Department for Business, Energy and Industrial Strategy
By email: nsisectorconsultation@beis.gov.uk

6 January 2021

Dear Sir/Madam,

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

We are writing on behalf of the British Private Equity and Venture Capital Association ("BVCA"), which is the industry body and public policy advocate for the private equity and venture capital industry in the UK. With a membership of over 700 firms, we represent the vast majority of all UK based private equity and venture capital firms, as well as their professional advisers and investors. Between 2015 and 2019, BVCA members invested over £43bn into nearly 3,230 UK businesses, in sectors across the UK economy ranging from heavy infrastructure to emerging technology. Companies backed by private equity and venture capital currently employ 972,000 people in the UK and the majority of the businesses our members invest in are small and medium-sized businesses.

As outlined in previous submissions[1], the BVCA supports, in principle, the measures being introduced in the National Security and Investment Bill (the "Bill") to protect the UK's national security interests. We consider that, if calibrated correctly, the new rules should be helpful in ensuring the UK remains an attractive location for investment and conducting business. However, the Bill must strike a balance between protection of genuine areas of critical national security interest on one hand, and raising unnecessary hurdles for foreign investment in UK infrastructure and businesses on the other.

Feedback from a range of our member firms is clear that, in the absence of sufficient clarity, a large number of transactions will be notified voluntarily, and a huge number of transactions will be notified as mandatory notifications in the absence of clear guidance as to what is outside the scope of the mandatory regime. The potential for a flood of notifications relating to transactions constituting no threat to national security (which could mask transactions that actually pose a threat) and damaging interruptions to inward investment is high. Clarity, transparency, precision, and proportionality are key.

We are particularly concerned about the impact of the new framework on venture capital funding for innovative UK-based start-ups and growth businesses in high-tech sectors like quantum technologies, engineering biology, artificial intelligence and others. This kind of investment depends on speed of execution (often much less than 30 days from proposal to completion) and low transaction costs that correspond to the much smaller investment size than is typical in M&A (so the costs associated with the national security due diligence and filing process will have a much bigger impact on the viability of an investment, relative to larger transactions). The UK has the biggest VC industry in Europe largely because global entrepreneurs see an ecosystem that helps their businesses access capital quickly and efficiently, allowing them to meet their growth ambitions.

[1] We have responded to previous consultations relating to the Bill, including the 2017 Green Paper (Chapter 7 and Chapter 8) and the 2018 White Paper. We also provided our feedback on the Bill to BEIS by way of a letter dated 18 December 2020.

British Private Equity & Venture Capital Association
5th Floor East, Chancery House, 53-64 Chancery Lane, London WC2A 1QS
T +44 (0)20 7492 0400 F +44 (0)20 7492 0401 bvca@bvca.co.uk www.bvca.co.uk

The proposals in the Bill have the potential to delay and increase the cost of transactions in this space to the extent that they will reduce the appeal of the UK as a base for international early-stage innovators, whose start-ups are much more mobile than more firmly established businesses, at a time when other jurisdictions are introducing policies that explicitly seek to attract these people to contribute to their national economies. For this reason, the Bill in its current form cuts directly across BEIS' policy goals under other proposals, such as December's consultation on restricting non-compete clauses, which aims to "unleash innovation, create new jobs… increase competition… [and] maximise opportunities for individuals to start new businesses… to drive the economic recovery". The Government needs to tread very carefully to avoid damaging this country's reputation as Europe's premier destination for innovative and ambitious start-ups and entrepreneurs, which, once tarnished, will be difficult to restore. This is particularly the case as the world moves to remote working which means the choice of jurisdiction to establish a start-up is even more global.

Key to avoiding this negative impact will be to define, narrowly and clearly, the "key sectors" requiring mandatory notification and limit the application of the Bill to those parts of the key sectors which pose a risk to national security. This will help ensure that transactions posing no threat to national security are not notified by well-meaning reputable investors whose investment is welcomed by the UK, who are concerned to avoid criminal and other sanctions, or worse, who decide to avoid investment in the UK given the time and costs required to make notifications as well as the uncertainty and execution risk this regime entails.

We continue to receive feedback from our members on this Bill, and will send on additional insights separately after the consultation closes.

Response to consultation questions applying to all sectors

Q1. 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?

No. It is critical that the key sectors which are in scope of the mandatory regime are clearly and narrowly defined as those which are of material interest to national security. This aligns with the political aim of the legislation. The list provided and associated definitions are generally very broad and all encompassing. In order for this regime to focus solely on national security, and not on broader premises of public or national interest, these sectors must be precisely and narrowly defined.

It becomes more problematic to identify whether there is a potential target transaction risk the more removed the relevant entity is from the relevant sector, and it would be helpful to have a greater explanation of the extent of the supply chain which needs to be considered in examining a particular transaction. For example, suppose that Company A operates gas generator plants. Company B is the exclusive supplier of gas turbines to Company A. Company C is a critical supplier of turbine blades to Company B. Company D is the sole manufacturer of the specialist metal alloy used to make the turbine blades. Will Companies C and D be caught even though they are not directly critical suppliers to a core sector? We consider that for the Bill to be proportionate in its application, direct suppliers should be captured rather than requiring an analysis of the entire supply chain which is often not possible in the course of due diligence during an investment or transaction.

Another example is "Energy" as a category. We note that specific energy sectors have been identified and some thresholds included (e.g., throughput of 3,000,000 of oil) which is helpful to provide clarity. However, it would be helpful to include specific thresholds for all the subsectors, such as energy

distribution and transmission networks that deliver supply to customers (e.g., to exclude smaller independent distribution networks) or a threshold for storage terminals. It would also be helpful to clarify the relevant time period for measurement – for example by reference to the last accounting period or an average over a number of years, etc.

The definitions currently do not provide such specification. Similarly, "dual use" as a category potentially brings into scope many businesses which manufacture or hold items which present no national security concern and we think some further parameters should be included to limit the scope of the definitions without compromising national security.

Furthermore, we have consulted member firms who predominately invest in the deep technology field and they have highlighted three definitions of particular concern, as set out below (and also discussed further in later questions). As currently drafted, the definitions are too broad, which will lead to unnecessary burdens for many small, fast growing businesses in areas of the economy that the UK wants to support.

Engineering Biology

The draft definition is not specific enough to allow for reliable self-assessment, and too broad to prevent companies that pose no risk to national security being needlessly included. In the draft definition, Engineering Biology is defined as an entity "*undertaking activities in the United Kingdom which consist or include… the research, development and production of… the design and fabrication of biological components and systems that do not exist in the natural world."*

The nature of modern biochemical engineering means that many compounds may be created which are highly unlikely to exist naturally. Due to the ambiguous definition of Engineering Biology, which refers to "*biological components"*, and for such components to "*not exist in the natural world"*, investors would be unable to determine definitively whether transactions in this area would be subject to the mandatory notification regime.

Furthermore, if the system *does* exist in the natural world, then it would be much more difficult to patent and of limited interest to investors.

Data infrastructure

The draft definition implies a relevant entity as anything that *"owns or operates"* some "*physical or virtualised infrastructure which hosts, stores, manages or processes or controls or transfers relevant data*". The term "*relevant data*" is expanded to include all information "*used for the operation of essential services or business continuity"* for all entities subject to the mandatory notification regime.

This is an extremely broad and expansive definition, encompassing nearly all forms of information that could be relevant to the functioning of a company subject to the mandatory notification regime, regardless of the extent to which that information poses a threat to national security. Subsequently, several companies that are subject to the mandatory notification regime for other reasons may also fall into the Data Infrastructure category because they are responsible for storing their own data.

Artificial Intelligence

The draft definition is too broad and is insufficiently clear for effective self-assessment. This is explained in detail in our answer to Question 8.

Q2. To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?

We have commented specifically on the various sector definitions in question 1 above and in the questions that follow where we consider them to be insufficiently precise and overly broad. The importance of keeping the definitions of sectors clear is compounded by the absence of any definition of a "risk to national security" itself. Other countries' foreign investment regimes include a definition of national security interest which provides some element of certainty to market participants and ensures that short term political agendas do not become national security concerns. This is particularly important for investors (and target businesses) to fully understand the scope of the regime in the absence of any de minimis threshold.

Q3. To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?

These sectors cover areas of the economy where foreign investment may cause risks to national security but they go far beyond this in extending to areas of the economy which do not pose any such risk. As such they must be more narrowly drawn. We also consider that a de minimis threshold and safe harbours for pre-approved investors would make the Bill more proportionate in its application and less of a deterrent for much needed investment across these sectors. See our response to question 5 below.

Q4. 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?

We consider the voluntary regime and call-in powers to be sufficient.

We think that in addition to clarifying the definitions for sectors to ensure that they only capture those segments of the sector that could pose a "risk to national security" and providing some indicia of what such risks might be, we consider that in order to minimise the impact on business, the Government should utilise the provision for secondary legislation to exempt certain transactions. This would be very helpful in ensuring the Bill is proportionate in its scope of application, especially for mandatory notifications, without compromising national security. The exemptions we propose are as follows:

- Acquirers that are funds managed by regulated fund managers should be such an exempted category. This would encourage benign inward investment in the UK, give much greater certainty to our members, and avoid unnecessary or disproportionate vetting of firms that are already supervised by the FCA and equivalent regulators globally.

- Businesses that have been vetted by and received funding from UK Government sources aimed at promoting innovation and growth in certain sectors should be deemed as presenting no target risk and therefore exempt from voluntary or mandatory notification. This again would be a proportionate approach consistent with the Government's aim of supporting innovative new business.

- Businesses and transactions that have been vetted by another UK regulator (such as OFGEM or OFCOM and other national regulators specific to a particular industry or infrastructure sector) would be exempt to avoid duplicating costs, confusing and contradictory regimes and extended waiting time periods. This has been done to an extent

(e.g., in the transport and communications sectors) but it would be helpful to do so across the board; and

- Businesses, particularly early-stage ventures, whose ownership structures conform to an approved set of criteria that appropriately limit control and information rights before and after the relevant transaction could also be granted a safe harbour exempting them from mandatory notification.

The UK should also consider an analogous framework to the Excepted Investor concept adopted by the CIFUS regime, whereby investors from certain key states fall under certain different provisions.

It will be critical to ensure that the Investment Security Unit ("ISU") has sufficient, appropriately skilled resources to allow it to process both the confidential guidance requests and the inevitably high number of notifications it will receive, particularly in the early years of the regime. In particular, we consider that to validly identify whether businesses pose a threat to national security requires a detailed operational and technical understanding of those sectors, particularly in areas such as technology and AI where innovation is constant.

It is also vital that the ISU has the appropriate senior links with relevant officials to provide decision-relevant insight from across Government and that the ISU itself be staffed with enough senior decision-makers to allow the notification process to run smoothly and efficiently, and for decisions to be reached as quickly as possible. As noted above, this is particularly important for venture transactions.

A significant concern among our members is with the quantity and nature of information required to be submitted to the ISU when completing a notification/call-in event. This information is often very sensitive so it is critical that it is stored in a secure manner and in accordance with GDPR.

Notifiable acquisitions that are completed without the approval of the Secretary of State should be voidable at the discretion of the Secretary of State, rather than automatically void. This would provide an extra layer of protection and a clear point at which a completed transaction is void.

The extra-territorial nature of the Bill makes the UK proposals significantly more expansive than similar regimes in other jurisdictions, where the target entity typically must be registered in the relevant jurisdiction. To avoid the UK becoming an outlier in this regard, we advocate that the new regime should only catch UK-registered targets or businesses with a significant UK presence.

Q5. 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?

One of our key concerns about certain definitions used in the Bill (in particular the sectors Advanced Robotics, Artificial Intelligence, Communications, Computing Hardware, Cryptographic Authentications, Data Infrastructure, Energy, Engineering Biology and Quantum Technologies) is the potential impact on our members active in the emerging company and venture capital community. You will appreciate that venture capital funding of innovative new companies in technology and related industries is critical to the UK's business ecosystem. Early-stage investments of relatively small amounts in an expedited timeframe to fund key milestones during R&D phases is common amongst young businesses with strong growth potential. It is also critical to the effective commercialisation of innovative IP generated within the UK that seed and early-stage UK investors are able to secure further co-investors and syndication partners to continue funding promising businesses as they seek to scale

up. The UK investor community does not have sufficient resources to achieve this alone, but the UK funding ecosystem currently compensates to some degree with its openness to foreign investment. This openness is especially important for attracting global (particularly US) specialist investors with considerable resources to venture away from their domestic markets to back the growth within the UK of exciting new businesses in sectors like health tech, life sciences and deep tech (many of which would be captured by the 17 key sectors identified in the Bill).

For example, the definition of Advanced Materials is very broadly defined in places. It includes gallium nitride which is already the main material used for LED devices and is becoming rapidly used in the power electronics industry. Given that semiconductors is not a sector where the UK is a global leader, it risks encouraging entrepreneurs to relocate to other jurisdictions, perhaps where there the industry is more established (US, Korea, China). Conversely, graphene is a newly emerging sector where the UK could become strong in if it can attract enough investment. Venture capital investments in this area will be caught by this legislation in subsequent funding rounds and as they need significant investment, will not find it possible to attract this capital from UK sources alone.

As a case study, a firm founded a company in 2019 to develop highly innovative T-reg cell therapies to prevent rejection in organ transplantation and treat autoimmune and inflammatory diseases, based on technology developed at King's College and UCL in London and Hannover Medical School in Germany. This is a competitive market space where significant capital will need to be invested to develop, manufacture and market cutting-edge therapies. The firm does not see any national security risk in this business. Cell therapies are a key area of opportunity for UK science and the UK cell therapy sector has already been strongly backed by Government by its establishment of the Cell and Gene Therapy Catapult. The firm chose to build the company in London based on access to two of the founding institutions and their belief that the UK is a strong location to attract future funding given the need for significant future investment. However, the business could have been established elsewhere, either in Germany (near to the other founding institution and giving the company a direct connection to the work coming out of the Hannover Medical School) or in the US (closer to the strongest funding market). While some work would have continued in the UK, the centre of gravity of the business would be elsewhere and the value created in the UK far reduced.

Imposing a mandatory filing obligation in this context will have a significant impact on the timeframe for funding rounds, which is usually much less than 30 working days. Speed of execution is particularly critical here, as the targets are often fast growing but initially loss-making businesses that will fail if they cannot secure timely injections of further capital.

In addition, the cost of preparing notifications may be prohibitive in the context of these investments, as national security due diligence and mandatory filings will represent a significant proportion of total transaction costs.

The number of notifications should primarily be limited by ensuring a narrow scope to the mandatory regime. Where this is not possible and notifications have to be made in the genuine interests of national security, they must be dealt with rapidly and cheaply ideally using a simple short template for initial screening purposes. Otherwise, the framework risks discouraging potential investors from investing in UK-based companies, and encouraging businesses to locate elsewhere. Were the development of high-tech innovations to shift out of the UK for these reasons, this loss of visibility would in itself be detrimental to national security.

For these reasons, we would strongly recommend adding a de miminis exclusion to the mandatory regime. This would be best applied sector by sector in the absence of any monetary threshold. In

addition, we would favour blanket: (i) acquirer-specific clearance of individual acceptable investors (where the investor is managed by a regulated fund manager); and (ii) target-specific clearance of acceptable businesses (e.g., those that have received funding from Government sources, as outlined above). These exceptions would be very useful in reducing the notification burden both on the investment community and the Government. Indeed, the work of the Future Fund (a Government-backed investment scheme) will be substantially undercut by making it materially harder for the companies the Future Fund has funded to raise additional venture capital. Attracting additional external investment is a key part of the construct of the Future Fund.

Our members' experience with the somewhat analogous US foreign direct investment ("FDI") review regime administered by the Committee on Foreign Investment in the United States ("CFIUS") provides the following observations:

- The regime compels "mandatory" CFIUS filings with respect to certain non-US investments in US businesses that deal in one or "critical technologies." Significantly, the CFIUS regulations define "critical technologies" with reference to US export control concepts, which contemplate – among other considerations – the national security implications of exporting various technologies to various destinations outside the US. Relevant US export control regulations, however, are not solely tailored to national security interests, and take into account other policy considerations. Accordingly, the export control classification of a given technology is not a perfect proxy for the national security implications of that technology's release to foreign investors. In our members' experience, certain technologies that are controlled for export purposes and that therefore constitute "critical technology" for CFIUS purposes do not in fact have meaningful national security implications. An example is cryptographic technology that provides encryption functionality in software. US companies that develop software with benign and ubiquitous encryption functionality can be subject to mandatory pre-closing CFIUS filing requirements notwithstanding the fact that an objective observer would find no meaningful national security concern with a foreign investment in or acquisition of the company or its technology. The key learning point is that the criteria for mandatory filings should be thoughtfully and narrowly tailored to legitimate and articulable national security concerns.

- The CFIUS regime does not offer transacting parties any meaningful opportunity to consult on an informal basis with the regulators. For example, there is no mechanism or channel for parties to ask CFIUS how it interprets ambiguous provisions in the CFIUS regulations, or to seek a non-binding view as to whether a generically-described transaction might be viewed as presenting national security issues. Moreover, decisions by CFIUS with respect to transaction subject to CFIUS review are confidential and not precedential. The provision of an official, even if informal, channel for communication with regulators may promote uniformity. Moreover, providing direct access to regulators may benefit smaller companies who may not have the resources to spend significant amounts on legal advice.

- Transaction costs have increased significantly. CFIUS diligence to determine if a voluntary or mandatory filing is required can consume up to 30% of the cost of legal diligence on a venture capital investment. Where filings are required, costs rise dramatically and can increase by a further $50,000 (even then, the advisers often have to write off much more, sometimes the same amount as billed) where mandatory filings are required. Some of these fees are sometimes written off by lawyers resulting in losses, with the rest borne by investors and/or the company. The significant potential cost increase and uncertainty impacts the overall attractiveness of a deal, with investors sometimes electing at the outset

not to pursue investments where a filing may be required. The Government and ISU officials who are overseeing the process should also consider what procedural efficiencies they can implement to mitigate any potential risks of investors choosing not to pursue a transaction due to these costs (or the additional time that will be added to the investment timetable), which can disproportionally dwarf traditional transaction costs and timeframe.

- The mandatory filing regime established by the regulations implementing 2020 CFIUS reforms require transacting parties to submit a filing – when one is required – no later than 30 days prior to closing (or more specifically, prior to a foreign investor being afforded CFIUS jurisdiction-triggering rights that are customary in a venture capital style investment). This 30-day lead period is incongruent with commercial realities in the venture capital and growth investment communities, where transactions normally close within a matter of weeks. As a consequence of this inflexibility and misalignment, "foreign" investors and "domestic" (*i.e.*, U.S.) investors are dissimilarly situated vis-a-via one another, with foreign investors often in a disadvantaged position. This disparity has a chilling effect on foreign investment, and adds complexity, delay, and transactions costs for all parties. The regime has added otherwise unnecessary delays to the completion of transactions, causing uncertainty and appropriate flexibility ought to be introduced.

In order to limit the impact on deal timelines and the potential for parties to use the rules strategically, we would welcome the removal of the ability to "stop-the-clock" whilst information is gathered as this gives rise to significant uncertainty. This is not an uncommon feature in regulatory regimes but there should be some guidance or limitation on the maximum period that might arise.

In relation to the timing for assessment once a trigger event has been called in, we would recommend including a reasonable threshold, on the basis of clear and objective criteria, for any extension of the review beyond the initial 30 working day period, in order to reduce the risk and uncertainty to the transacting parties involved. Failure to do so may have a cooling effect on investment into (and within) the UK. We recommend that notified transactions should be deemed cleared where the acquirer has received no clearance nor extension decision from the Government within 30 days of notification. This will ease the burden on the ISU, prevent deals being held up due to lack of Government resource and provide certainty to parties that receive no decision within the timeframe.

Response to consultation questions applying to specific sectors

Advanced Robotics

Q6. 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?

Artificial intelligence is used across a multitude of industries for complex tasks, including advanced robotics, which would not pose any risk to national security. We consider that the range of tasks be limited to sensitive tasks involving national security, with a clear definition of what these tasks encompass, would be more appropriate than including artificial intelligence itself as a sector.

Q7. 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?

See response to question 6 above.

Artificial Intelligence

Q8. 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?

See response to question 6 above. "Artificial intelligence" covers a huge range of increasingly ubiquitous yet innocuous applications that may be classed as complex (such as software designed to assist in due diligence processes or litigation management) that are likely to pose no national security risk.

"Complex tasks" cover nearly all software-based tech companies, as most will use some form of off-the-shelf pattern recognition, classification, or optimisation algorithm. The fact that such "complex tasks" can be addressed through software is what attracts investors in the first place. As such greater clarity on the nature of the sensitive tasks and how they would pose a risk to national security is required. The definition of a complex task includes *"image recognition, object identification, natural language understanding, statistical prediction based on uncertain or incomplete information"*. The uncertainty in these definitions has consequences for investment strategies in companies that may or may not be considered AI under this definition.

In addition, the language used to determine the scope of a *"complex task"* and *"artificial intelligence"* is inconsistent. The draft definition states that complex tasks "*include*" certain activities, whereas AI *"means"* certain activities. It is not apparent whether the lists following these words are exclusive, or merely examples. This requires clarification before it comes into force to avoid companies that do not obviously fall into scope notifying the Government of transactions as an insurance against intervention.

By way of example, a member firm has noted an investment into a company that has undergone Series A funding and uses desktop-sized super-resolution microscopes, combined with specialised software, to track biological molecules to resolutions of up to 20nm. It is not clear the extent to which this software can be considered to perform a *"complex task"* as used in the draft definition of AI, as a consequence of the ambiguity as to whether the functions of the company's software could be said to engage in *"image recognition, object identification… [or] statistical prediction".* The member firm is unable to determine definitively whether a transaction involving this company would be subject to the mandatory notification regime.

Q9. This definition is intended to include companies that develop AI technologies but do not purchase AI products. Is that accurately reflected?

There are two ways to interpret the definition, as a consequence of the ambiguity of the subject to which the verb "use" applies in the first sentence.

If the definition means that "An entity carrying on activities… that use AI" is subject to the mandatory notification regime, then this definition subsequently applies to acquirers of AI products in addition to developers of AI.

If instead, the definition means that an entity that "[develops or produces] goods, software, or information that use AI" is subject to the mandatory notification regime, then this requires clarification in order to be understood. For instance, it is not clear what it would mean for a "good" or "information" to use AI.

Additionally, it is not clear that the distinction between developers and purchasers of AI exists in the way that the Government's consultation question implies. The future of the AI industry will involve many companies purchasing relatively untrained AI architecture, and then teaching that AI how to perform a task in that company. It is not clear whether or not the Government considers this to be a new piece of intellectual property subject to the mandatory notification regime.

Communications

Q10. 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?

We consider the definition to be overly broad – see response to question 12 below.

Q11. Is the definition clear that the Communications sector definition includes entities that provide public and private electronics communications networks, and their associated facilities?

We consider the definition to be overly broad – see response to question 12 below.

Q12. How can the definition be narrowed to exclude private communications networks that do not pose a risk to national security?

We also note that communications are already heavily regulated and therefore we query the need to specifically include any communications business that is currently regulated by Ofcom and communications related legislation[2]. The Telecoms (Security) Bill seeks to address potential national security risks and we consider that any transactions or businesses regulated through that regime should be excluded from the remit of this Bill to avoid inconsistency and confusion of two different regimes. If a general "Communications" must be included to cover those transactions not regulated by the Telecoms (Security) Bill, then greater guidance on what constitutes a "risk to national security" in this sector and a conceptual de minimis threshold (that are not turnover related but relate to the significance and scope of the particular communications network to the UK) will be required to ensure that the Bill is proportionate.

Computing Hardware

Q13. 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?

Since almost all consumer electronic devices contain central processing units, this will cover a very wide range of businesses that again pose no risk to national security per se. We suggest excluding from this definition all consumer electronics and the creation or supply of intellectual property that relates to products intended for consumer use.

[2] Communications Act 2003, the Wireless Telegraphy Act 2006, the Investigatory Powers Act 2016, the Data Protection Act and General Data Protection Regulation (EU) 2016/679, the Privacy and Electronic Communications Regulations 2003.

Q14. We consider that integrated circuits with the principal purpose of providing memory should be covered here. Is it clear what products this would cover?

As per our response to question 13, given the extensive use of integrated circuits for memory we consider that consumer electronic devices should be excluded.

Critical Suppliers to Government

Q15. 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?

Critical suppliers to emergency services are Government-controlled and so we would expect that the Government's procurement processes, and any operational restrictions to be imposed by Government, should be sufficient to protect the national interest. Therefore, we query the need to include this as a key sector but in any event consider that this should be very narrowly drawn. We also consider it appropriate to limit it to direct suppliers (or indirect suppliers who have received notice from Government of an indirect supply) rather than impose sanctions on investors in indirect suppliers who may not be aware of the full supply chain.

Q16. Are there alternative ways to ensure notification of relevant transactions, for example through contracts?

As per our response to question 15, we consider that any national security concerns can be adequately addressed during the Government procurement process and in appropriate change of control provisions in contracts requiring advance notice to Government of an acquisition. Such clauses should be disclosable to third party purchasers to ensure particular transactions are investments are not in scope without the investor's knowledge. This already exists in contracts with the Ministry of Defence and is generally well-understood by defence contractors.

Critical Suppliers to the Emergency Services

Q17. 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?

See response to question 15.

Q18. Are there aspects of the broader supply chain to direct suppliers that should also be captured within this regime?

See response to question 15.

Data Infrastructure

Q19. 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.

As explained earlier, the definition of data infrastructures is very broad and would, for example, include landlords of real estate who lease land to the operator of a data centre with very minimal control or visibility on the operations of such a data centre. Similarly, the inclusion of providers of physical security services and monitoring physical access to sites is also unlikely to be relevant to "facilitating privileged access to the data infrastructure". Similarly, there will be software used by providers of services to data infrastructure operators (including security systems) which does not afford any access to the data either by the software provider or the customer and so we query the need to include this limb. We suggest that this definition be narrowed to hone in on operators of "Relevant data infrastructure" who have access to data held or who control access to such data.

See also our response to question 1.

Q20. 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?

N/A

Q21. 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?

N/A

Q22. 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?

N/A

We would be very keen to discuss the contents of this letter with you and look forward to hearing from you in order to establish whether a meeting of this sort is possible.

Yours faithfully,

Amy Mahon
Chair, BVCA Legal & Accounting Committee