National Security and Investment bill

Key information for Data Infrastructure sector

Draft definition and policy rationale

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

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

We welcome industry input on the draft data infrastructure definition via the consultation process.

DEFINITION STARTS

1. An entity that:
    a. owns or operates *relevant data infrastructure* or manages *relevant data infrastructure* on behalf of other entities, or
    b. owns the site on or building in which *relevant data infrastructure* is located, or
    c. through the provision of specialist or technical services to entities in 1 or 2, could access relevant data on relevant data infrastructure. Depending on their operation, this may include:
        i. security services controlling and monitoring physical access to the site where the relevant data infrastructure is located, or
        ii. equipment installation services, installing the relevant data infrastructure, or
        iii. equipment repair and maintenance services in respect of the relevant data infrastructure
    d. provides services which give it privileged access to virtualised relevant data infrastructure
    e. produces or develops software designed for use in the services in paragraph (1d).

2. ***Relevant data infrastructure*** means physical or virtualised infrastructure which:
    a. hosts, stores, manages or processes or controls or transfers *relevant data;* or
    b. is used by Public Communications Providers for *peering*; or
    c. connects any major international cabling routes; or
    d. employs software defined networking or network functions virtualisation

3. ***Relevant Data*** *means data used for the operation of essential services or business continuity of any entity that falls under the mandatory notification regime of the National Security and Investment regime.*

4. ***Privileged access*** *means physical, logical and/or administrative access, where such access would otherwise be restricted or compartmented without such privileged access. Privileged access includes editing rights and/or configuration rights.*

5. ***Peering*** *means the exchange of data directly between [Public Communications Providers], rather than via the internet*

DEFINITION ENDS

Consultation questions for Data Infrastructure sector

Sector-specific questions

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. 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?

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. a landlord/site owner's access to a data infrastructure facility that is owned or operated by a different entity;
    b. a third party service provider (such as security, installation, maintenance) having access to data infrastructure facilities and sensitive data;
    c. a third party virtualised service provider having access to data infrastructure or sensitive data.

General questions for all sectors

1. Are the sector definitions sufficiently clear to enable investors and businesses to self-assess whether they must notify and receive approval for relevant transactions? If not, how can the definitions be improved?
2. To what extent are technical and scientific terms correct and sufficiently clear and commonly understood for the purposes of determining relevant activities?
3. To what extent do these definitions include the areas of the economy where foreign investment has the greatest potential to cause national security risks?
4. How else, aside from mandatory notification under the NSI regime, can the Government ensure relevant transactions receive appropriate screening while minimising the impact on business?
5. Do these definitions strike the right balance between safeguarding national security and minimising the burdens placed on businesses and investors? Is it possible to narrow the scope of the definitions without compromising national security?

Useful links

Bill overview page (including factsheets and consultation documents).
Secretary of State's statement of policy intent.