scope of the existing media plurality regime in the Enterprise Act 2002, which covers broadcasters and newspapers. The media plurality public interest regime will remain in its current form and separate to the new national security regime.

Questions

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?

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

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?

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?

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?

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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?

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

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

Computing Hardware

Proposed definition

1. An entity that:
    a. creates or supplies intellectual property relating to the functional capability of
        i. Computer processing units
        ii. the instruction set architecture for such units
        iii. computer code that provides low level control for such units
    b. designs, maintains or provides support for the secure provisioning or management of:
        i. roots of trust of computer processing units
        ii. computer code that provides low level control for such units
    c. fabricates or packages computer processing units

Rationale

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.

These changes have also brought challenges. Advances in technology now mean that there are ubiquitous goods with the potential to be directed remotely should a hostile actor obtain access or control. For example, this could enable a hostile actor to use these goods to cause harm, or to identify vulnerabilities in them. Mergers related to businesses that undertake these activities, therefore, have the potential to give hostile actors knowledge or expertise that could be used to undermine our national security.

The definition specifies two activities in this area of the economy, which have the potential to present the highest national security risks if bought by hostile actors:

- The ownership, creation or supply of intellectual property relating to the functional capability of:
    - computer processing units;
    - the instruction set architecture for such units;
    - computer code that provides low level control for such units

- the design, maintenance or provision of support for the secure provisioning or management of:
    - roots of trust of computer processing units;
    - computer code that provides low level control for such units

This means that enterprises that own, create or supply intellectual property in relation to the way that processing units function will be in scope. Businesses that manage roots of trust in relation to processing units are also in scope. We are keen to engage with the sector during the consultation process to develop and refine this further.

What is a "computer processing unit"?

A "computer processing unit" is a hardware device that can be programmed to carry out a range of functions.

This would include, but is not limited to:

- A Central Processing Unit (CPU) for a laptop or smartphone
- A Field Programmable Gate Array (FPGA) device
- A microcontroller for general purpose application
- A System on Chip
- Application specific integrated circuits
- Graphics Processor Units

What are "roots of trust"?

"Roots of trust" means hardware, firmware, or software components that are inherently trusted to perform critical security functions, (including, for example, cryptographic key material bound to a device that can identify the device or verify a digital signature to authenticate a remote entity).

This means that enterprises that own, create or supply intellectual property in relation to the way that processing units function will be in scope. Businesses that manage roots of trust in relation to processing units are also in scope. This could include businesses that design firmware containing the cryptographic material for a processing unit.

What is Fabrication?

This relates to businesses which process the production of a microelectronic circuit on a semiconductor substrate or using other advanced materials, for example, from raw silicon to circuits on silicon.

What is Packaging?

This relates to businesses which process the turning of 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.

Questions

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

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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?
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?

Critical Suppliers to Government

Proposed definition

1. An entity that is, whether directly or indirectly, contracted to provide goods and services which if lost or compromised could result in a detrimental impact on the availability, integrity or delivery of government services, or an adverse impact on national security, or the functioning of the state, whose contracts include one or more of the following:

    a. The handling of SECRET or TOP SECRET material

    b. A requirement for List X and / or List V accreditation

    c. A requirement for employees of the company to be vetted above Baseline Personnel Security Standard (BPSS)

    d. The processing or storage of personally identifiable information (PII) of 5000 or more individuals in the aggregate as part of 'the company's' provision of goods or services to Public Sector organisations.

    e. The collection, distribution or handling of Government monies, including but not limited to taxes, benefits, grants and subsidies

    f. The supply or maintenance of infrastructure, software or hardware as an integrated element of Government network functions, including the provision of data storage and use of data centres

    g. The design and/or construction of Government property, including but not limited to drawings, CAD, blueprints, specifications, digital models, digital twins and calculations

    h. Unaccompanied access to buildings owned or managed by central or local Government organisations

    i. Provision of security services to physical estates or cyber networks

    j. Provision of energy and fuel supplies to Government

Rationale

The Government is keen to include in the NSI mandatory regime suppliers that provide goods or services on which the Government relies to carry out its duties, while keeping this list as narrow as possible to reduce the burden on suppliers and investors.

As such, this definition focuses on elements of Government contracts that are particularly sensitive or critical. This is not an exhaustive list of all areas in which certain transaction could

cause concern, but it represents a series of conditions which would be found in contracts of high importance to the functioning of Government.

By protecting these areas of the Government's supply chain, we are attempting to guard against a number of risks. For example, damage or disruption by a hostile owner to critical suppliers could impair the Government's ability to deliver key services. Unauthorised access to sensitive or classified information could undermine critical security work.

Over time, it is possible that the Government will be able to specify in contracts that certain transactions should be notified to the NSI regime, rather than relying on legislation to require notification. However, this is not currently an option. It is not feasible or proportionate to amend all supplier contracts to account for this, and even inserting into all new contracts is a significant process.

We are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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

Critical Suppliers to the Emergency Services

Proposed definition

1. An entity that is contracted by the emergency service, governing body, or professional organisations, to provide goods or services to Emergency Services that are critical to the delivery of that emergency service.
2. In paragraph (1), "emergency service" refers to:
    a. Fire and Rescue services and their authorities
    b. Police
    c. British Transport Police
    d. Ministry of Defence Police
    e. Civil Nuclear Constabulary
    f. Ambulance
    g. Border Force
3. In paragraph (1), "Services that are critical to the delivery of that emergency service" are, for the purposes of these powers, defined as:
    a. Personal Protective Equipment
    b. Non-PPE hardware used operationally
    c. Vehicle hardware
    d. Forensic Services
    e. IT and Communications Infrastructure

Rationale

The Emergency Services are essential to our safety and security. The Government is keen to include in the NSI mandatory regime suppliers that provide goods or services on which the Emergency Services rely to carry out their duties.

We do not however seek to include such goods and services that, while important, are non-essential to the execution of key emergency service functions, such as general office supplies or non-emergency IT infrastructure. We also do not seek to capture critical goods and services related exclusively to counter terrorist activity in the police and wider emergency services, as such goods and services are sufficiently covered by existing powers. We further do not at present seek to include the broader supply chains used by direct suppliers to emergency

services as it is deemed that such supply chains are unlikely to be individually critical to the delivery of core emergency services.

Through including these critical suppliers in the mandatory regime, we aim to ensure the Emergency Services can continue to carry out their duties. In particular, we wish to protect against the possibility of:

- Interruption to the supply of key goods or services This risk is especially acute for consumable goods. For example, interruption in the provision of clinical grade PPE could impact Ambulance Services ability to respond to certain medical emergencies, and interruption in the supply of oxygen could impact the ability of fire and rescue services to fight fires.
- Sabotage of key goods and services, in particular IT and communications infrastructure. For example, damaging the core systems used to process and direct 999 calls could reduce the ability of the public to report, and emergency services to respond to, emergencies, and sabotage of communications systems could reduce the ability of emergency services to communicate during live incidents
- Access to sensitive and restricted information. For example, the ability to listen in to emergency service communications could harm operations.

The supply chains for the Emergency Services are complex, and we are keen for views on how effectively the definition captures the critical areas without imposing unnecessary burdens. In particular, the definition has a UK-wide focus, but a great deal of procurement for emergency services takes place on a local level.

This definition also only captures direct suppliers, rather than the wider supply chains on which those direct suppliers themselves rely, and so may miss critical suppliers further down the chain. Ensuring we include critical suppliers while not placing disproportionate administrative burdens on the wider economy calls for a careful balance, and we welcome views on whether the proposed balance is right. We are therefore keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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?

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

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?

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?

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?

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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?

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

Cryptographic Authentication

Proposed definition

1. An entity that designs, produces or creates technology to verify the identification of a person, user, process or device, where the method of verification employs cryptography in performing that function to protect the authenticity, confidentiality or integrity of the information.

Rationale

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.

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. We should be capturing entities that research and/or develop products which have authentication as a primary function and that employs cryptography in performing that function.

Companies that provide cryptographic authentication operate across much of the economy, providing software and hardware tools for businesses to enable a number of key capabilities, including:

- Verification of user identity through biometric data (such as speech or facial recognition, iris or fingerprint scanning), or multi-factor authentication (such as a hardware token or software application).
- Authentication of a human-operated or automated device to a network to allow access to the network, data and other resources.
- Verification of the origin and integrity of an email, message or document through digital certificates, and security protocols

Examples of technologies in scope include:

- Systems that authenticate the biometric property of an individual to allow access to a restricted area
- a credit or debit chip and pin card at an ATM
- the digital information held on an e-passport to determine the identity of the holder

Hostile actors may be able to access critical systems and undermine national security if they gain access to this technology by acquiring a business in this sector. Significant damage to the UK could result if authentication systems are compromised or bypassed, including through sabotage and espionage, to allow a hostile actor to gain unauthorised access to systems critical for national security. We are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Data Infrastructure

Proposed definition

1. An entity that:
    a. owns or operates relevant data infrastructure or manages relevant data infrastructure on behalf of other entities, or
    b. owns the site on or building in which relevant data infrastructure is located, or
    c. through the provision of specialist or technical services to entities in 1 or 2, could access relevant data on relevant data infrastructure. Depending on their operation, this may include:
        i. security services controlling and monitoring physical access to the site where the relevant data infrastructure is located, or
        ii. equipment installation services, installing the relevant data infrastructure, or
        iii. equipment repair and maintenance services in respect of the relevant data infrastructure
    d. provides services which give it privileged access to virtualised relevant data infrastructure
    e. produces or develops software designed for use in the services in paragraph (1d)
2. “Relevant data infrastructure” means physical or virtualised infrastructure which:
    a. hosts, stores, manages or processes or controls or transfers relevant data; or
    b. is used by Public Communications Providers for peering; or
    c. connects any major international cabling routes; or
    d. employs software defined networking or network functions virtualisation
3. “Relevant Data” means data used for the operation of essential services or business continuity of any entity that falls under the mandatory notification regime of the National Security and Investment regime.
4. “Privileged access” means physical, logical and/or administrative access, where such access would otherwise be restricted or compartmented without such privileged access. Privileged access includes editing rights and/or configuration rights.
5. “Peering” means the exchange of data directly between Public Communications Providers, rather than via the internet

Rationale

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 secure and resilient in the face of established, new and emerging risks, protecting the economy as it grows.

National security risks to data infrastructure can arise where an entity's activities give it access to data via physical or virtualised infrastructure used to store large volumes of sensitive data and/or to facilitate connectivity. Such access could be achieved through ownership, management or control of key data infrastructure, or by the provision of certain technical services to such infrastructure. The draft sector definition addresses these scenarios and excludes entities that operate within data infrastructure, but do not have privileged access to sensitive data.

A primary purpose of the definition is to capture entities that have a significant ability to impact national security. We want to understand if, for this purpose, the definition has appropriate coverage – specifically, on operating models, on the provision of technical services, and virtualised services. We therefore welcome industry engagement during the consultation process to develop and refine this further.

Questions

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?

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

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?

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?

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?

Sector specific questions *(note that numbering of sector specific questions matches the numbering on page 13-15)*

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? In your response, we are particularly interested in whether we have accurately covered the various operating and ownership models within the data infrastructure sector; the provision of technical services to relevant data infrastructure; and the provision of virtualised services to relevant data infrastructure.

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 within your facility? To what extent are these provided by in-house staff or outsourced and how is security of data ensured?

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?

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 are 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?

Defence

Proposed definition

1. An entity that is involved in 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 mentioned in this subsection 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 subsection 1
3. “Defence” has the same meaning as in section 2(4) of the Official Secrets Act 1989 (c. 6)
4. “Government contractor” has the same meaning as in the Act of 1989

Rationale

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.

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.

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 providing goods or service for defence or national security purposes where they satisfy either one of the two conditions.

The first condition in the definition is that the entity is a government contractor or any sub-contractor 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.

The second condition is that the entity has been notified by HMG that they hold, or may come into possession of, classified material. HMG has an established Security Policy Framework (link) 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 a number of 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.

We are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Energy

Proposed definition

1. An entity involved in the ownership and operation of:

    a. terminals, upstream petroleum pipelines and infrastructure which forms part of a petroleum production project, with a throughput of greater than 3,000,000 tonnes of oil equivalent per year;

    b. infrastructure (such as import jetties) which forms part of a gas importation and storage project which, if at maximum capacity, could output 20 million cubic meters of gas per day for at least 50 days, where: “gas” has the same meaning as 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; "petroleum", "petroleum production project", "terminal", and "upstream petroleum pipeline" have the same meaning as in section 90 of the Energy Act 2011 and "tonne of oil equivalent" is a unit of energy defined as the amount of energy released by burning one tonne of crude oil.

    c. Energy distribution and transmission networks that deliver secure, reliable electricity and gas to customers, ensuring continued supply as far as possible in the supply chain;

    d. Energy suppliers that provide energy to significant customer bases, where “significant customer bases” means 250,000 or more final customers;

    e. Gas and electricity interconnectors, long range gas storage and Gas Reception Terminals, including Liquefied Natural Gas that contributes to the security of supply

    f. Electricity undertakings that:

        i. carry out the function of supply; or

        ii. carry out the function of generation via individual generators that would have a total capacity, in terms of input to a transmission system, greater than or equal to 100 megawatts; or

        iii. carry out the function of generation via generators that, when cumulated with the generators of affiliated undertakings, would have a total capacity, in terms of input to a transmission system, greater than or equal to two gigawatts.

    g. The supply of petroleum-based road, aviation or heating fuels (including liquefied petroleum gas) to the UK market, by companies who provide or handle more than 500,000 Tonnes per annum, and, a downstream facility

owner if the owned facility has capacity in excess of 20,000 tonnes, through at least one of the following activities:

i. the import of any of crude oil, intermediates, components and finished fuels;

ii. the storage of any of crude oil, intermediates, components and finished fuels;

iii. the production of intermediates, components and finished fuels through a range of refining or blending processes;

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

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

Rationale

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.

The energy sector covers many industries and, such is its importance, we are keen to include investment in the following sub-sectors in the mandatory regime:

- The UK's gas and electricity networks, supplying gas and electricity to homes across the UK.
- The oil sector, from extraction to refinement and distribution.
- Power generation including renewables.
- New technologies such as battery storage

The increasing digitalisation and globalisation of the energy system means we must be extra vigilant in identifying investment in novel energy technologies. While the definitions focus on established technologies, 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. We are keen to engage with the sector during the consultation process to develop and refine the definition further.

Questions

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?

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

Engineering Biology

Proposed definition

1. An entity undertaking activities in the United Kingdom which consist of or include:
    a. the research, development and production of synthetic biology; or
    b. providing a service connected with engineering biology.
2. "Synthetic biology" means the design and fabrication of biological components and systems that do not exist in the natural world. This includes, but is not limited to, design and engineering of biological based parts such as enzymes, genetic circuits, and cells; novel devices and systems; redesigning existing natural biological systems; and using microbes to template materials, or cell-free systems.
3. "Engineering biology" means:
    a. the process of innovating, researching, demonstrating and developing synthetic biology;
    b. making products consisting of or derived from synthetic biology

Rationale

Synthetic biology is the design and fabrication of biological components and systems that do not already exist in the natural world. The process of taking synthetic biology concepts and turning them into real world solutions is engineering biology. Engineering biology captures the entire innovation ecosystem, spanning breakthrough research to demonstration, and will be the way that synthetic biology research is turned into defence capabilities.

By providing greater safeguards in our engineering biology sector, we hope to protect national security and make the UK a global biotechnology partner of choice. We aim to protect our national security by ensuring manufacturing scale-up facilities, sensitive knowledge, data, and delivery systems are prevented from being removed from the UK.

We are keen that in addressing bio-engineering risks through NSI we do not impede legitimate research and development activity that will be crucial to combating current and future threats, and which makes an important contribution to UK economic prosperity. Ensuring balance between providing appropriate safeguards while not imposing disproportionate burdens on companies and investors is therefore important.

Bio-engineering is, by its very nature, rapidly evolving and technically complicated. Commercial bio-engineering tools or enabling technologies are both dual-use and difficult for Government to comprehensively monitor well enough to proactively call in transactions that are not notified. This is not a sector where we can easily identify organisations involved in defence and security related work. There are potentially harmful uses for almost all aspects of

engineering biology, from basic research through to manufacture and use. The UK must also protect its manufacturing capability.

For example, companies that would be of interest include, but are not limited to, those developing vaccines, disease resistant crops, novel materials, novel sensors, novel power and energy approaches, forensic technologies, DNA data storage, and novel approaches to certain chemicals. All of these have the potential for military use and / or could provide our adversaries with insights that could be used against the UK's national security. We are therefore keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Military and Dual Use

Proposed definition

1. An entity the activities of which consist in or include:
    a. developing or producing restricted goods;
    b. 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
2. "Relevant export control legislation" means:
    a. Schedules 2 and 3 to the Export Control Order 2008;
    b. the Schedule to the Export of Radioactive Sources (Control) Order 2006;
    c. Annex I to Council Regulation (EC) No. 428/2009
3. "Restricted goods" means goods, software or information the export or transfer of which is controlled by virtue of their being specified in the relevant export control legislation but excluding any goods, software or information which are controlled only to the extent that they are prohibited from being exported or transferred to one country only.

Rationale

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 by a potentially hostile actor – with their expertise and intellectual property – is highly likely to raise national security concerns.

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 great importance to the Government, this is beyond the scope of this legislation and is best addressed through other means.

This definition covers entities that:

- develop or produce restricted goods; or
- hold related information (including but not limited to information comprised in software and documents such as blueprints, manuals, diagrams and designs) that is capable of use in connection with the development or production of restricted goods and the information is responsible for achieving or exceeding the performance levels, characteristics or functions of the good.

Restricted goods are goods, software or information 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) No. 428/2009

We are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

Quantum Technologies

Proposed definition

1. An entity that:
    a. Researches:
        i. quantum computing or simulation;
        ii. quantum imaging, sensing, timing or navigation;
        iii. quantum communications;
        iv. quantum resistant cryptography; or
        v. quantum connectivity
    b. develops or produces anything designed, modified or adapted for use or application in:
        i. quantum computing or simulation;
        ii. quantum imaging, sensing, timing or navigation;
        iii. quantum communications;
        iv. quantum resistant cryptography; or
        v. quantum connectivity
    c. supplies services, including design and integration services employing:
        i. quantum computing or simulation;
        ii. quantum imaging, sensing, timing or navigation;
        iii. quantum communications;
        iv. quantum resistant cryptography; or
        v. quantum connectivity
2. “Quantum communications” means:
    a. the transmission of information, utilising the properties of quantum mechanics, specifically superposition, entanglement, single photon technology or the use of conjugate variable technologies; or
    b. includes the establishment of cryptographic keys or the generation of the true random numbers using a quantum physical process

3. “Quantum computing or simulation” means the study, simulation, emulation or realisation of systems that utilise certain properties of quantum mechanics, in particular superposition, entanglement or quantum annealing, to process information, run algorithms or perform operations on data.
4. “Quantum imaging” means utilising phase or amplitude properties of quantum mechanics, specifically superposition, entanglement or the use of single-photon optics, to create images of objects.
5. “Quantum navigation” means utilising phase properties of quantum mechanics, specifically measurements of suspensions of atoms or ions, or photon interferometry, to establish the location or movement of objects.
6. “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.
7. “Quantum sensing” means utilising phase properties of quantum mechanics, specifically measurements of suspensions 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.
8. “Quantum timing” means utilising phase properties of quantum mechanics, specifically measurements of suspensions of atoms or ions or atomic gases, to provide a timing or synchronisation signal.
9. “Quantum connectivity” means the ways (algorithms, protocols and physical principles) in which components or devices utilised in any of the above technologies communicate with other components and devices or with data.

Rationale

Many of the devices on which the digital revolution was built, such as computers, phones and MRI scanners, rely on the physics of quantum mechanics. The advancing understanding and control of what are known as ‘quantum effects’ (for example superposition and entanglement) will lead to a new wave of advances in areas such as sensing, data transmission and encryption, timing and computing that will have significant defence and national security applications. These are often referred to as ‘second generation’ quantum technologies.

Due to (in many cases) the early stage of technological development, as well as the pace of scientific discovery, it is not possible to envisage all potential future applications for quantum technologies. However, some application areas are already emerging that have potential national security implications. For example, 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 technologies could also represent important military capabilities, for example, enhanced sensing or navigation.

Although the technical risk has not yet materialised, quantum computers, when fully scalable machines do come, are expected to pose a significant threat to the cryptographic systems which underpin much of our existing cyber security.

Government considers all areas of second-generation quantum technology development to be of potential importance for national security interest, in particular given the UK's leading position in this field.

The draft definitions build on those in the Enterprise Act Amendments 2018 (and 2020), which extend powers to the Secretary of State to intervene in mergers which might give rise to national security implications. Those definitions were consulted on widely with the quantum community at the time. We are however now proposing amendments to reflect both that these technologies have evolved, and to give as much specificity and certainty as possible to companies as to whether they fall under the mandatory reporting requirements of the NSI Bill (whilst also aiming to exclude related technologies that do not have national security implications). As a result, we acknowledge that the definitions as drafted are in places technical in nature. We are keen to engage with the sector during the consultation process to develop and refine this further and would particularly welcome consultees' views on whether they can be widely and clearly understood by the quantum technology business community.

Questions

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

Satellite and Space Technologies

Proposed definition

1. An entity carrying on activities which consist in or include operating, designing, producing, creating or applying:

    a. facilities for the transmission of voice, data, text, sound and video using a satellite telecommunications infrastructure

    b. space debris management, provision of in-orbit servicing and robotics capabilities, in-orbit maintenance and manoeuvring, and space traffic management. This includes any technology or system that through design could have a dual use in disrupting or interfering with satellites

    c. provision of Internet access by satellite infrastructure

    d. provision of specialised telecommunications applications

    e. provision of in-orbit and intra-orbit communications links, including radio frequency and optical links

    f. operation, maintenance, or control of ground infrastructure and associated facilities related to space-based services

    g. manufacture of instrumentation, spacecraft and launch vehicles, satellites, planetary probes, orbital stations, manned space vehicles

    h. satellite provision, processing and utilisation of earth observation data

    i. provision of satellite position, navigation or timing data

    j. provision of space infrastructure operational control facilities, including control stations, uplink and downlink facilities

    k. provision and processing of situational awareness information for orbital, near-earth and solar weather events

    l. operation and maintenance of orbital and sub-orbital launch facilities and capabilities

    m. provision of testing service of equipment for space-based services

    n. provision of space science and exploration activities (the disciplines that involve the study and exploration of outer space)

Rationale

The UK is a world-leader in small satellite technology, telecommunications, robotics and Earth observation, while British 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, GNSS, etc.).

The Government believes that most companies in the sector are sufficiently sensitive that they should be included in the mandatory regime of NSI. This definition has therefore been kept deliberately broad due to the wide range of rapidly changing technologies that are covered by the sector. The sector covers a range of aspects such as manufacturing, launch, and operations, all of which can be deemed as sensitive in nature. Even aspects of the sector that may not initially appear to be sensitive (for example, space science and exploration activity) can arguably be seen to push technology forwards and pave the way for new future operational capabilities, meaning that they should also be in scope for the NSI mandatory regime.

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. The rate of innovation and progression in the sector is only speeding up, and this definition seeks to cover all current and future sensitive aspects that could pose a potential risk if acquired by a potentially hostile actor. We are therefore keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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?

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

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?

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?

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?

Transport

Proposed definition

1. An entity which owns or operates a maritime port or harbour which handles at least 1 million tonnes of cargo annually in the most recent relevant year for which the Annual Port Freight Statistics records are published by the Department for Transport, Category 1 goods as listed in paragraph (2.c) or vessels capable of carrying at least 12 passengers. Within such maritime ports or harbours, a company which owns and operates terminals, wharves or other port related infrastructure except where that company does not handle Category 1 goods.

2. In paragraph 1:

    a. “entity” may include a private company, a Board governing a Trust port or a port owned by a local authority.

    b. “operates” means to control the functioning of a machine, process or system.

    c. “harbour” includes estuaries, navigable rivers, piers, jetties and other works in or at which ships can obtain shelter or ship and unship goods or passengers, in accordance with s313 of the Merchant Shipping Act 1995.

    d. “Category 1 goods” are:

        i. Human Medicines, covering Prescription-only, Pharmacy and General Sales List Medicines, clinical trials and children’s vitamins (for import and export)

        ii. Medical Devices and Clinical Consumables (for import and export)

        iii. Vaccines (for import only)

        iv. Nutritional Specialist Feeds, including Infant Milk Formula (for import only)

        v. Biological materials such as blood, organs, tissues and cells (for import only)

        vi. All Veterinary Medicines authorised under the Veterinary Medicines Regulation 2013, including finished and un-finished products, and Active Pharmaceutical Ingredients (for import and export)

        vii. It also includes unauthorised medicines permitted for import under the Veterinary Medicines Directorate’s Special Import Scheme (for import only).

        viii. Critical food chain dependencies, e.g. chemicals and key additives used within the food supply chain (for import only as required).

ix. Chemicals for water purification and treatment (for import only as required).

x. Critical spare parts for the energy sector (for import only as required).

xi. Items required for Military or National Security purposes (for import or export as required).

3. An entity which owns or operates an airport in the United Kingdom which handled at least six million passenger movements or 100,000 tonnes of freight annually in the most recent relevant year for which records are published by the Civil Aviation Authority.

4. An entity which provides en route air traffic control services or which owns such a provider.

5. In paragraph (3):

   a. “airport” has the meaning set out in section 66 of the Civil Aviation Act 2012;

   b. “freight” means goods transported in bulk in passenger aircraft or aircraft used for the transportation of cargo only;

   c. the owners of an airport are:

      i. a company which owns the airport (“C”);

      ii. any holding company of C (“H”); and

      iii. any parent company of C or H;

   d. the “operator” of an airport is the entity with overall responsibility for its management;

   e. “relevant year” means 2018 or such later year as may be specified in regulations made by the Secretary of State.

6. In paragraph (4):

   a. “en route air traffic control services” mean services provided pursuant to a licence under section 6 of the Transport Act 2000; .

   b. the owners of an en route air services traffic provider are:

      i. a company which owns such a provider (“C”);

      ii. any holding company of C (“H”);

      iii. any parent company of C or H.

Rationale

The transport sector is essential to keeping the country moving, and many essential services rely on it to function, especially through freight and ensuring people can get to work.

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, this focuses on areas which both 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. It covers key transport infrastructure in the maritime, aviation and air traffic control sectors.

The definition will capture assets who own or operate in three areas:

- Maritime: major ports or harbours are those that handle at least one million tonnes of cargo annually in the most recent relevant year for which the Annual Port Freight Statistics records are published by the Department for Transport, Category 1 goods as listed in schedule 1 or vessels capable of carrying at least 12 passengers. Within such maritime ports or harbours, this includes a company which owns and operates terminals, wharves or other port related infrastructure except where that company does not handle Category 1 goods. The definition incorporates all fifty-one ‘major ports’.
- Aviation: this captures those airports with significant annual throughput in passengers (six million annually) or freight (100,000 tonnes annually) according to CAA published figures. Initially the definition will work by reference to the published figures for 2018 because of reduced demand due to the Covid pandemic in 2020, but there will be power for the Secretary of State to make regulations to change this to a later year once demand recovers. This bolsters regulation already in place by the Civil Aviation Authority and overseen by DfT. It does not capture those companies that undertake specific operational roles at airports such aircraft ground handling, maintenance or provision of other passenger services such as catering or retail.
- Air traffic control: this is a regulated area but the importance of a secure air traffic system inclusion allows for a greater level of assurance and scrutiny.

There are a number of potential risks from nefarious investment, including an enhanced ability to undertake espionage within the sector, targeting intellectual property, identifying vulnerabilities in our systems, and accessing other sensitive information, which could harm the safety and effectiveness of the transport system.

There are risks around an ability to undertake disruptive or destructive actions which could harm security, such as the denial or degrading of key services or supply lines which could compromise our critical national infrastructure. This could endanger lives through creating problems in the movements of critical goods or compromising passenger safety and undermine public trust in a safe transport network.

The transport sector definition broadly seeks to avoid duplication in areas 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.

Rail infrastructure operators are not included in the definition as they are either publicly owned (e.g. Network Rail) or other notification processes already exist (e.g. Channel Tunnel Fixed Link). Similarly, the definition does not include roads, which are maintained through local councils or Highways England, or rail franchises, which are established through DfT and use equipment leased and maintained by Network Rail.

Emerging technology within the transport sector, such as AI or autonomous vehicles, is captured under other sector definitions and so is not included here.

We are keen to engage with the sector during the consultation process to develop and refine this further.

Questions

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

This consultation is available from: www.gov.uk/government/consultations/national-security-and-investment-mandatory-notification-sectors

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.