



September 2026

UK NSIA ANNUAL REPORT 2025-26: RISING FILINGS, TARGETED INTERVENTION AND A GROWING FOCUS ON STRATEGIC TECHNOLOGY

The UK Government has published its fifth annual report on the operation of the National Security and Investment Act 2021 (“NSIA”), covering the period from 1 April 2025 to 31 March 2026.¹ Notification volumes continue to increase, but intervention remains relatively rare. The report provides insight into the Government's evolving national security priorities, particularly in relation to advanced technologies, strategic know-how, data infrastructure and critical capabilities.

The message for investors is clear: the UK is open to investment, but deals involving sensitive technology, advanced materials, critical infrastructure, data assets, defence supply chains or higher-risk investor profiles are likely to attract greater scrutiny and longer review periods.

KEY POINTS

- + **Notification volumes continue to rise.** The Investment Security Unit (“ISU”) received 1,324 notifications during 2025-26, a 15% increase on 2024-25 and a 46% increase compared with 2023-24.
- + **Most deals clear without intervention.** 95.6% of reviewed transactions were cleared during the initial review period, with only 4.4% called in for a more detailed assessment.
- + **Final orders remain uncommon.** The Government issued nine final orders (approximately 0.7% of notifications), down from 17 in 2024-25. Eight transactions were permitted subject to conditions, while one was prohibited.
- + **Technology and capability are central to national security assessments.** The Government continues to focus not only on ownership of sensitive businesses, but also on access to intellectual property, know-how, research capability and strategic technologies.
- + **Defence remains important, but other sectors are increasingly scrutinised.** Defence remains the largest source of notifications and call-ins, but final orders in 2025-26 were concentrated in Advanced Materials, Data Infrastructure and Military and Dual-Use.
- + **UK investors are not exempt from scrutiny.** Most notifications, call-ins and final orders related to UK-linked acquirers, confirming that the NSIA is not a foreign investment regime in the narrow sense.
- + **Chinese-linked transactions continue to receive enhanced scrutiny.** Although representing only a small proportion of overall notifications, Chinese-associated acquirers featured disproportionately in call-ins and final orders.

¹ [National Security and Investment Act 2021 Annual Report 2025-26 \(HTML\) - GOV.UK](#)



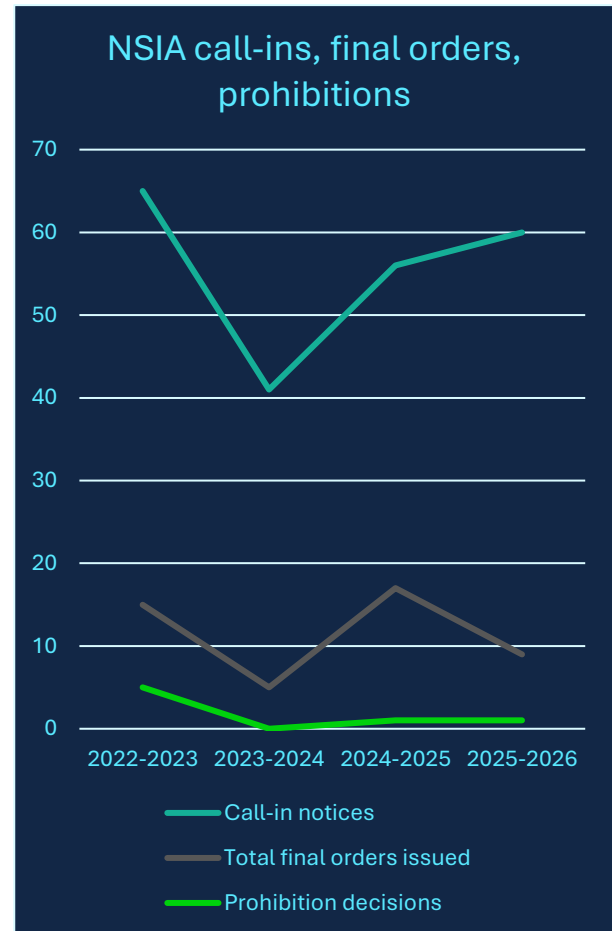
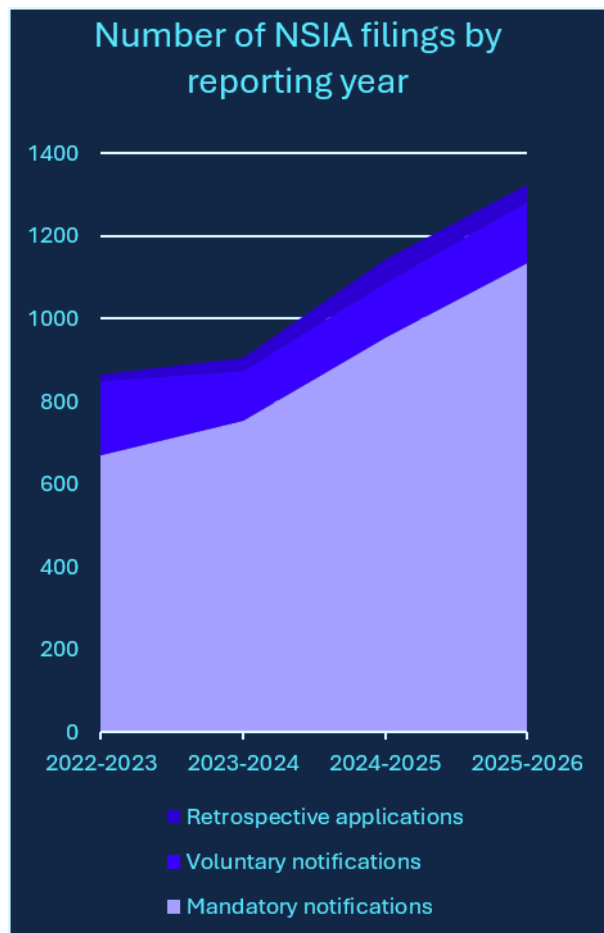
+ Reforms on the horizon. The Government has reaffirmed plans to narrow aspects of the mandatory regime, introduce new exemptions as well as amend and expand mandatory sectors. While timings remain subject to the parliamentary process, the direction of travel is towards a more targeted regime that focuses resources on transactions presenting the greatest national security risk.

WHAT THE ANNUAL REPORT TELLS US

Filing volumes continue to increase

As the chart below left shows, the NSIA regime continues to generate substantial filing activity. In 2025-26, the ISU received 1,135 mandatory notifications, 147 voluntary notifications and 42 retrospective validation applications. The Government accepted 1,242 notifications and rejected 37, with 78 notifications still pending acceptance or rejection at the end of the latest reporting period (see Section 1 of the report).

The continued increase in notifications likely reflects investors' growing awareness of the NSIA regime, rather than an increase in the number of notifiable transactions.



Filings are becoming routine, but the process is taking longer

The increase in filing volumes is beginning to affect transaction timetables. The median time from receipt to acceptance rose to 11 working days for mandatory notifications, 13 working days for voluntary notifications and 10 working days for retrospective validation applications, compared with seven, eight and six working days respectively in the previous reporting period. This suggests parties should allow additional time for the pre-review stage before the statutory review clock begins.

Once a notification was accepted, approximately 95.6% of deals were cleared in the initial statutory 30 working day review period. This is almost identical to the previous year (95.5%) and echoes the Government's view that the "vast majority of inward investment continues to pose no threat to our national security".

Parties should not treat the statutory 30 working day period as the whole timetable. The practical deal timetable should allow for pre-acceptance



review, potential questions on the filing and, for sensitive transactions, the possibility of an extended assessment period. Indeed, where transactions were called in, the average period between call-in and final outcome was approximately 47 working days. For those that ultimately resulted in a final order, the average was 97 working days.

Our analysis of the report's detailed data on assessment duration shows that called-in transactions are on average subject to a number of weeks of "stopped clock" periods, during which day-counting is paused pending compliance with information or attendance notices.

Remedies: a preference for mitigation, but a willingness to prohibit where technology transfer risks cannot be addressed

The Annual Report figures reinforce an important feature of the NSIA regime: intervention does not usually mean prohibition. Of the nine final orders issued during the reporting period, eight allowed the transaction to proceed subject to conditions, while only one resulted in the transaction being blocked. (Four further transactions were withdrawn by the parties after call-in, but it is impossible to tell whether these were abandoned for reasons related to the NSIA review.) This continues the pattern seen since the NSIA came into force, with the Government generally seeking to manage national security concerns through tailored remedies rather than preventing investment altogether.

Although the Annual Report does not categorise the forms of remedy used, recent final orders indicate a familiar toolkit. Conditions have included restrictions on access to sensitive information and intellectual property, governance and security requirements, commitments relating to UK operations and supply arrangements, and limitations on the transfer of technology, data or know-how. For parties involved in sensitive transactions, particularly those involving advanced technologies, critical infrastructure or government-facing capabilities, discussions around potential mitigation should therefore begin early in the deal process.

The sole prohibition of the reporting period provides a particularly revealing example of the Government's current priorities. The transaction concerned a proposed joint venture between Versarien plc and Anhui Boundary Innovative Materials Technology Co Ltd (BIMT),² involving the transfer of tangible and intangible assets relating to the production and use of graphene. The Government's concern centred on security of know-how and intellectual property relating to graphene technologies with dual-use applications. This is far from the traditional targets of national security intervention, such as defence contractors or critical infrastructure, and shows the Government's keen interest in adversaries' access to potentially militarily useful information.

The *Versarien/BIMT* decision is also a useful reminder that asset acquisitions, joint ventures, collaboration agreements, technology licensing arrangements and other structures involving access to sensitive technology can attract the same level of scrutiny as a conventional M&A transaction.

Non-notified transactions remain firmly on the enforcement radar

The Annual Report records that six non-notified acquisitions were called-in during the reporting period, in addition to 54 notified acquisitions. In exercising its statutory functions, the ISU may monitor and record publicly available Internet data, including news reports, websites, public records such as Companies House and Land Registry, blogs and social networking sites. It may also be alerted to transactions by other parts of Government, or even by third-party data aggregators.

Parties should therefore keep in mind that there is a real risk of call-in that could derail transaction timetables, and furthermore that – while the ISU has not to date issued any penalties for non-compliance – it has that power, and may choose to do so in the future.

² [Acquisition of tangible and intangible assets held by Versarien Plc by the prospective UK Joint Venture Co and Anhui Boundary Innovative Materials Technology Co Ltd: notice of final order – GOV.UK](#)



Higher-risk investor profiles continue to attract scrutiny

UK-linked acquirers accounted for the largest proportion of accepted notifications, call-ins and final orders. However, Chinese-linked acquirers were disproportionately represented in more intensive review outcomes. Chinese-linked acquirers accounted for 30% of call-ins and three of the nine final orders, while China represented only a small percentage of accepted notifications.

This is broadly consistent with trends across other investment screening regimes, where transactions involving Chinese investors continue to attract enhanced scrutiny. All the same, this is not to say that China-linked transactions are doomed to failure, as some will be cleared.

Sector trends: Advanced Materials and Data Infrastructure move up the risk agenda

Defence remains the most common area of the economy for notifications and call-ins.

Notifications were most commonly associated with Defence, followed by Military and Dual-Use and Critical Suppliers to Government.

However, final orders tell a more targeted story. Of the nine final orders made during the reporting period, five were associated with Advanced Materials, three with Data Infrastructure and two with Military and Dual-Use, and one each for Critical Suppliers to Government, Defence, Manufacturing, Quantum Technologies and Suppliers to the Emergency Services (with some cases falling within multiple mandatory sectors).

This reflects a broader shift from traditional defence assets towards technologies and capabilities that may create future military, intelligence, infrastructure or economic security risks. The *Versarien*/BIMT prohibition described above illustrates this point.

Enforcement: still soft in practice, but not risk-free

The Government identified 42 potential offences of completing a notifiable acquisition without approval during the reporting period. In line with previous years, no penalties were issued and no criminal prosecutions concluded. Where offences were identified but no penalty was imposed, parties were required to provide reassurance that steps had been taken to prevent recurrence.

The absence of penalties should not be taken as evidence that the regime will always be lightly enforced. The legal consequences of completing a notifiable acquisition without approval remain severe: the transaction is void unless retrospectively validated, civil or criminal penalties may apply, and the Government is entitled to ramp up enforcement whenever it sees fit.

PRACTICAL IMPLICATIONS FOR BUSINESSES

Businesses should:

1. **Conduct NSIA analysis early**, ideally before signing or bid submission, where the target operates in or adjacent to sensitive sectors.
2. **Look beyond defence M&A**, particularly for asset deals, IP licences, collaboration agreements, joint ventures, data arrangements and acquisitions of control over sensitive assets.
3. **Build realistic timetables** into transaction documents, including pre-acceptance time, the 30-working day review period and the possibility of call-in and extended assessment.
4. **Assess investor risk carefully**, including ownership/control, financing, state links, existing capabilities and access to sensitive information.
5. **Document non-filing decisions**, especially where the transaction is close to a mandatory sector or involves sensitive assets or non-UK investor links.
6. **Prepare mitigation options early** for higher-risk transactions, particularly where risks relate to IP access, data flows, UK Government supply, sensitive facilities or technology transfer.



FINAL THOUGHT...

The 2025-26 Annual Report shows a regime that is becoming increasingly embedded in UK transaction planning and execution. Notification volumes continue to rise, but intervention rates remain low and the overwhelming majority of transactions continue to be cleared.

The report highlights an increasing focus on advanced technologies, strategic know-how, data assets, advanced materials and dual-use capabilities. The *Versarien*/BIMT prohibition is particularly notable because it demonstrates that access to intellectual property, technical expertise and research capability can be as significant as ownership of a business when the Government assesses national security risk.

Looking ahead, the Government has signalled further reforms to the regime, including new exemptions, additions and subtractions from the mandatory notification sectors, and improvements to the notification process. These changes are intended to reduce unnecessary burdens and improve predictability, while enabling Government resources to focus on genuinely sensitive transactions.

CONTACT



MARTA ISABEL GARCIA

Partner

+ 44 20 7809 2141

marta.garcia

@stephensonharwood.com



PHILIP MCMAHON

Managing Associate

+ 44 20 7809 2029

philip.mcmahon

@stephensonharwood.com