Department for Digital, Culture, Media & Sport

National Security and Investment Bill

Introduction and consultation

16/11/2020 - TechUK

National Security and Investment Bill

What is it?

- The NS&I Bill was introduced to Parliament on 11 November.
- The bill will strengthen the Government's powers to **scrutinise and intervene in transactions** to protect national security, while **providing businesses and investors with certainty and transparency**.
- Many of the key changes introduced in the Bill are **consistent with the requirements of existing investment screening regimes in like minded countries**. As a result, many international investors will already be familiar with these kinds of requirements.
- **Mandatory notification of some transactions in key sectors** will ensure that the Government is automatically informed of potential transactions in these crucial areas, and able to take action accordingly to investigate and mitigate any national security risks.
- A **voluntary notification** system which is intended to encourage notifications from parties who consider that their trigger event may raise national security concerns.
- The Government will also retain a **power to proactively examine any transaction across the economy that may present national security risks**, even where notification is not mandatory.

National Security and Investment Bill

Why has it been introduced?

- The NSI Bill aims to **modernise the UK's investment screening regime**, bringing us more in line with the regimes of likeminded allies and partners around the world.

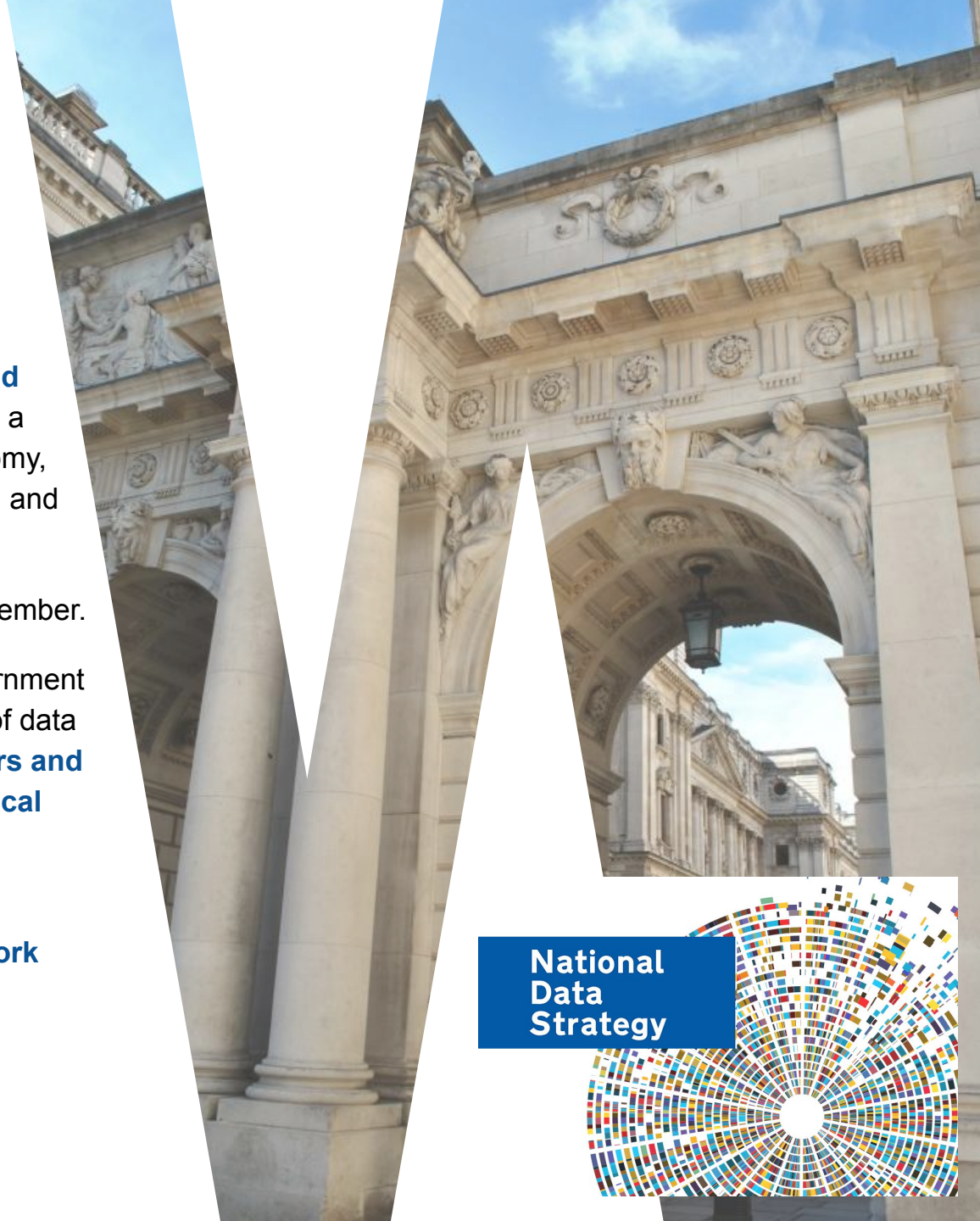
- The fundamentals of the UK as an international investment destination remain as strong as ever. **An open approach to international investment must include appropriate safeguards** to protect our national security and the safety of our citizens.

- The Government's powers to scrutinise transactions date from the Enterprise Act 2002. Technological, economic and geopolitical changes mean that reforms are required to **address the new and emerging national security challenges we face**.

- The Government has been clear for a number of years about its intention to introduce new powers in this area and **as we rebuild from COVID-19** where sensitive British businesses may be vulnerable, we must go further and ensure that the Government can intervene in any deal that raises national security risks.

- We are **committed to working with investors to provide clarity and certainty** around the requirements of this Bill, and welcome broad responses to the consultation.

- The **National Data Strategy (NDS)** is the framework for the action this government will take on data. The strategy is ambitious and pro-growth, placing the availability of data and confidence in its use at its heart.
- The NDS sets out the **government's commitment to ensuring the security and resilience of our data infrastructure**. It is a vital national asset that supports our economy, delivers public services, and drives growth, and we need to protect it appropriately.
- The **NDS consultation** is open until 2 December.
- The NS&I bill is just one way that the government will strengthen the security and resilience of data infrastructure, **provide confidence to users and enable the continued growth of this critical sector**.
- The NDS will also provide **coherence and impetus to the wide range of data-led work across government**.



National Security and Investment Bill

Who is captured and why - Data Infrastructure

- **Data infrastructure is one of 17 mandatory sectors in the bill.** This reflects that data is now a key driving force of the world's modern economies.
- **Data Infrastructure underpins our modern use of data**. It provides the ability to store, process and transfer data. The Government has a responsibility to ensure that data and its supporting infrastructure is secure and resilient in the face of established, new and emerging risks.

- **National security risks to data infrastructure** can arise where an entity's activities give it access to data via physical or virtualised infrastructure used to store large volumes of sensitive data and/or to facilitate connectivity.
- Such access could be achieved through ownership, management or control of key data infrastructure, or by the provision of certain technical services to such infrastructure.

- The **draft sector definition** addresses these scenarios.
- We have used the definitions of *relevant data* and *relevant data infrastructure* to ensure that the scope is focused on the activities that pose national security risks.

What this means for the Data Infrastructure sector

Notification

- Transactions from entities in a mandatory sector, which meet the minimum threshold for trigger events, will need to notify.
- This will ensure that the Government is automatically informed of potential transactions in these areas, and able to take action accordingly to investigate and mitigate any national security risks.
- Transactions subject to mandatory notification will not be allowed to proceed without Government approval - any deal that is not notified will be automatically void in law.
- A voluntary notification system will also be introduced and the Government will retain a power to proactively examine any transaction across the economy that may present national security risks, even where notification is not mandatory.
- For the first time, timelines for assessments will be set out in law and not set by the Government on a case-by-case basis. This offers greater certainty for business.

What this means for the Data Infrastructure sector

Sanctions

- The regime will be underpinned by civil and criminal sanctions, creating effective deterrents for non-compliance with statutory obligations.
- Sanctions for non-compliance with the regime include fines of up to 5% of worldwide turnover or £10 million – whichever is the greater – and imprisonment of up to 5 years.
- The new regime will be subject to judicial oversight, so parties will have the right to challenge decisions in the courts.
- The majority of transactions across the economy will be unaffected by these new powers. This new approach represents a proportionate response to the fraction of transactions that do raise national security threats, giving the Government the requisite powers to combat them.

Public consultation

- The consultation document sets out the Government's **proposed definitions** for the types of entity within each sector that could come under the Bill's mandatory regime.

- Responses to this **consultation will be used to refine the definitions** so they provide enough clarity to allow parties to self-assess whether they need to notify.

- The **final definitions will be put into secondary legislation**, which the Government intends to introduce in time for commencement of the Bill in 2021.

Invitation to respond to consultation on the definition

A primary purpose of the definition is to capture entities that have a significant ability to impact national security. We want to understand if, for this purpose, the definition has appropriate coverage – specifically, on operating models, on the provision of technical services, and virtualised services.

We welcome industry engagement during the consultation process to develop and refine this further.

1. 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:
   a. the various operating and ownership models within the data infrastructure sector;
   b. the provision of technical services to relevant data infrastructure; and
   c. and the provision of virtualised services to relevant data infrastructure.

2. 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?

Invitation to respond to consultation (continued)

3. How many businesses provide the following services to relevant data centres, and what proportion of their overall business is the sector likely to constitute:

a. security services;
b. installation/maintenance/repair services; and
c. virtualised services?

4. We would like to understand existing approaches to managing the national security risks to relevant data and relevant data infrastructure. In your response, we are particularly interested in 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.

+ general questions for all sectors on clarity, accuracy, burden on business and other suggested ways to screen relevant transactions.

How to respond to the consultation

Issued: 11 November 2020

Respond by: 6 January 2021

Enquiries to: nsisectorconsultation@beis.gov.uk

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

Or respond by email to:
nsisectorconsultation@beis.gov.uk

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

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

Department for Digital, Culture, Media & Sport

Any questions?

investment.screening@beis.gov.uk