Cooley

UK Government Publishes National Semiconductor Strategy

June 6, 2023

On 19 May 2023, the UK Department for Science, Innovation and Technology published the National Semiconductor Strategy, setting out the UK's 20-year vision to grow deep foundations in semiconductor technology, while also bolstering the UK's national security and resilience in an industry that has suffered supply chain issues and geopolitical tensions.

Below we examine some of the key aspects of the strategy and their implications on the semiconductor sector.

1. Growing the domestic sector

The strategy recognises the importance of semiconductor technology to the growth of the UK economy and sets out several ambitious initiatives to achieve growth in the industry, including investments of up to £1 billion over the next decade, increased support for new semiconductor startups through a dedicated incubator programme, and development of training, research and education in semiconductor-related fields.

However, questions remain regarding whether the planned initiatives go far enough to ensure that the UK semiconductor industry keeps apace with other jurisdictions. For example, when compared to other regimes, the £1 billion investment pales in comparison to the proposed US investment of $52 billion and the European Union investment of 43 billion euros into semiconductor technology. Ultimately, the impact of the UK government's investment will depend on how the funding is allocated and applied, which currently is not detailed in the strategy.

2. Protecting national security

The strategy clearly demonstrates the increasing importance of national security in the development of industrial policy in the UK, as well as the changing nature of threats posed to UK interests.

The strategy defines semiconductors as 'a class of materials which are used to create the hardware that underpin electronic devices ... they are the basis upon which integrated circuits, or computer chips, are built. They are also used in discrete devices, such as those involved in power management, radio frequency, lasers and sensors'.

The strategy highlights that while semiconductors are critical to UK national security, they also give rise to several risks. In particular, the strategy focuses on two main areas of risk – namely, the acquisition of sensitive UK semiconductor companies and technologies by hostile states to build up their own defence and military capabilities to the detriment of UK national security, and the use of semiconductors as a vector for cyberattacks.

To mitigate these risks, the strategy highlights the following tools:

- **National Security and Investment Act 2021 (NSI Act)**: The NSI Act came into force on 4 January 2022 and introduced for the first time a mandatory notification and preclosing clearance requirement for transactions in specified sectors. The broad range of sectors (17 in total) captured certain acquisitions and investments of target companies engaged in the sectors of 'computing

hardware' and 'advanced materials', which would include companies working in the semiconductor industry in the UK. In addition to introducing a mandatory notification regime, the NSI Act also provides the UK government with wide powers to 'call in' transactions (including asset acquisitions) that pose a risk to UK national security and enables parties to voluntarily notify their transactions to the government.

In the first year of the NSI Act's operation, the UK government made a number of decisions to block or impose conditions on investments in the semiconductor industry – for example, in the **acquisition of Newport Wafer Fab by Nexperia BV**.

The strategy notes that the areas where the government has seen some issues potentially arising vis-à-vis semiconductor activities are:

- UK-developed research and technology that is a building block for future applications, which could be deployed in ways contrary to UK security interests and values.
- Activity in the compound semiconductor industry, which can be used commercially and for defence and security.
- Semiconductor assets that are used explicitly for UK defence purposes.

The government clarifies in the strategy that it will continue to make decisions on a case-by-case basis, with the focus of its review being on national security risk. It also commits to improving, within the next six to 12 months, the transparency of the NSI Act's operation in relation to semiconductors by reviewing the scope of the definitions of 'computing hardware' and 'advanced materials', as well as providing more guidance on which elements are considered to be more sensitive.

In highlighting the NSI Act as a key tool in protecting the UK against security risks, the strategy emphasises the importance of the NSI Act being deployed as a central and critical plank of the UK national security architecture. This also shows that the government recognises the importance of focusing on national security issues in the context of a rapidly expanding and developing sector.

- **Export controls**: Noting the national security risks presented by exports in the semiconductor sector, the strategy highlights the UK export control regime as the mechanism by which exports that pose a security concern can be controlled. This regime includes the enhanced **military end-use control provisions**, which were introduced in 2022 and permit the government to prevent exports for military end-use in an embargoed destination (regardless of the nature of the item). This proposal is set against the backdrop of the **decision by the US in October 2022 to impose new export controls on advanced computing and semiconductors to China**. By committing to review and expand the export control regime, the strategy reinforces the government's enhanced security focus.
- **Building on hardware strengths to improve cybersecurity**: The strategy identifies the risks of hostile actors tampering with semiconductors before they are fabricated into wafers (i.e., a thin slice of semiconductor material used for the fabrication of integrated circuits), thereby opening a security 'backdoor' or causing a deliberate failure in the device. As such, the strategy sets out key actions for the government to:
  - Prioritise hardware security during chip design stages (as outlined in the **National Cyber Strategy**).
  - Reduce risks at the chip level with continued government investment in and support of the **Digital Security by Design programme**, which aims to ensure the memory safety of software and secure the compartmentalisation of applications to block most cyberattacks.

3. Mitigating the risk of supply chain disruptions

The strategy recognises the complexity of the semiconductor supply chain, and the fact that different countries hold specific specialities means that it will be necessary for the UK government to work domestically and internationally to improve resilience of supply. The strategy sets out actions that the government will take, including:

- Publishing semiconductor resilience guidance to improve the sector's understanding of the potential risks to supply chains and

the steps they can take to prevent future disruption.

- Establishing a cross-government and industry forum to help mitigate supply chain disruptions.
- Engaging with external suppliers to critical industries on risks to chip supply.
- Identifying the supply chains for critical sectors around the world that are most at risk of being impacted by a semiconductor-related supply chain shock.

The safety and resilience of semiconductor supply is crucial in ensuring that expansion and growth in the sector can occur in the UK.

Conclusion

The publication of the strategy was long-awaited and represents an important step in the UK's efforts to secure its position as a global leader in the semiconductor industry – while also safeguarding its economic and national security interests. The measures in the strategy to diversify supply chains and promote domestic manufacturing, whilst also protecting national interests and enforcing minimum security requirements, demonstrate a proactive approach from the government to reducing vulnerabilities and enhancing control over critical semiconductor technologies. Time will tell whether the proposed level of investment goes far enough to enable the UK to build its competitive position on the global stage, but what is clear is that investments into the sector will face continued close regulatory and security scrutiny.

If you would like further information or advice on how the strategy may impact your business, please do not hesitate to contact the authors below.

Key Contacts

Caroline Hobson London	chobson@cooley.com +44 20 7556 4522
Christine Graham London	cgraham@cooley.com +44(0) 20 7556 4455

Victoria Barlow London	vbarlow@cooley.com +44 20 7556 4583
Juan Nascimbene London	jnascimbene@cooley.com +44 (0) 20 7556 4558