RESPONSE OF GLOBAL INFRASTRUCTURE INVESTOR ASSOCIATION TO THE CONSULTATION ON SECTORS IN THE SCOPE OF THE PROPOSED MANDATORY REGIME IN THE NATIONAL SECURITY AND INVESTMENT BILL 2020

6 JANUARY 2021

1. INTRODUCTION

Global Infrastructure Investor Association ("**GIIA**") welcomes the opportunity to respond to the UK Government consultation on the secondary legislation to define the sectors subject to mandatory notification in the National Security and Investment Bill 2020 (the "**NSI Bill**" or "**Bill**"). We are keen to work constructively with the Government, to achieve an outcome which reflects the concerns of our members and ensures that the proposed mandatory regime does not adversely affect their incentives to invest in the UK.

GIIA is the membership body for the world's leading institutional investors in infrastructure (giia.net). Our members operate in 55 countries across 6 continents and are responsible for over US$780bn of assets under management globally with over 1/3 of that value invested in the UK. GIIA is therefore well placed to provide the Government with the views of the global infrastructure investor community.

Of the 17 sectors the Government has proposed to include within the scope of the NSI Bill's mandatory regime, we provide below our views on four sectors which are of particular interest to GIIA members: Communications, Data Infrastructure, Energy and Transport.

GIIA considers that considerable work is needed on all the four definitions, primarily to ensure that they do not capture transactions which are highly unlikely to raise national security issues and are sufficiently clear, bearing in mind the crucial importance of clarity of scope in the context of a mandatory regime backed by very significant sanctions for non-compliance.

Before providing comments on the four sector definitions (see Section 3), we also provide some general observations on the NSI Bill, which we would strongly urge the Government to take into account both with regard to the Bill generally, and in developing the secondary legislation associated with the proposed mandatory regime.

We confirm that nothing in this response is confidential. We would be happy to be contacted by BEIS in relation to our response.

2. GENERAL OBSERVATIONS ON THE NSI BILL

This section sets out GIIA's general observations on the NSI Bill and the nature of the regime that it envisages. These observations form the backdrop for the specific comments on the four sector definitions set out in Section 3.

2.1 **The current proposals will result in a very high volume of mandatory (and voluntary) notifications.** The envisaged scope of the mandatory regime is currently very wide. Most of the 17 sectors are broadly defined, and there are no turnover or (in many cases) other size thresholds. As is clear from the Government's Impact Assessment, the Government understands that this, together with associated voluntary notifications, will result in a very large number of notifications, the vast majority of which are not expected to raise any national security issues whatsoever (the Impact Assessment suggests that only 5-10% of notifications will require an in-depth national security assessment and less than 1% will be subjected to remedies). This raises serious questions as to whether the Government is casting the net too widely, given its stated goal not to deter foreign investment. Our comments in Section 3 below provide some suggestions for how the scope of the mandatory regime could be narrowed without adversely affecting UK national security, bearing in mind that the call-in power will be able to pick up those rare cases that fall outside the scope of the mandatory regime, but nevertheless raise material national security issues.

2.2 **Resourcing and timing.** Given the very large expected number of notifications (even if the breadth of the mandatory regime is reduced), it will be of vital importance that the Government has a sufficient number of well-trained personnel to manage notifications efficiently within the envisaged 30 working day initial screening period. Indeed, given its goal not to deter foreign investment into the UK, it should be the Government's firm objective to take significantly less than the full 30 working day period to clear the vast majority of cases. The Government should also ensure that the notification process is simple, and that lengthy periods of "pre-notification discussions" do not become the norm, as is the case for merger notifications to the Competition and Markets Authority. In this regard, we note that the information required for a national security review should in principle be much more straightforward than for a competition analysis. There is also a concern as to the timing of when notifications can be made, as explained further in paragraph 2.10 below.

2.3 We are aware that the Government has plans to recruit around 100 staff to perform the new review role within BEIS. It will be crucial that the vast majority of staff are in place and fully trained from the moment the new regime is in force if unnecessary delays are to be avoided. In addition to this, robust systems should be in place to facilitate coordination between BEIS and other Government departments where required, including stringent data protection protocols.

2.4 **The Government's approach to the call-in power.**

(a) **Lack of clarity on risk factors.** The Draft Statement of Policy Intent (the "**Draft Statement**") published by the Government describes how the Secretary of State expects to use the call-in power under the NSI Bill, including the three risk factors that will be considered. GIIA expects that whether a full national security assessment will be required (and remedies may be necessary) will frequently turn largely on acquirer risk (and will certainly do so in the context of a 100% acquisition of a business within the scope of the mandatory regime). However, the Draft Statement is brief and does not provide sufficient clarity for investors to assess with confidence whether a transaction would be at risk of a call-in, including which investment partners might increase the acquirer risk. It is striking that the Draft Statement (including the acquirer risk section) is significantly shorter than the equivalent draft Statement of Policy Intent published by the Government in connection with the National Security and Investment White Paper in 2018[1]. Whilst GIIA welcomes the comments made in the Draft Statement on pension funds, state-owned entities and sovereign wealth funds, these statements are limited in scope and are not definitive. GIIA recognises that the Government wishes to have significant discretion in this area. However, if further guidance cannot be provided in the Statement of Policy Intent, this is likely to lead to a very significant number of cautious voluntary notifications, as well as to deter investment into the UK. It would also hugely increase the importance of informal advice (considered further below) as a means of providing greater clarity to investors as to whether they, and potential partners, could raise national security issues. Further, although we recognise this is not the Government's intention, a lack of boundaries in this area also raises concerns as to potential "mission creep" and the risk of decision-making motivated by protectionism or other industrial policy goals distinct from national security; particularly in light of the power of the Secretary of State to amend the Statement and other aspects of the regime through regulations.

(b) **Retrospective application.** The Bill's current provisions have the effect that, once it enters into law, the Government will be able to call-in any transaction which completed on or after 12 November 2020. GIIA considers this retrospective application to be unjustified. First, we query whether retrospective application is

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/728311/20180717_Statement_of_policy_intent_-_shared_with_comms.pdf

appropriate at all, given that the provisions of the Enterprise Act 2002 would presumably apply to most such transactions such that the Secretary of State could intervene on public interest grounds to protect national security, if appropriate. The Government should provide a clear statement in guidance that the call-in power will not be used where a transaction falls within the scope of the Enterprise Act 2002. We note in this regard that the transitional provisions in the Bill clearly provide for the Enterprise Act to have on-going effect until such time as any action is taken under the new regime in relation to the relevant event. Second, whilst GIIA understands the Government wishes to be able to review transactions which were rushed through following announcement of the NSI Bill, imposing the risk of a call-in on well advanced transactions which were already expected to complete in late 2020 or early 2021 is unreasonable, particularly where a binding transaction agreement had already been signed prior to 11 November 2020. GIIA considers that, if any retrospective application is regarded as essential, the starting date from which the call-in power can be applied should be no earlier than 1 January 2021 and that it should not be applied at all to deals which signed (but did not close) prior to 12 November 2020.

(c) **The 5 year/6 month look-back.** The Bill would allow the Government to use its call-in power up to five years after a transaction completes. Although the Government notes that similarly lengthy look-back powers exist in other countries, GIIA considers this excessive. We would suggest that a period of two years would be more appropriate. It is understood that the six-month limit in clause 2(2) is intended to refer to the date on which the Secretary of State actually became aware of a transaction, rather than when the deal was announced or publicised. GIIA notes that this is different from the position under the Enterprise Act 2002, whereby a detailed Phase 2 investigation can be launched up to four months after closing of, or sufficient publicity in relation to, a transaction, whichever is later. GIIA would see significant merit in adopting a similar approach under the NSI Bill. However, if the Government is not willing to accept this, it should make clear in guidance that the six-month period refers to when the Secretary of State actually became aware, and that this can be achieved by writing to the Secretary of State. Additionally, GIIA suggests that the Government includes a clear statement in guidance that the call-in power cannot be used with respect to a transaction which has previously been screened but not called in, to allow investors sufficient certainty that their transactions cannot be considered again once they have passed the initial screening.

2.5 **Exemptions for low risk investors.** GIIA believes that acquisitions by low-risk financial investors (including non-UK ones) into infrastructure assets should not pose any national security risks. The present breadth of the mandatory regime and uncertainty regarding the Government's approach on acquirer risk, runs the risk of undermining investor confidence in this sector in the UK. The NSI Bill envisages at clause 6(5)(b) that regulations may make provision for exemptions by reference to the characteristics of the acquirer. GIIA would urge the Government to introduce such regulations as a matter of priority to exempt certain low risk categories of investors from mandatory notification. GIIA would expect the vast majority of our infrastructure investor members to be capable of being exempted. GIIA believes that the creation of exemptions for institutional investors with a track record of financial investment into UK infrastructure assets would provide significant additional clarity to the market and reassurance to infrastructure investors. This exemption system could be established by way of a certification regime for particular investors, perhaps supported by an annual attestation to be completed by those investors to confirm each year that they continue to qualify for the exemption.

2.6 **Treatment of passive investors.** GIIA would also urge the Government to clarify its approach to passive investors in investment funds. GIIA believes that it should be made clear that limited partners in the classic limited partnership structures used by many investment firms, where they are passive investors and decision-making rests solely with the general partner/manager, should not be subject to the regime. In other words, the

Government should not "look through" investment funds to the passive investors which hold the beneficial interests in those funds, since those investors have no means to influence the management of the underlying businesses.

2.7 **Treatment of investment consortia.** Under the Bill, the obligation to make a mandatory notification is on the acquirer. In the context of infrastructure investments in the UK (and many other transactions), the direct acquirer will very frequently be an acquisition vehicle owned by a number of funds managed by various investment firms/fund managers. GIIA would welcome clarity as to the impact of the provisions in Schedule 1 of the NSI Bill on investment consortia. Specifically, does the Government understand the combined effect of paragraphs 3 and 11 to be that each member of an investing consortia, regardless of stake, would be treated as having a common purpose and would therefore each be considered as being subject to the notification obligation, alongside the direct acquiring entity? If so, GIIA would consider it rather perverse that an investor taking, say, a 5% share in a consortium would be subject to a mandatory notification obligation, when if it was acquiring that stake independently and separately, it would not be so subject.

2.8 A related point is whether the Government, in carrying out its screening process and national security assessment, would only consider those members of an investment consortium which would hold either an effective 15% or more stake in, or material influence over, the relevant business, or would consortium members with lower stakes also be considered? If the latter, the Government should explain why this is necessary given such investors would not seem to satisfy the trigger event risk threshold.

2.9 **Definition of control.** GIIA would also welcome clarification on the intended application of clause 8(6) of the NSI Bill, which sets out the "third case" in which an acquisition of control will be deemed to have occurred, and therefore in which a mandatory notification obligation may arise. First, is it intended that any entity which *de facto* has the ability to secure or prevent the passage of any class of resolution governing the affairs of the entity will be caught (for example, a 14.9% stake might in practice be sufficient to block a special resolution in certain listed companies)? If so, this would indicate that material influence could give rise to a mandatory notification, which is not understood to be the intention. Of more frequent relevance, GIIA would point out that shareholder agreements often provide investors with direct or indirect veto rights over certain matters, which would not give rise to decisive influence for EU merger control purposes or material influence for UK merger control purposes (for example, traditional minority protection rights such as a requirement for 90% of votes to resolve to wind up the company). If such minority rights are counted as the right to prevent a class of resolution, a financial investor obtaining a minority protection right would be caught by this. Assuming this is not the intended effect (it should not be), this needs to be made clear in the wording of the final Act.

2.10 **Parameters for timing of notifications and related publicity.** Other than the obligation in the Bill to obtain clearance for a notifiable acquisition before it is effected, there is currently no guidance as to the point in a transaction at which a mandatory notification can be made. GIIA notes that it may be advantageous for parties to obtain a clearance for their proposed transaction, or at least to commence the notification process, in advance of publicity being given to the transaction and potentially in advance of any binding agreement being in place. Guidance as to whether notifications can be made at a stage before transaction agreements are signed (e.g. on the basis of heads of terms or a letter of intent, or indeed before that) would be welcomed. This is the case for merger filings under both UK and EU merger control. This issue is however related to how much publicity will be associated with notifications and the clearance process. The extent to which the notification process is confidential, at least until decision, would impact the willingness of parties to approach the Government for clearance early.

2.11 **Stop the clock powers.** GIIA welcomes the fact that the "stop the clock" powers envisaged by clause 24 of the NSI Bill only apply to information notices issued following the issue of a call-in notice and not during the initial screening period. However, in the context of a regime

where the assessment period is already quite long (up to 75 working days for a national security assessment, on top of the initial 30 working day screening period, and with the possibility of further voluntary extensions), GIIA considers that it is not appropriate for the time limits to automatically pause as soon as questions are raised by BEIS. GIIA believes that stop the clock powers should only apply if responses are not provided to questions within a reasonable period set by BEIS when sending the questions, for example, three or five working days, depending on the complexity of the questions.

2.12 **Crucial importance of informal advice.** GIIA's understanding is that it is not the Government's intention to grant "pre-clearances". This refers to the possibility, which is available under the Australian foreign investment regime, for the Government to confirm that it would not commence a full national security assessment in relation to any investors participating in an auction process (or indeed, confirm that for only some of them). Assuming that is the case, GIIA observes that informal advice will be absolutely crucial for investors, particularly in the earlier years of the regime, and indeed, in the run-up to the regime coming into effect.

2.13 To be clear, by informal advice, we do not mean guidance as to the information that BEIS would require in the context of a notification for a specific transaction. Whilst such guidance should certainly be available, this is more in the nature of "pre-notification discussions" than informal advice. By informal advice we mean guidance in advance of a potential transaction being agreed as to whether the transaction would be likely to raise national security concerns. This should include the ability for buyers to discuss whether particular consortium partners would be likely to raise possible concerns, and the ability for sellers in an auction process to clarify whether certain possible buyers would be likely to raise national security issues. It should also encompass guidance to investors as to whether they are likely to raise national security issues in general, regardless of the transaction in question.

2.14 Such informal advice would of course not be binding on the Secretary of State, but it would need to be reliable such that it would only be departed from rarely and with good reason. If such confidential conversations cannot be had in the absence of particular transactions and at the early stages of particular transactions, this will hugely complicate the process of putting together consortia for acquisitions, particularly in the context of auction processes (as noted above, acquisitions of the types of infrastructure businesses caught by the proposed mandatory regime are very often made by consortia consisting of a number of investors rather than individual buyers). This would make investing into the UK more complicated and less attractive. It would also be likely to lead to a large number of unnecessary voluntary notifications, particularly in the early years of the new regime. GIIA therefore urges the Government to confirm that informal advice (and not merely pre-notification discussions) will be available and to set out in guidance the process for obtaining such advice.

2.15 **Publication of decisions**. GIIA understands that it may be the Government's intention not to publish its national security assessment decisions where unconditional clearance is given, with only prohibition decisions and clearance decisions subject to remedies being published. GIIA considers that this would be an undesirable position as the Government expects there to be only around 10 decisions a year which involve remedies. Not publishing unconditional clearance decisions following a national security assessment will lead to a lack of certainty for investors as to the types of situation that are considered unproblematic by the Government, particularly in the early years of the new regime. The lack of precedent decisions would also be likely to increase the number of unnecessary voluntary notifications. Accordingly, save where strictly necessary for national security reasons, both the fact of unconditional clearance after a national security assessment, and the decision itself, should be published (redacting any sensitive information). However, this should only occur after the relevant transaction has been publicised, or alternatively closed.

3. RESPONSE TO CONSULTATION QUESTIONS

3.1 Before commenting on the specifics of the communications, data infrastructure, energy and transport sectors, GIIA notes that each of these sectors is currently subject to cybersecurity regulation pursuant to the Network and Information Systems Regulations 2018 (SI 2018/506) ("**NIS Regulations**"). The NIS Regulations contain a definition of an "operator of an essential service" or "**OES**".

3.2 The Government explains that the NIS Regulations (see: https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018):

> '*…provide[s] legal measures to boost the overall level of security (both cyber and physical resilience) of network and information systems that are* ***critical for*** *the provision of* ***digital services*** *(online marketplaces, online search engines, cloud computing services)* ***and essential services (transport, energy****, water, health, and digital infrastructure services)*' (emphasis added).

3.3 GIIA notes that the definitions of OES for the energy sector in the NIS Regulations bear some similarity to some of the proposed definitions for the NSI Bill mandatory regime, in particular as regards some of the thresholds used (albeit this is not always the case, as we note below). In contrast, none of the thresholds used in the NIS Regulations for the digital infrastructure subsector have found their way into the proposed definition for the communications sector for the proposed NSI Bill. Lower thresholds are also used for the transport sector. As we note below, it seems clear that each of the four sectors has been defined overly broadly in the consultation, but this is particularly true for the communications and data infrastructure sectors for which no thresholds are provided. Given that the thresholds in the NIS Regulations were self-evidently intended to capture only those businesses which are genuinely essential for (cyber) security purposes, it is not obvious why a much wider approach is needed for the NSI Bill. We comment on this further in each of the communications and data infrastructure sections below.

3.4 <u>Communications</u>

The Government explains[2] that its policy objective for the NSI Bill is to "*provide updated powers to comprehensively scrutinise and intervene in investment to protect national security".* The Government then proposes very broad definitions for the communications sector, based on definitions found in the Communications Act 2003.

For the reasons explained further below, GIIA submits that the proposed Communications Act 2003 definitions, originally designed in the context of very different policy objectives, are far too broad and would catch thousands of businesses that should raise no national security concerns whatsoever.

GIIA respectfully suggests that the Government should instead use the pre-existing statutory definition for the communications sector of OESs from the NIS Regulations. This definition was drafted to achieve national cyber-security objectives and would provide more appropriate and proportionate definitions for the communications sector in the NSI Bill. If the Government remains concerned that such an approach might miss businesses which could raise national security issues (despite the fact they are not considered to raise cyber security issues), we also set out below a suggestion for supplementing the NIS Regulations definition with the power for the Secretary of State to designate additional entities on the advice of GCHQ.

In addition to the NIS Regulations definitions including major telecoms networks and international cable landing stations, we note that the following services (mentioned in the

[2] Page 5 of the consultation.

Government's NSI Bill consultation) are explicitly within the scope of the NIS Regulations definitions - see paragraph 10 of Schedule 2 to the NIS Regulations:

- Top-level domain name registries (more than 2 billion queries on average in 24 hours);
- domain name system service providers (more than 2 million requests per 24 hours on average or hosting more than 250,000 active domain names); and
- internet peering point (or Internet Exchange Point) operators with more than 50% market share.

GIIA Proposed definition

GIIA proposes the following revised definition for the communications sector in the NSI Bill:

"1. An entity carrying on activities in the United Kingdom which is:

a. deemed designated as an OES pursuant to paragraph 8(1) of the NIS Regulations and notified to the Office of Communications pursuant to paragraph 8(2) of the NIS Regulations; and/or

b. designated as an OES by the Office of Communications pursuant to paragraph 8(3) of the NIS Regulations; and/or

c. any other entity designated by the Secretary of State following consultation with GCHQ."

We respectfully submit that this definition, based on existing legislative definitions, will better achieve the Government's policy objectives than the overly broad definition currently proposed.

Why the Communications Act definitions are inappropriate

The Communications Act 2003 implemented into UK law the 2002 European Telecoms Regulatory Framework, which itself built on EU liberalisation and harmonisation regulatory measures dating back to 1997. The definitions of '*electronic communications network*', '*electronic communications service*' and '*associated facilities*' were deliberately drafted to be very broad in order to facilitate market liberalisation and entry. In particular, in parallel to the harmonising 1997 EU telecoms regulatory ('*Open Network Provision*') framework, the EU legislated to remove '*special and exclusive rights'* in the communications sector that had previously been granted to state owned monopolies and precluded market entry to the sector. Following the abolition of special and exclusive rights in the sector in 1996, the 2002 European Telecoms Regulatory package for the first time provided (by means of the Authorisation Directive 2002/20/EC) that entities were able to provide electronic communications networks and/or services and associated facilities without needing a prior licence or authorisation.

As a result, many thousands of companies fall within the scope of the definitions proposed by the Government in the NSI Bill. By way of non-exhaustive example, as drafted any entity **in any sector** with an internal private branch exchange or internal telecoms network would fall within the scope of the proposed definition. Indeed, the Government has recognised in the consultation that the definition captures "*a very wide range of private communications networks, many of which will not present national security concerns*."

To the extent that the Government is not persuaded by our proposal to base the definitions for the Communications sector on OESs it is suggested that the definition is instead narrowed in the following ways:

1. *"An entity carrying on activities in the United Kingdom which satisfies both sections (a) and (b) set out below:*

a. its activities in the United Kingdom consists in or include:

(i) *providing a **public** electronic communications network;*

(ii) *providing a **public** electronic communications service;*

(iii) *making available facilities that are associated facilities by reference to a **public** electronic communications network or a **public** electronic communications service; and*

b. pays an annual administrative fee to Ofcom above a threshold specified by the Secretary of State from time to time.

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."

Key elements of this revised definition are:

- to restrict it to **'public'** electronic communications services and networks. This will remove self-provision of networks (by companies in *any* sector) from its scope; and
- to restrict the definition to companies that pay Ofcom an annual fee (at a level to be specified by the Secretary of State). This will include (*inter alia*):
    - all holders of individual spectrum licences (including all mobile operators);
    - major fixed telecoms companies; and
    - holders of Code Powers that build and operate:
        - national and international fibre infrastructure;
        - mobile phone masts; and
        - broadcast transmission infrastructure.

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?

Please see comments above.

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

No comments.

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?

GIIA has no doubt that the proposed definitions cover the areas of the economy where foreign investment has the greatest potential to cause national security risks. As set out above, GIIA's concern is rather that the proposed definition is far too broad, as the Government itself acknowledges. GIIA's proposals for reducing the scope appropriately have been set out above.

In addition, we note that:

- the definition of 'electronic communications service' will be expanded by the implementation of the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020, which will expand the definition to include "internet access services" and "interpersonal communications service", thereby further extending the scope of the currently proposed definition.

- The inclusion of "associated facilities" makes the proposed definition extremely wide. The rationale for this inclusion is stated to be to ensure the inclusion of certain businesses, such as those providing sub-sea fibre optic cables and services, the associated telecoms supply chain and digital infrastructure companies, etc. However, the current definition is likely to capture a much wider range of facilities beyond those specifically referred to in the rationale. For example, it must be unnecessary to include in the scope of the mandatory regime *every* business which forms *any* part of the telecoms supply chain, e.g. providers of *any* components or equipment, regardless of importance or potential to be used for disruptive or destructive actions, espionage, or to exert leverage. Some form of materiality threshold needs to be introduced.

- Much of the infrastructure and equipment which would be caught by the current definition is entirely "passive" with no real potential to be used for hostile purposes. Telecoms towers (particularly where these are not essential for mobile phone operators) are just one such example. A clear carve-out for such passive infrastructure would be appropriate.

The alternative definitions proposed and set out above seek to limit the definition to capture only those entities which have a reasonably prospect of posing a national security risk in hostile hands and exclude, in particular, smaller, private players unless and until they expand to become caught by the existing regulatory regimes referred to above.

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?

- GIIA considers that it would be appropriate to have a more narrowly defined scope for the mandatory notification regime, covering only those businesses which are genuinely likely to raise national security issues if they fall into hostile hands. The Government will of course have use of the call-in power for transactions that are outside the scope of the mandatory regime. The mandatory regime therefore does not need to pick up every conceivable possible issue, and we propose above a number of alternative approaches which would be more appropriate in scope.

- Further, as explained in section 2 above, we would urge the Government to introduce, as a priority, exemptions for infrastructure investors which have a long history of investing in communications infrastructure and have not been considered to pose national security risks in the past.

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?

- For the reasons stated above, at present the proposals place too heavy a burden on businesses and investors as the definitions are too broad. GIIA believes strongly that it would be possible to narrow the scope of the definitions without compromising national security, including in light of the Government's call-in power. The mandatory regime should only be used for acquisitions of businesses which are

genuinely likely to raise national security issues if they fall into hostile hands. Our proposals for how the definitions could be narrowed are set out above.

Sector specific questions

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?

As explained above, the proposed definition is too broad.

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

The question comes close to restating the proposed definition. For the reasons set out above, we do not think that is the right question (or definition).

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

We suggest that private networks (which are only used for self-provision) are excluded from the scope of the mandatory regime under the NSI Bill. We have suggested drafting to this effect above.

3.5 **Data Infrastructure**

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?

In contrast to the Communications sector, with the exception of the data protection and e-privacy rules (which are not relevant for the NSI Bill), the data infrastructure sector is largely unregulated, except where it is within the scope of communications sector regulation.

In that regard, we note that all of the following are already within the scope of the Government's proposed definition for the Communications sector above (and also our proposed revised drafting set out above):

- peering by public communications providers;
- major international cabling routes; and
- software defined networking and network functional virtualisation (in the context of an electronic communications network and/or service).

We note that paragraph 3 of the proposed Data Infrastructure definition goes some way to adopting the approach of the existing NIS regime. However, as drafted, the proposed definitions do not fully adopt the NIS Regulations approach and so they are disproportionately broad in scope as a result. GIIA therefore sets out our proposals for improving the definition below.

GIIA respectfully suggests that, mirroring our proposal for the Communications sector, the Government could use the pre-existing statutory definition for OES from the NIS Regulations to define the parameters of companies within the scope of the NSI Bill in the data infrastructure sector. Given these definitions were drafted to achieve national (cyber)security objectives, they again provide more appropriate and proportionate

definitions for the NSI Bill. As above, to ensure that nothing is missed, we suggest that this narrower definition could be supplemented with the power for the Secretary of State to designate additional entities on the advice of GCHQ.

Finally, given the scope for potential overlap between this sector and the Communications sector, we suggest that further consideration is given to either merging the two sectors or alternatively ensuring that there is no overlap and that e.g. international cables, peering, DNS, etc are dealt with in one definition or the other, but not in both.

GIIA comments on proposed definition

To the extent that the Government is not persuaded by our submission to base the definitions for the Digital Infrastructure sector on OESs we suggest that the proposed definition is narrowed in the following ways:

- the geographic scope of entities in paragraph 1 should be restricted to entities in the UK;

- specialist or technical services for the purposes of paragraph 1(c) will need to be defined more specifically. The definition currently provides that this "may" include, depending on the context, various services. The non-exclusive list of example services and the use of "*could access relevant data on the Relevant data infrastructure*" leads to ambiguity as to what falls within this category. This is insufficiently precise for a mandatory regime. There needs to be no room for doubt as to what is caught by a mandatory regime backed by very significant sanctions;

- the inclusion of paragraph 1(e) would include any software provider or developer which merely has a use case of providing virtual access. This is very broad and we would suggest that the threshold trigger should be actual use rather than just design. We also query whether the risk presented by such software developers or providers is covered through the scope of paragraph 1(d);

- in the definition of '*Relevant data infrastructure',* references to peering and international cable routes should be removed on the basis that these are covered in the communications sector definition, (or alternatively these should be carved out from the communications sector definition);

- in the definition of '*Relevant Data':*

    - the references to 'operation of essential services' should be linked to those deemed designated OESs or designated OESs pursuant to paragraphs 8(1) and 8(3) of the NIS Regulations (see detailed drafting in our Communication sector text above);

    - if this change is not adopted, then it seems that the Relevant Data definition relates back to entities that fall within the mandatory notification regime (i.e. the other 16 categories under the NSI Bill). These include some general IT industries – such as AI and Computing Hardware. Depending on how these other industry categories are scoped, the definition of Relevant Data in the context of these industries could be unintentionally broad. It will be important to read the definition of Relevant Data carefully alongside the guidance for these categories.

- in the definition of '*Privileged access'* it is unclear whether access rights for inspection purposes pursuant to a lease on a site where an investor is the landlord would be caught by this definition. We suggest that the drafting is clarified to ensure that such rights are not covered by the mandatory regime;

- the definition of '*peering'* is not clear: a better definition is that of 'IXP' in paragraph 10(5)(c) of Schedule 2 to the NIS Regulations. In any event, as discussed above in our communications sector comments, IXPs would be included if definitions for the communications sector based on the NIS Regulations are used.

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

- See our comments in response to Question 1.

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?

- We note the definition of Relevant Data appears to be limited by paragraph 3, in that it only applies to data used for essential services or business continuity of an entity which falls within the mandatory regime (i.e. within one of the defined 17 sectors). GIIA welcomes this limitation, but nevertheless considers that the scope is too broad for a mandatory regime in that it will or may capture businesses which are not genuinely like to raise national security issues. As noted above, we therefore suggest that this is linked to the pre-existing NIS Regulations regime which was introduced to address national cyber-security concerns.

- The lack of clarity regarding those providing security, equipment installation, and repair and maintenance services for the purposes of paragraph 1(c) has been noted above. The related point is that it must be the case that some of those providing such services would only very rarely, if at all, raise potential national security issues. For example, the apparent suggestion that any business which provides security services to control and monitor physical access to a site where relevant data infrastructure is located may be within the scope of the mandatory regime must surely be too broad for a mandatory regime. The definition should apply only to certain companies with material activities in specific sensitive sectors or should be linked to a list of particular sensitive locations for national security in which a company might have activities. In the vast majority of cases, it is very unlikely that physical security companies would raise national security issues, and GIIA would suggest a power to intervene in acquisitions of such entities should be reserved for the call-in regime.

- GIIA also notes that the limited definition of Relevant Data is only relevant for the first limb of Relevant data infrastructure. As a result, data of entities falling outside the mandatory regime would seem to be captured by those parts of the definition. Is this necessary?

- We note that, as drafted, there is significant overlap between the proposed definitions relating to Data Infrastructure and Communications sectors. We suggest that these overlaps are removed and/or clarified.

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?

- GIIA considers that it would be appropriate to have a more narrowly defined scope for the mandatory notification regime, covering only those businesses which are genuinely likely to raise national security issues if they fall into hostile hands. The Government will of course have use of the call-in power for transactions that are outside the scope of the mandatory regime. The mandatory regime therefore does not need to pick up every conceivable possible issue.

- Further, as explained in section 2 above, we would urge the Government to introduce as a priority exemptions for infrastructure investors which have a long history of investing in data infrastructure and have not been considered to pose national security risks in the past.

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?

- Paragraph 1(b) of the definition is itself reasonably broad and brings landlords (including the ultimate freeholder) of a site or building used to house Relevant data infrastructure into scope. Given this is not qualified around enabling access to Relevant Data (which the guidance note suggests is the core criteria), GIIA's view is that it is not clear what this part of the proposed definition is trying to protect against.

- Point 2(d) of the definition of Relevant Data Infrastructure is not linked to Relevant Data. Therefore, any physical or virtualised infrastructure which employs either software defined networking or network functions virtualisation would fall within scope. As we understand it, private enterprises can deploy software defined networking in their IT architecture, so this seems too broad. The use of software defined networking or network functions virtualisation should be linked back to use in connection with Relevant Data.

- For the reasons stated above, at present the proposals place too heavy a burden on businesses and investors as the definitions are too broad. GIIA believes strongly that it would be possible to narrow the scope of the definitions without compromising national security, including in light of the Government's call-in power. The mandatory regime should only be used for acquisitions of businesses which are genuinely likely to raise national security issues if they fall into hostile hands.

Sector specific questions

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.

See comments above.

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?

No comments.

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?

No comments.

22. We would like to understand existing approaches to managing the national security risks to relevant data and relevant data infrastructure. In particular, how 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?

No comments.

3.6 **Energy**

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?

GIIA's view is that there are aspects of the Government's definition of the Energy sector which are not sufficiently clear to enable our members to self-assess whether a notification would be required.

- Paragraph 1(e) refers to long range gas storage and Gas Reception Terminals, neither of which are defined. It is also unclear how it would be determined whether a particular interconnector, storage site or gas reception/LNG terminal contributes to security of supply. Some sort of volume threshold would seem to be appropriate. In this regard, we note that the NIS Regulations provide volume thresholds for interconnectors (1GW/20 million cubic metres of gas per day), gas storage facilities and LNG facilities (both 20 million cubic metres of gas per day), and GIIA would suggest that these should be used as a minimum. This assumes that the contribution to security of supply point is intended to apply to interconnectors and storage projects, as well as gas reception terminals, which is also unclear. It is also unclear how paragraph 1(e) inter-relates to paragraph 1(b) insofar as it relates to gas storage sites.

- Paragraph 1(f)(iii) refers to "affiliated undertaking" but such term is not defined. In particular, is it intended to relate to generation activities of the acquirer? If so, would it cover activities of any consortium member acquiring a relevant business or only some of them?

- Paragraph 1(g) refers to companies who "provide or handle" 500,000 tonnes per annum of petroleum-based road, aviation or heating fuels. Again, the language is vague and it is unclear if the term "provide" is intended to mean "supply" or "sell" or "transport". It is also unclear how the first part of (g) is intended to inter-relate to the second part relating to downstream facility owners. For example, are (i) to (v) only applicable to downstream facility owners? Is supply (first part of definition) considered to be distinct from distribution or delivery (points (iv) and (v))? If so, how?

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

See comments in response to Question 1.

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?

- Generally, GIIA notes that the rationale for the Energy section only refers to a desire to include energy networks, the oil sector, power generation and new technologies like battery storage. However, the proposed definition is broader than that;

capturing energy suppliers, importation and storage projects and LNG terminals amongst others. If the Government does not consider that such activities are likely to raise national security issues if they were to find themselves in hostile hands, they should be removed from the scope of the mandatory regime, with any possible concerns being dealt with under the voluntary regime.

- Paragraph 1(a) of the definition currently includes in its scope any entity which owns or operates terminals, upstream pipelines or infrastructure forming part of a petroleum production project with a throughput of greater than 3,000,000 tonnes of oil equivalent per year. Although we note this is a threshold used in the NIS Regulations, this nevertheless seems a little low, bearing in mind it represents approximately 3% of the UK's total petroleum production. This is a relatively low threshold that would surely capture a number of entities where investment would not have the potential to cause national security risks. GIIA would suggest a value based on 5% of the UK's production might be more appropriate.

- Paragraph 1(c) refers to energy distribution and transmission networks that deliver secure, reliable electricity and gas to customers. GIIA understands the rationale for inclusion of this type of business. We would however question whether every independent gas transporter (IGT), independent electricity distribution network operator (IDNO) and offshore transmission operator (OFTO) ought to be included. Many IGTs and IDNOs will have a small number of connections and would therefore seem to be more appropriately caught by the call-in regime. Some OFTOs would also seem to be unlikely to raise significant national security issues. GIIA notes that the NIS Regulations set a threshold for OES status for transmission and distribution system operators linked to a potential to disrupt delivery of electricity/gas to more than 250,000 customers. Similarly, a 2 GW threshold is provided for OFTOs. GIIA would suggest that these thresholds are adopted as a minimum in the mandatory NSI regime.

- Paragraph 1(d) refers to energy suppliers with a significant customer base, which is defined as 250,000 customers. It is unclear to GIIA why suppliers are likely to raise national security issues given they are not responsible for actually delivering energy to homes and businesses (this responsibility lies with the network companies). In any event, a threshold of 250,000 customers seems relatively low (GIIA understands that it would currently capture 10 suppliers). Given the Supplier of Last Resort regime, it seems very doubtful that all of these 10 suppliers ought to be seen as raising national security risks.

- In any event, paragraph 1(f)(i) seems to provide that any electricity undertaking carrying out the function of supply is captured. In other words, every single electricity supplier would seem to be captured and the threshold in 1(d) would seem to be redundant for electricity suppliers (which will effectively make it redundant for gas suppliers also given that electricity suppliers typically also supply gas). This surely cannot be what is intended given that smaller suppliers cannot be thought to raise significant national security issues.

- The 100 MW threshold in para (f)(ii) seems very low. We believe it accounts for only 0.1% of the total installed UK electricity generation capacity in 2019 of 103.1 GW.[3]We note that the NIS Regulations use a threshold of 2 GW, which would seem more appropriate as a minimum.

- To the extent that paragraph 1(f)(iii) is intended to capture aggregation of the Target's activities with those of the buyer and its affiliates (as noted above, this is

[3] See page 29 of https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/904503/UK_Energy_in_Brief_2020.pdf

not currently clear), this would seem to mean that an acquisition by an entity which already had 2GW of generation of any generation business whatsoever would seem to be captured. Is this intended? If so, that goes too far and there should be a capacity threshold for the Target business only; a suggestion for this would be 1GW of additional generation.

- The 500,000 tonne and (in particular) 20,000 tonne thresholds used in paragraph 1(g) both seem low when compared to our understanding that UK refineries produced over 58 million tonnes of product in 2018.[4]

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?

- GIIA considers that it would be appropriate to have a more narrowly defined scope for the mandatory notification regime, covering only those businesses which are genuinely likely to raise national security issues if they fall into hostile hands. The Government will of course have use of the call-in power for transactions that are outside the scope of the mandatory regime. The mandatory regime therefore does not need to pick up every conceivable possible issue.

- GIIA again reiterates our call for prompt exemptions for infrastructure investors which have a long history of investing in the UK energy sector and have not been considered to pose national security risks in the past.

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?

- At present the balance creates too heavy a burden on businesses and investors for the reasons set out above.

3.7 **Transport**

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?

- In paragraph 1, the term "passengers" is not defined. In particular, is this only intended to refer to passengers on vessels operating predominantly or significantly as passenger vessels, or would passengers on vessels operating predominantly as cargo vessels also count?

- The definitions of the term "operates" in paragraph 2 is unclear ("to control the functioning of a machine, process or system"). Presumably it is not intended to cover any entity that operates *any* machine, process or system at a port/harbour? If so, it may cover e.g. logistics companies or other small entities which conduct a small part of the relevant port's operations.

- In paragraphs 5(c) and 6(d), it is unclear what the difference between a holding company and a parent company is.

[4] See page 51 of ***https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840015/DUKES_2019_MASTER_COPY.pdf***

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

See comments in response to Question 1.

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?

- It is appropriate to frame the definition to apply only to ports/harbours, airports and air traffic control sectors.

- However, GIIA would question whether it is appropriate to capture all 51 "major ports". Would ownership of *any* of those ports by a hostile actor really raise potential national security issues? We note that the NIS Regulations determine whether a port facility or harbour authority is an OES by reference to percentages of total UK traffic, with the lowest percentage being 10%. This would seem to be a more appropriate approach.

- With respect to airports, it is unclear why the Government has taken a threshold of 6 million passenger movements when the NIS Regulations refer to 10 million. Consistency with the NIS Regulations would again seem to be appropriate.

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?

- GIIA would again emphasise the need for exemptions for infrastructure investors which have a long history of investing in the UK transport sector and have not been considered to pose national security risks in the past.

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?

- See comments above.