22 December 2020

During the Defence Sub-Committee evidence session on the 14 December, I committed to write about the powers Government has to deal with companies where there are retrospective concerns relating to national security.

As provided for in the National Security and Investment (NSI) legislation, the Government will be able to proactively "call in" specific acquisitions of control or ownership of entities or assets for a national security assessment. Once implemented, the call-in power will apply from 12 November 2020, ensuring that from this date onwards acquisitions of control and ownership of key companies are subject to Government scrutiny on national security grounds. Additionally, the Bill provides for a retrospection period for this power, meaning the Government will be able to undertake national security assessments for transactions that it had not previously been made aware of for up to 5 years after they were completed. The Secretary of State cannot 'reach back' beyond 12 November for this purpose, however.

More widely, there are no powers to retrospectively intervene in previous changes of control or ownership. Both the Enterprise Act 2002 and the NSI Bill contain powers to investigate and potentially unwind transactions for specified periods after they complete; four months for the Enterprise Act and six months for the NSI Bill. For the sectors subject to mandatory notification under the NSI Bill, there is no time limit on calling in a notifiable acquisition where a notification was not received.

There are a number of facilities available to the Government to address risks posed by companies to our security beyond the NSI regime. I have outlined some of the key levers below.

Firstly, the Government has the export controls framework to address risks raised where companies seek to move sensitive assets or intellectual property abroad. Export controls apply to military goods and technology; to "dual-use" items (i.e. goods and technology having both civil and military applications); and, to items that may be used in a weapons of mass destruction programme. These controls are based on and consistent with international standards. All licence applications are rigorously assessed against a risk assessment framework (the "Consolidated Criteria"). This assessment takes account of the risks that the export might pose to national security and to international peace and security, the risk of diversion to undesirable end-uses, and the risks around human rights. The Government will not grant an export licence if to do so would be inconsistent with these Consolidated Criteria. Furthermore, similar controls extend to academia; the Academic Technology Approvals Scheme (ATAS) works with the export controls framework to protect UK research and national security interests. It applies to all international students (apart from exempt nationalities) who are subject to UK immigration control and are intending to

study at postgraduate level in certain sensitive subjects. The subjects are those where students' knowledge could be used in programmes to develop Advanced Conventional Military Technology (ACMT), weapons of mass destruction (WMDs) or their means of delivery.

Secondly, there are sector-specific controls which address national security risks raised in the operational activity of companies. For instance, the Office for Nuclear Regulation is responsible for the regulation of nuclear safety and security across the UK, including reviewing the design of nuclear power stations; licensing nuclear sites; authorising key activities on those sites; and, inspecting them throughout their lifetime. Such a security-centred role is held by other regulators. Where foreign owned companies have an operational role in energy infrastructure, they must demonstrate their capacity and reliability in line with licensing regulations and are closely monitored by regulators such as Ofgem or the Oil and Gas Authority. For example, Ofgem has rules on how electricity and gas licensees can operate. These regulators can fine companies, or even revoke licenses, if the licensee fails to comply with orders.

Thirdly, the Centre for the Protection of National Infrastructure (CPNI) acts as a national technical expert for protective and personnel security. It provides advice to Government, businesses and other organisations on how to reduce vulnerability to a range of threats. For instance, it can support engagement with critical national infrastructure and other sensitive locations to mitigate and address a variety of security risks.

Fourthly, for partners handling sensitive Government information, the Security Policy Framework provides guidance and support for contractors with direct access to classified materials, mandating particular security outcomes. For instance, the Framework supports partners and Government bodies to put in place governance and accountability frameworks which includes mandatory UK nationality for Board level and Security controllers. This extends to List X contractors; companies operating in the UK who are working on UK Government contracts which require them to hold classified information.

Lastly, I would like to outline that there are funding mechanisms which allow the Government to work with companies to ensure long-term equity investment and growth in security-sensitive areas. For instance, the National Security Strategic Investment Fund (NSSIF) is the Government's corporate venturing arm for dual-use advanced technologies. The NSSIF's objectives include accelerating the adoption of the Government's future national security and defence capabilities and the development of the UK's dual-use technology ecosystem.

I hope this letter helps clarify the variety of levers at the Government's disposal to protect our national security and reassures the Committee that the NSI legislation will bring more security for British businesses and people from hostile actors targeting our country.