



# **National Security and Investment**

## **A consultation on proposed legislative reforms**

Presented to Parliament  
by the Secretary of State for Business, Energy and Industrial Strategy  
by Command of Her Majesty

July 2018



© Crown copyright 2018

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [www.nationalarchives.gov.uk/doc/open-government-licence/version/3](http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3)

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at [www.gov.uk/government/publications](http://www.gov.uk/government/publications)

Any enquiries regarding this publication should be sent to us at:

National Security and Investment Review  
Consumer and Competition Policy Directorate  
Department for Business, Energy & Industrial Strategy,  
1st Floor, 1 Victoria Street,  
London, SW1H 0ET

ISBN 978-1-5286-0709-4

CCSCCS0718072828

07/18

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office.

# Foreword

The UK economy has a proud and hard-won reputation as one of the most open economies in the world. As of 2017, the UK had the third-highest inward foreign direct investment stock in the world. This is not just a fact. It is a reflection of the values on which our economic approach is based – one which welcomes overseas investment, one which champions enterprise and innovation, and one which supports jobs and growth.

Investors across the globe welcome the stability that the British system and economy offers, allowing them to invest with confidence, based on our standards of corporate governance, our framework of laws and policies and – above all – our business-friendly environment.

Of course, an open approach to international investment must include appropriate safeguards to protect our national security and the safety of our citizens. Technological, economic and geopolitical changes mean that reforms to the Government's powers to scrutinise investments and other events on national security grounds are required.

We are not acting in isolation. Many of our allies around the world – including the United States, Australia, Germany, France and Japan – are similarly looking to modernise their powers in this area.

The proposals set out in this White Paper follow the guiding principles that have underpinned our policy development from the outset – including certainty and transparency wherever possible, ensuring the UK remains attractive to inward investment, and focused clearly on the minority of cases which raise national security concerns.

I invite responses from businesses and other interested parties both within the United Kingdom and around the world. Their responses will help the Government to refine these proposals further and ensure the right way forward.

The new framework must work both to protect national security and to keep Britain open for business. This is essential to maintain our reputation as a leading destination for foreign investment and to continue building a Britain fit for the future.



**THE RT HON GREG CLARK MP**  
**SECRETARY OF STATE FOR BUSINESS, ENERGY AND INDUSTRIAL STRATEGY**

# Contents

Foreword.....	3
General information about the consultation.....	5
Executive Summary.....	9
Background.....	17
Chapter 1 – The case for change .....	20
Chapter 2 – The Green Paper consultation and responses.....	26
Chapter 3 – The trigger events which could be called in .....	30
Chapter 4 – The statutory statement of policy intent.....	52
Chapter 5 – How the Government will screen notifications .....	58
Chapter 6 – The call-in power .....	63
Chapter 7 – Calling in a trigger event and the subsequent assessment process .....	71
Chapter 8 – The remedies available to protect national security .....	81
Chapter 9 – The potential sanctions for non-compliance.....	93
Chapter 10 – Judicial oversight.....	98
Chapter 11 – How the proposed reforms will interact with other regimes .....	102
Annex A – List of consultation questions .....	112
Annex B – Indicative list of potential conditions .....	113
Annex C – List of sanctions and offences created by the regime .....	116

# General information about the consultation

## Purpose of this consultation

This White Paper is the next stage in the Government's reform of its powers in relation to protecting national security from hostile actors' acquisition of control over entities or assets.

It follows the National Security and Infrastructure Investment Review Green Paper published in October 2017 and takes account of the responses to that consultation. A summary of responses to that consultation is published alongside this White Paper.

The White Paper sets out the Government's proposed reforms for creating clear and focused powers within a predictable and transparent process.

The Government will use the responses to the White Paper to refine these proposals ahead of the introduction of primary legislation when Parliamentary time allows.

**Issued:** 24 July 2018

**Consultation responses:** required by 16 October 2018

**Enquiries to:**

National Security and Investment Consultation  
Consumer and Competition Policy Directorate  
Department for Business, Energy & Industrial Strategy,  
1st Floor, 1 Victoria Street,  
London, SW1H 0ET

Tel: 0207 215 5000

E-mail: [nsiireview@beis.gov.uk](mailto:nsiireview@beis.gov.uk)

## Territorial extent

The proposed reforms will extend to the whole of the UK. National security is a reserved matter in Scotland and Wales and an excepted matter in Northern Ireland. The UK Government will continue to engage with the devolved administrations to ensure these proposals can function effectively with areas of devolved competence.

## How to respond

Your response will be most useful if it is framed in direct response to the consultation questions set out in the relevant chapters and listed in Annex A. Responses should be submitted via the Citizen Space website:

<https://beisgovuk.citizenspace.com/ccp/nsi>

Alternatively, respondents can email responses to [nsireview@beis.gov.uk](mailto:nsireview@beis.gov.uk) or can provide hard copy responses to the correspondence address above.

### **Additional copies**

You may make copies of this document without seeking permission. An electronic version can be found at <https://www.gov.uk/government/consultations/national-security-and-investment-proposed-reforms>

## Confidentiality and data protection

### **Details of data controller and data protection officer**

The data controller is the Department for Business, Energy & Industrial Strategy (BEIS). You can contact the BEIS DPO at:

The Data Protection Officer

Department for Business, Energy & Industrial Strategy (BEIS)

1 Victoria Street

London SW1H 0ET

Email: [dataprotection@beis.gov.uk](mailto:dataprotection@beis.gov.uk)

### **Purpose of the processing, legal basis for the processing, and recipients of the personal data**

BEIS will be processing your personal data solely for consultation purposes. We are collecting your data as part of our public task and may need to share with other government departments in performing this public task. This is necessary to conduct a comprehensive consultation process on these proposals.

### **Details of transfers to third country**

The data you provide will not be transferred outside the European Economic Area.

### **Retention period**

The information you provide will be retained for three years.

### **Data subject's rights**

A full list of your rights is accessible at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

## **Right to withdraw consent**

You have the right to withdraw your consent at any time where BEIS is relying on consent to process your personal data.

## **Provision of personal data as part of a statutory requirement and possible consequences of failing to provide the personal data**

To the extent that you are providing your personal data in relation to a BEIS public task the failure to provide this information will mean that we are unable to process your consultation responses.

## **Existence of automated decision-making**

The provision of the information you provide is not connected with individual decision making (making a decision solely by automated means without any human involvement) or profiling (automated processing of personal data to evaluate certain things about an individual).

## **Right to lodge a complaint with a supervisory authority**

You have the right to lodge a complaint with the ICO (supervisory authority) at any time. Should you wish to exercise that right, full details are available at:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

## **General information**

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want information that you provide to be treated as commercially sensitive or confidential please say so clearly in writing when you send your response to the consultation. It would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

We will summarise all responses and place this summary on the GOV.UK website. This summary will include a list of names or organisations that responded but not people's personal names, addresses or other contact details.

## Quality assurance

This consultation has been carried out in accordance with the [Government's Consultation Principles](#).

If you have any complaints about the consultation process (as opposed to comments about the issues which are the subject of the consultation) please address them to: [enquiries@beis.gov.uk](mailto:enquiries@beis.gov.uk)

# Executive Summary

1. This White Paper follows the announcement of the Government's intention to reform its powers in September 2016 and a consultation on a Green Paper published in October 2017. The Government has taken, and will continue to take, a considered and consultative approach to these important and complex issues.
2. The Government will reform its powers to protect national security from hostile actors using ownership of, or influence over, businesses and assets to harm the country. The reforms will be proportionate and focused in their application, with each case following a clear and predictable process.
3. These reforms will bring the UK closer in line with other countries' regimes, and are taking place as many other governments are also updating their powers in light of the same technological, economic and national security-related changes.
4. The new regime is only related to national security. National security is not the same as the public interest or the national interest. The success of the new regime will require its tight focus on national security and not on wider public interest issues.
5. The Government's 2017 Green Paper concluded that no changes were needed to the wider public interest regime. The Government has no plans to amend the public interest considerations on the basis of which ministers can intervene in mergers, other than as necessary to introduce the new national security-related regime described in this White Paper.

## The Government's approach to reforms

6. Foreign investment and an active and competitive economy are key to the UK's growth and development; the UK warmly welcomes the contribution that foreign investment makes and seeks to increase international partnerships in areas such as research and innovation. Only a small number of investment activities, mergers and transactions in the UK economy pose a risk to our national security.
7. However, for these cases, it is vital that the Government is able to intervene in order to prevent or mitigate these risks. Currently, the Government's powers to intervene in relevant transactions derive from the Enterprise Act 2002. As

the Green Paper concluded, these powers are limited in places – particularly in contrast to other countries’ regimes.

8. The Government amended the Act earlier this year to allow more interventions in certain key areas of the economy. Full reform, however, requires primary legislation to introduce a new regime; one that works for the Government, investors and businesses.
9. This means the Government must have the breadth and flexibility it needs to deal with evolving national security threats. It also means not burdening businesses and investors unnecessarily. As such, the Government is not intending to introduce a mandatory notification regime. Instead, the Government will introduce a regime that allows it to target the small number of instances where national security is at risk.
10. While the Government is proposing a voluntary notification system (as exists under the Enterprise Act 2002), it will encourage notifications from parties who consider that their transaction or other event may raise national security concerns. To help inform this assessment, the Government will publish details about when and how it expects national security concerns are likely to arise.
11. Early notification is in all parties’ interests. Where a transaction or other event is notified but does not, in fact, raise national security concerns, the Government will be able to issue early confirmation to allow it to proceed.
12. In the event that parties choose not to notify the Government, it reserves the right to intervene (including after the event for a prescribed period) to protect national security.
13. Any intervention will be carried out in a transparent and predictable manner.
14. The new regime will update our rules and powers in a manner proportionate to the national security risks we now face. The UK is not alone in doing so – other countries and international organisations have updated their rules and powers (or are in the process of doing so) to ensure that they can protect their own national security interests.
15. The new approach does not change the UK’s openness to foreign investment or its open and dynamic economy. The Government is committed to deliver its vision of making the UK the world’s most innovative economy and the best place in the world to start and grow a business. The Government will continue to strive to increase overseas investment from, and collaboration with, partners across the world. This White Paper seeks views from businesses,

investors and other groups about how the Government can implement these reforms in the most suitable way possible.

## The proposed new regime

16. The proposed new regime is summarised in Figure 1.

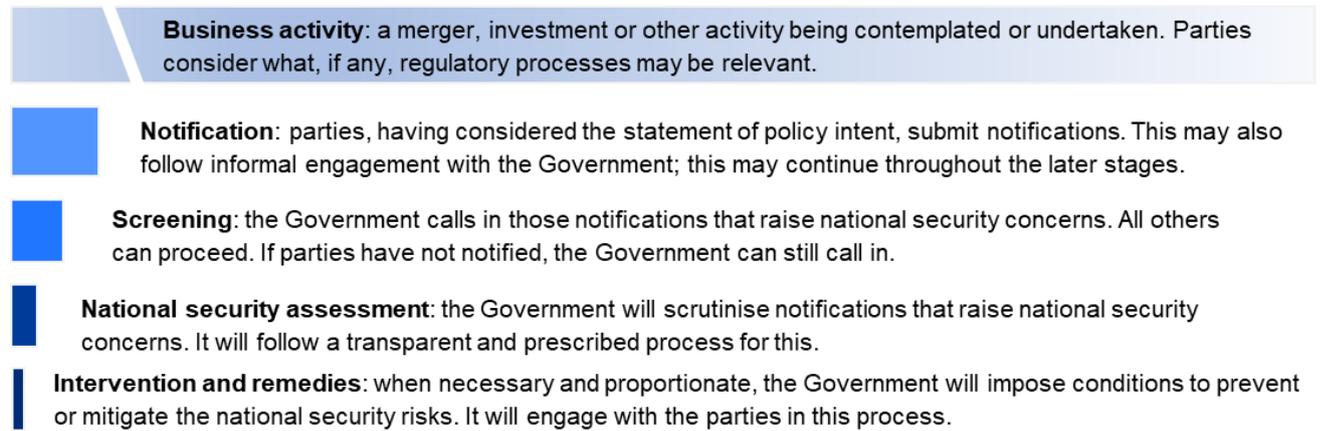


Figure 1: summary of the overall regime, showing the relative frequency (not to scale)

### Notification

17. The Government will encourage notification of investments and other events that may raise national security concerns. It will publish a detailed statement of policy intent to describe where and how it considers these are most likely to arise. This should allow parties to determine whether to discuss the activity informally with Government officials and/or whether to submit a formal notification to the Government.
18. However, it reserves the right to call in transactions or other events (including after they have taken place for a prescribed period) to undertake a national security assessment.
19. The Government considers that the proposed regime, with the inclusion of a clear statement of policy intent, will encourage notifications in relation to the trigger events about which it has national security concerns. A key purpose of this consultation is to seek respondents' views about those trigger events that parties consider they would notify to the Government, or which they would seek further advice about. The Government may reform the proposals in light of this feedback and further policy development.

### Screening

20. The Government's initial analysis expects there to be around 200 notifications made each year. It will aim to quickly screen out those in which it has no national security concerns.

## Full national security assessments

21. For those notifications that the Government expects will raise national security concerns each year (its initial analysis indicates this may be around half of those notified) the Government will subject these to a full assessment. It will do so following a prescribed and transparent process.

## Imposition of remedies

22. If, following its assessment, the Government concludes that national security is at risk, it will impose such remedies as necessary and proportionate. The Government's initial analysis indicates that this will arise in around half of those cases subject to a full national security assessment having been called in per year.

## Glossary of key terms

23. The White Paper uses a number of key terms:
  - **trigger events**: any acquisition of control or significant influence over an entity or asset. This will normally be in the form of a merger, investment, or other commercial activity. However, it may also arise through any other means by which someone acquires significant influence or control. It also captures acquiring any additional or further means of exerting significant influence or control over an entity.
  - **entity**: the proposed legislation would use this term to cover any form of entity, such as companies or partnerships, over which control or significant influence may be acquired.
  - **asset**: to prevent the reforms being subverted or evaded, the proposed legislation would also allow the Government to scrutinise the acquisition of control over real and personal property, intellectual property and contractual rights when this might raise national security concerns.
  - **significant influence or control**: the formal or practical means to direct an entity's operations or strategic direction, or to direct the operation of an asset. Further guidance about the interpretation of this phrase will be set out in the statement of policy intent.
  - **statement of policy intent**: the document that the Government will publish (approved by Parliament) to explain how the call-in power is expected to be used and to set out where and how it considers national security risks might arise from control being acquired over entities or assets. A draft is published alongside this White Paper.
  - **Senior Minister**: the Cabinet-level minister who is the key decision-maker for the new regime.

- **notification:** the means by which parties will submit details to the Government where they believe that a trigger event may raise national security concerns.
- **screening:** the Government's initial national security assessment of a valid notification. Those that do not raise these concerns will be 'screened out' quickly so that they can proceed. Others will be called in for a more detailed assessment.
- **call-in power:** the power for the Government to subject a trigger event to a more detailed assessment of the national security risk that it may raise. The Government can 'call in' any trigger event that meets the legal test, even if it has not been notified to the Government.
- **remedies:** the conditions the Government will impose to prevent or mitigate national security risks, following its assessment. As a last resort, this might mean blocking the trigger event or unwinding it if it had already taken place.

## A broader set of 'trigger events' that can be scrutinised

24. The reforms will expand the range of circumstances where the Government has powers to address national security risks. These 'trigger events' cover the range of means by which a hostile actor can acquire the ability to undermine our national security in the short or long term.
25. These will include any investment or activity that involves the acquisition of:
  - more than 25% of an entity's shares or votes; or
  - significant influence or control over an entity; or
  - further acquisitions of significant influence or control over an entity beyond the above thresholds.
26. The circumstances in which a person can acquire further control over an entity will be set out in the statement of policy intent.
27. The proposed regime will also provide the Government with powers to prevent the reforms being subverted or evaded through being able to assess control gained over assets. This could include the acquisition of:
  - more than 50% of the asset; or
  - significant influence or control over the asset.

## Clarity about where and how the regime applies

28. A detailed statement of policy intent will set out where and how the Government expects national security risks to arise from trigger events by covering:

- **the target risk:** a description of entities and assets where the acquisition of control can be used to undermine national security, and details about the sectors of the economy where the Government expects these risks are more likely to arise;
- **the trigger event risk:** a description of the means of control and influence that must take place in order that the trigger event can potentially undermine national security; and
- **the acquirer risk:** details about the parties which the Government considers are more likely to pose a national security risks through acquiring entities or assets.

## A clear, transparent and predictable screening process

29. The Government encourages notifications about trigger events that may raise national security concerns. Given the detail provided in the statement of policy intent about the target, trigger event and acquirer risks, the Government expects there will be around 200 notifications each year.
30. For any notified trigger events that do not, in fact, raise these concerns, the Government will quickly screen these out and confirm its view within a prescribed period. Its initial analysis indicates this to be possible for around half of the 200 notifications.
31. For those notifications that do raise significant concerns, the Government is likely to 'call in' the trigger event for a full national security assessment. A clear and circumscribed legal test would need to be met in order for the Government to exercise this power.
32. The Government will be able to call in any trigger event that raises national security concerns, including those not notified to it. It will be able to do this when the trigger event is in contemplation or progress, or within a prescribed period after a trigger event has taken place. Under the Enterprise Act 2002, the approximate time during which the Secretary of State can act in relation to a relevant merger situation on public interest grounds is, in effect, three months. Some other screening regimes around the world have considerably longer – or indefinite – retrospective periods. This White Paper suggests this period under the new regime could be up to six months.
33. So as to ensure that it is aware of trigger events that may raise these concerns, the Government will increase the resources dedicated to market monitoring, and invest in the tools and systems necessary. It will also have powers to request information in relation to specific trigger events that the Government is aware of in order to inform its decision as to whether to call in a trigger event for screening.

34. Once the Government has called in a trigger event for national security assessment, it will then have a prescribed period of time in which to assess potential national security concerns. This will be a period of up to 30 working days, potentially extendable by a further 45 working days.
35. The Government will publish information about all trigger events it calls in for assessment.
36. The proposed process is summarised in Figure 2 below.

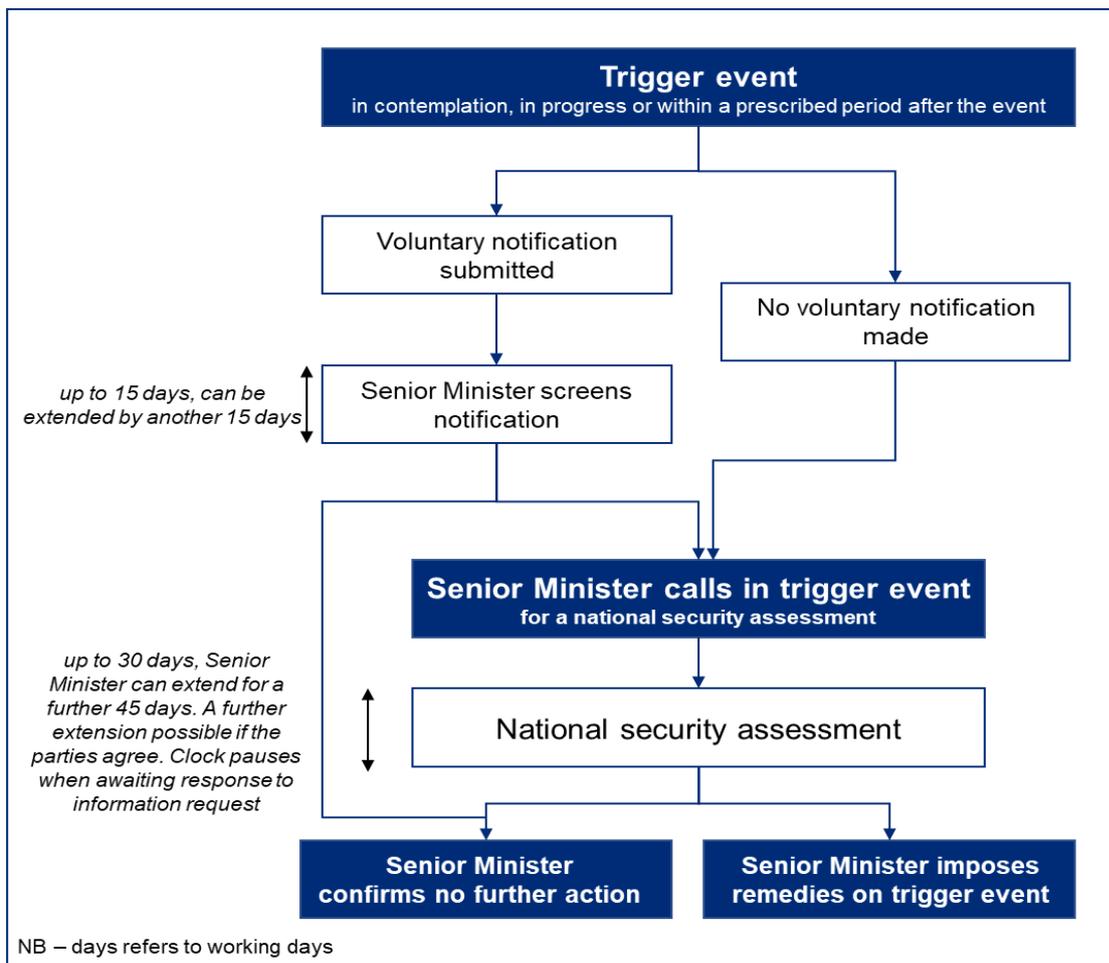


Figure 2: the screening, call-in and assessment process

## A set of strong remedies and sanctions available to protect national security, subject to rigorous judicial oversight

37. Should the Government conclude that the trigger event does pose a risk to national security, it will be able to impose conditions in order to prevent or mitigate these risks, allowing the trigger event to proceed. As a last resort, it will be able to block or unwind the trigger event. The Government's initial

analysis indicates that around half of those trigger events called in for a full national security assessment will require remedies.

38. Appropriate to a national security-related regime, the proposed legislation would create a number of sanctions, civil and criminal, that will apply in the event of non-compliance with remedies imposed on a trigger event, or other orders (such as information-gathering requests) served on parties.
39. Any decision to impose a remedy or a sanction would, like all decisions and actions under the proposed legislation (including calling in a trigger event), be subject to challenge and judicial oversight.

### **The proposed reforms will be implemented in an efficient and co-ordinated manner alongside other regimes**

40. The proposed reforms will involve removing national security considerations from the Enterprise Act 2002 and its competition or public interest assessment process.
41. In making this change, the Government will ensure that the new assessment process interacts in a way that is as efficient as possible for parties that are subject to these, and any other statutory and regulatory, processes. It will also maintain the independence of the Competition and Markets Authority.

# Background

42. The UK recognises the vital contribution that the vast majority of foreign investment transactions make to our economy and prosperity. Only a small number of investment activities, mergers and transactions in the UK economy pose a risk to our national security. However, for these cases, it is vital that the Government is able to intervene in order to prevent or mitigate these risks.
43. Any Government's first duty is to protect national security. It is right, therefore, that the Government periodically reviews whether it has the right powers, structures and processes needed to intervene in the rare circumstances where national security is at risk. In 2016, this Government announced such a review, that has led to this White Paper.
44. In the period since, a number of other countries and organisations have undertaken similar reviews and reached the same conclusion – that changes in our global economy and national security landscape mean that rules need updating to address the risks we face.
45. In reforming its powers, the Government will continue to deliver its vision of making the UK the world's most innovative economy and the best place to start and grow a business.
46. This means ensuring the Government has the powers and flexibility it needs to intervene in those small number of cases where investments or other trigger events raise national security risks. It also means ensuring that we maintain a rules-based system which is predictable and transparent to encourage the investment that will help our economy to continue to grow and prosper.

## The 2017 Green Paper

47. The National Security and Infrastructure Investment Review led to the publication of the Government's [Green Paper](#) in October 2017. It concluded that in an increasingly complex and interconnected international political and economic landscape, and in a world with ever-evolving technology presenting new security challenges, the Government's powers needed updating. The review highlighted that the UK's powers were both limited in places and inconsistent, particularly in contrast to other countries' regimes.
48. The Green Paper proposed both short-term and longer-term reforms. The short-term reforms were to address risks in vital, emerging technology

industries. The Government subsequently [amended the thresholds](#) for the turnover and share of supply tests within the Enterprise Act 2002, in three areas of the economy: goods and services that can be used for military or military and civilian use, computing hardware and quantum technologies.

49. The Green Paper also sought views about longer-term reforms. This is the focus of this White Paper which sets out the Government's conclusion about the way forward and invites input on the specific details of these proposed reforms. Following this consultation, the Government will respond in line with the [Government's Consultation Principles](#) and proposes to legislate when Parliamentary time allows.

## Principles underpinning these proposals

50. In the Green Paper, the Government established five principles underpinning its review. These have shaped the Government's policy development to date and will continue to do so. These are to:
- ensure the UK remains [attractive](#) to inward investment;
  - provide [certainty](#) and [transparency](#) wherever possible;
  - reflect [national security](#) concerns;
  - ensure a [targeted](#) scope wherever possible; and
  - ensure powers are [proportionate](#).

## Structure of the White Paper

51. This White Paper is structured as follows:
- [Chapter 1](#) describes the factors that mean reform is needed.
  - [Chapter 2](#) summarises the [key policy issues set out in the Green Paper](#) and the Government's conclusion about the way forward.
  - [Chapter 3](#) describes the [trigger events](#) covered by the new regime.
  - [Chapter 4](#) explains how the [statement of policy intent](#) will provide as much clarity as possible about where the national security risks that concern the Government arise.
  - [Chapter 5](#) describes the process for the Government's [initial screening of notifications](#) which it encourages parties to submit.
  - [Chapter 6](#) describes the [call-in test](#) that would need to be met for trigger events to undergo a full national security assessment.
  - [Chapter 7](#) sets out the [process for calling in a trigger event and how the subsequent assessment process will operate](#).
  - [Chapter 8](#) explains how the Government will be able to impose [remedies](#) on parties, or (as a last resort) block or unwind trigger events.
  - [Chapter 9](#) describes the criminal and civil [sanctions](#) that will apply in certain circumstances.

- Chapter 10 describes the **judicial oversight** and redress available to parties in relation to decisions made under the proposed regime.
- Chapter 11 explains how the proposed reforms and processes will **interact with other regimes**, including the UK competition regime.

# Chapter 1 – The case for change

## Summary

- the UK faces continued and broad-ranging hostile activity, including through the exploitation of acquisition of control or influence over UK entities or assets.
- the UK's current powers to prevent or mitigate this are no longer sufficient in light of the risks posed by national security, technological and economic changes.
- the UK is not alone in reforming its powers – other countries and the EU are reforming their approaches.
- the changes do not affect the fundamental position of the UK as being open for business – we welcome foreign investment and the benefits it brings.

## Introduction

1.01 The UK welcomes foreign investment which is key to economic growth. International partnerships continue to be a critical element to the UK's success in areas such as research and innovation. Of course, it is vital that the Government is able to intervene to protect national security in the relatively small number of transactions and other trigger events that could pose a risk.

1.02 This chapter summarises the case for changes to our current powers, including the national security, technological and economic context. This was described in more detail in the Government's 2017 Green Paper.

## The UK Government's current relevant powers to protect national security

1.03 As set out in Chapter 4 of the Green Paper, the Government has a comprehensive set of powers to protect national security. The following paragraphs focus only on the Government's powers in relation to business transactions.

## Merger control

1.04 The wider merger regime reflects the openness of our economy. It is characterised by transparent rules designed to guard against anti-competitive

behaviour and uphold proper conduct. These rules are administered consistently by expert bodies that operate independently of the Government:

- the Competition and Markets Authority (CMA) is responsible for assessing the effect on competition from mergers; and
- the Takeover Panel oversees the Takeover Code which governs the process of takeovers where the Code applies.

1.05 Ministers' ability to intervene in mergers is significantly restricted to issues of specified public interest, namely:

- national security (including public security);
- financial stability (prudential regulation in European mergers); and
- media plurality.

1.06 Ministers can only intervene under the Enterprise Act 2002 on public interest grounds if the merger meets the definition of a relevant merger situation including the turnover or share of supply tests.<sup>1</sup> There are limited exceptions (under the Special Public Interest Regime) where the Government can intervene without the merger meeting these tests. However, these are limited to relevant government contractors and media companies. The Government's amendments to the Enterprise Act 2002 earlier this year also lowered the turnover threshold and modified the share of supply test in relation to certain areas of the economy.

### **Sector regulation and export control**

1.07 Some sectors of the economy are subject to specific regulatory systems. These are for a wide range of purposes, but a number are relevant to the protection of our national security. For example, the Office for Nuclear Regulation independently regulates nuclear safety and security at 30 civil nuclear licenced sites in the UK. In some sectors, the Government or independent regulator operate a licence or authorisation scheme, ensuring that proper scrutiny of people and organisations engaged in key activities is undertaken. Chapter 4 of the Green Paper provided further details about these existing statutory and regulatory powers.

1.08 The Government, like many others, also controls the export of so-called 'strategic items'. Through the Export Control Joint Unit within the Department for International Trade, the Government assesses applications for export licences for strategic items ensuring that the items do not end up in the wrong hands. The items subject to strategic export control are set out in a number of lists, collectively known as [Strategic Export Control Lists](#).

---

<sup>1</sup> This is covered in sections 23 and 23A of the Enterprise Act 2002.

## Why changes are needed

- 1.09 The Government is clear that its current powers, including under Part 3 of the Enterprise Act 2002, are no longer sufficient to address the challenging and changing national security threats the UK faces. As Chapters 3 and 7 of the Green Paper described, there have been significant national security, technological and economic changes that have taken place in recent years, and these will continue to evolve.
- 1.10 These changes have implications for our national security. National security is not the same as public interest or the national interest.
- 1.11 These reforms will bring the UK closer in line with other countries' regimes, and are taking place as many other governments are also updating their powers in light of the same technological, economic and national security-related changes.

## Risks to our national security

- 1.12 The UK faces continued and broad-ranging hostile activity from foreign intelligence agencies and others. As set out in Chapter 3 of the Green Paper, [the most recent UK national security risk assessment](#) shows that the country faces greater and more complex threats compared to the previous assessment published in 2010.
- 1.13 Foreign intelligence agencies continue to engage in hostile activity against the UK and our interests, and against many of our close allies. This includes human, technical and cyber operations at home and overseas to compromise the Government, diplomatic missions, Government-held information and critical national infrastructure; attempts to influence Government policy covertly; and operations to steal sensitive commercial information and disrupt the private sector.
- 1.14 The Government has a well-developed and co-ordinated approach to protecting our national security. However, it lacks comprehensive statutory powers in relation to the ownership and control of businesses and other entities which could be used to undermine our national security.
- 1.15 Ownership and control of entities and assets could be used to facilitate any of three different types of risk to national security:
- [disruption or destruction](#) – the ability to corrupt processes or systems;
  - [espionage](#) – the ability to have unauthorised access to sensitive information or contribute to the proliferation of weapons; or

- **inappropriate leverage** – ability to exploit an investment to dictate or alter services or investment decisions or in other geopolitical or commercial negotiations.

## Technological advances

- 1.16 Technological advances continue to fundamentally change the way we live our lives. For example, continued advances in computing power and connectivity in and out of the home are changing the way people interact with their family, friends, businesses and the government. These advances present huge opportunities to positively transform our lives. But they also present complex challenges, including to national security.
- 1.17 These advances raise particular national security concerns in certain sectors of the economy. That is why, as its first step in reform earlier this year, the Government introduced into Parliament amendments to the Enterprise Act 2002 in order to enable Government to intervene in more mergers that may raise national security concerns in three areas of the economy – dual use and military use, quantum and computing hardware technologies. This involved, for these parts of the economy, reducing the UK turnover threshold from over £70 million to over £1 million and removing the requirement for an increase in the share of supply as a result of the merger.<sup>2</sup> While these changes were an important step, addressing the full range of issues requires full reform and primary legislation.

## The proposed reforms will maintain the UK's openness and economic success

- 1.18 The Green Paper also emphasised how the UK's openness, including to foreign investment, had played a key role in delivering a strong economy.
- 1.19 Foreign direct investment into the UK leads to tangible and considerable benefits for our economy and citizens. It can bring new jobs – almost 76,000 new jobs were created by inward investment projects in 2017/18.<sup>3</sup> Foreign direct investment can boost domestic labour productivity, through bringing new technology, skills, and managerial best-practice to the UK, and promoting

---

<sup>2</sup> The Government published further guidance, '[Enterprise Act 2002: Changes to the turnover and share of supply tests for mergers](#)', about these changes.

<sup>3</sup> Department for International Trade, 'Inward investment results 2017 to 2018', <https://www.gov.uk/government/statistics/department-for-international-trade-inward-investment-results-2017-to-2018>

the diffusion of ideas through collaborating with UK institutions and businesses.<sup>4</sup>

- 1.20 This is why any reforms must successfully protect our national security whilst maintaining our position as a world-leading destination for FDI and international research and innovation partnerships. Maintaining an investment screening mechanism for national security purposes does not automatically create a barrier to foreign investment in the UK.
- 1.21 As of 2017, the United Kingdom had the third highest inward FDI stock in the world (\$1.6 trillion), only behind the United States (\$7.8 trillion) and China including Hong Kong (\$3.5 trillion).<sup>5</sup> Measured relative to GDP, the UK's FDI stock was 45% (on average between 2006 and 2016) of our national economy, the second highest among G20 countries.<sup>6</sup> On average between 2007 and 2017, the UK was one of the world's top FDI destinations – ranking third among the G20 nations for flows of inward FDI.<sup>7</sup>
- 1.22 The UK is, of course, not only a recipient of FDI. UK-based businesses are also active across the world economy: in 2017, foreign companies spent £35 billion acquiring 254 UK companies, while UK companies spent £77 billion acquiring 150 overseas companies.<sup>8</sup>

## Other governments' and organisations' responses to these challenges

- 1.23 The challenges described above – hostile state activity, technological developments and economic changes – are not unique to the UK. They are global developments. As such, the UK Government is not alone in recognising these challenges and considering and adapting its approach accordingly. [Germany](#), [Japan](#) and [Australia](#) are amongst countries which have made reforms recently.

---

<sup>4</sup> See evidence highlighted in <https://bankunderground.co.uk/2017/08/17/foreign-owned-firms-and-productivity>.

<sup>5</sup> Data from United Nations Conference on Trade and Development (UNCTAD) World Investment Report 2018, <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2130>.  
<http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2130>.

<sup>6</sup> Data from United Nations Conference on Trade and Development (UNCTAD) Data Centre, <http://unctadstat.unctad.org/EN/>, UK's annual average FDI stock as a proportion of its GDP (2006 to 2016).

<sup>7</sup> Data from United Nations Conference on Trade and Development (UNCTAD) World Investment Report 2018, <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2130>.

<sup>8</sup> Source: Office for National Statistics (2018), '[Mergers and acquisitions involving UK companies: October to December 2017](#)'.

- 1.24 Additionally, the European Commission has proposed an [EU-wide FDI screening regulation](#) to provide a cooperation mechanism between Member States, to mitigate against potential security risks posed by FDI from third countries into the EU. The proposal sets out procedural requirements for Member States both with and without a formal national security screening mechanism, as well as annual reporting obligations. This cooperation mechanism also obliges Member States to share information on their screening activity, including live cases, in order for other Member States to provide comments. There is also the facility for the European Commission to provide non-binding opinions.
- 1.25 If the proposed EU Regulation comes into force before the end of the Implementation Period, the UK will become subject to it until the Implementation Period concludes in December 2020. The Government will carefully consider what the EU Regulation means for both our existing powers under the Enterprise Act 2002 and the proposed legislation set out in this White Paper.

# Chapter 2 – The Green Paper consultation and responses

## Summary

- the 2017 Green Paper sought views on three options – an expanded call-in power, a mandatory notification regime, and a combination of both.
- there was, narrowly, more support for an expanded call-in power rather than a mandatory notification regime. There was very little support for the combined option.
- all respondents emphasised that any new regime needed to ensure predictability and transparency, and minimised administrative burdens.
- the Government has decided to pursue the expanded call-in power option with a voluntary notification regime. It will supplement this legislation with clear guidance about the most likely areas of interest in order to provide further certainty.
- the White Paper seeks input on the detail of how this option will be implemented.

## Introduction

2.01 This chapter summarises the key policy options described in last year's Green Paper and the Government's decision about the way forward.

## The Green Paper

2.02 Recognising the complex nature of these areas of policy and law, the Government has taken a considered and consultative approach to reforms.

2.03 In developing its proposals, the Government reviewed its existing statutory and regulatory powers and also examined the equivalent approaches and regimes in other countries. In October 2017, the Government then published a Green Paper, the [National Security and Infrastructure Investment Review](#).

2.04 The Green Paper sought respondents' views on three broad potential options to address the challenges described in the previous chapter. These were:

- an expanded version of the call-in power, modelled on the existing power within the Enterprise Act 2002, to allow the Government to scrutinise a broader range of transactions and events for national security concerns (detailed from paragraph 115 of the Green Paper);

- the introduction of a [mandatory notification regime](#) for foreign investment in key parts of the UK economy (from paragraph 127 of the Green Paper); or
- [both of the above](#) – a combination of both reforms (cited in paragraph 114).

2.05 The Green Paper also invited comments on a number of more detailed components required to inform the final set of reforms. For example, the potential powers to request information to enforce the reforms or what guidance accompanying the new regime could best cover.

## Responses to the Green Paper

2.06 During the subsequent three months of consultation, the Government received 45 written responses and met a further nine organisations. Alongside this White Paper, the Government has published a detailed account of their responses; this section seeks only to provide a summary.

### Overall themes

2.07 Overall, most respondents recognised the challenges facing the Government and the need for reforms to protect national security.

2.08 Across almost all responses, respondents typically stressed a number of key themes in their views. Many of those replicate the principles for the Government's review as set out in the background to the Green Paper and to this document – the need for [proportionate powers](#) and [transparent processes](#) for example. There was also frequent reference to providing [certainty](#) wherever possible, and [predictability](#).

### Views about the three broad options

2.09 There was, narrowly, more support for an expanded call-in power rather than a mandatory notification regime. Very few respondents favoured the combined option.

2.10 Respondents in favour of an expanded call-in power emphasised it was the most proportionate approach – ensuring that the Government only intervened in those specific deals that might raise national security risks. However, many respondents in favour of the option also stressed the need for clarity about the Government's interests and intentions to provide more certainty for businesses and investors about a broad power.

2.11 The option of mandatory notification was favoured by some respondents primarily because of the certainty they considered it to provide. This was

because the changes would be focused on the areas of the economy where national security risks were most concentrated (described as ‘essential functions’) and the types of trigger event most likely to give rise to these (foreign investment that meets certain thresholds or establishes other means of control).

- 2.12 Those opposed to a mandatory notification regime, by contrast, raised significant concerns about the ‘deadweight’ loss – that is, the cost and time (for businesses and the Government) that would be taken up with the notification and screening of transactions with no national security interests. Some respondents also expressed concern that a mandatory notification regime could undermine the UK’s reputation as an open economy.
- 2.13 There was very little support voiced for the third option combining both components – instead, respondents described this as having the costs of the mandatory regime without the certainty it provides given that the Government would reserve the right to intervene into any part of the economy.

### **The Government’s decision**

- 2.14 Having considered the consultation responses, and undertaken further analysis, [the Government has decided to pursue an expanded call-in power with a voluntary notification regime](#). It has concluded that the constantly changing national security landscape necessitates a broad and flexible power for the Government to intervene in the relatively rare but specific circumstances where investments, acquisitions or other events can give rise to national security concerns.
- 2.15 It has concluded that a mandatory notification regime, whilst potentially giving some certainty to businesses and investors, would necessarily not always be able to keep pace with this evolving landscape. To provide this certainty would instead require frequent amendments or use of the ‘designation’ power described in the Green Paper.<sup>9</sup> This would, the Government concluded, remove the certainty which was the key benefit of such an approach.
- 2.16 The Government is also mindful of the additional costs associated with a mandatory notification regime both for investors and for the Government. It does not wish to impose any unnecessary burden on either businesses or the taxpayer given the relative rarity of trigger events that raise national security risks.

---

<sup>9</sup> As described from paragraph 136 of the Green Paper, the Government sought views on the ability for it to bring individual businesses or assets (that are part of national infrastructure sectors) into scope of a mandatory notification regime. This would be done by the Government ‘designating’ them.

- 2.17 Mindful of respondents' views that it was not always clear as to where national security concerns arise, the Government has concluded that the expanded call-in power should be accompanied by a [clear and detailed statement of policy intent](#). This document will describe the key factors that make it more likely that a trigger event would be of national security interest to the Government and so should assist parties in determining when they should submit a notification for screening.

## The White Paper

- 2.18 The remainder of this White Paper provides detailed explanations of various proposed components that, together, will form the Government's new regime.
- 2.19 The Government considers that those components, together, provide for a new regime that will work for both the Government and businesses.
- 2.20 While clear in its goal and overall approach, the Government welcomes respondents' input on the precise mechanisms, tests, details and draft statement of policy intent needed to finalise the reforms. Wherever possible, the Government seeks consensus on these important issues.

# Chapter 3 – The trigger events which could be called in

## Summary

- acquisitions of control over entities or assets only rarely raise national security concerns, but these can occur in a [range of ways](#).
- the new regime will therefore cover a broader range of transactions and trigger events, potentially including:
  - acquisitions of more than [25% of votes or shares](#) in an entity;
  - acquisitions of [significant influence or control over an entity](#);
  - [further acquisitions of significant influence or control over an entity](#) beyond the above thresholds;
  - acquisitions of more than [50% of an asset](#);
  - acquisitions of [significant influence or control over an asset](#).
- together, these trigger events will also ensure that certain [new projects](#) that may raise national security risks can be scrutinised.
- there may be exceptional instances where [loans or conditional acquisitions](#) (like futures options) give rise to national security risks.

## Introduction

- 3.01 The new reforms must ensure that Government can prevent national security threats arising however hostile actors acquire control or influence over entities or assets. As described in Chapter 1, this requires the Government to be able to call in a broader range of events than it can currently do under the Enterprise Act 2002 or other legislation.
- 3.02 The Government encourages parties to submit notification in relation to those trigger events which they believe raise national security concerns.
- 3.03 The Government invites respondents' views about the extent to which its draft tests provide the clarity and certainty it seeks to provide to parties.

## The current position

- 3.04 At present, the Enterprise Act 2002 is the key legislative vehicle for Government to scrutinise potential national security issues that may arise from mergers. Section 23 of the Act defines a relevant merger situation as two or more enterprises ceasing to be distinct. The Government has the power to

intervene on specified public interest grounds where this occurs and where the turnover or share of supply test is met

- 3.05 These powers only apply, in the most part, to mergers where the acquired company has an annual UK turnover of more than £70 million or the merger should result in the creation of, or increase in, a 25% or more combined share of sales or purchases in the UK (or in a substantial part of it), of goods or services of a particular description.
- 3.06 The only exceptions to this rule are:
- mergers related to certain defence or media organisations where there are no turnover or share of supply tests;<sup>10</sup> and
  - mergers related to businesses which produce or design goods covered by parts of the Strategic Export Control Lists and/or certain advanced technological goods where the UK turnover threshold is over £1 million and/or where there does not need to be an increase in the share of supply.<sup>11</sup>
- 3.07 The 2017 Green Paper also described other relevant powers and levers currently available to protect national security, including sector-specific regulation, export control and use of ‘Golden Shares’.

## The need for reform

- 3.08 As Chapter 6 of the Green Paper described, the Government has concluded that technological, economic and national security/geopolitical changes since 2002 mean that the existing tests limit its ability to ensure that hostile actors cannot undermine our national security through acquiring control over key businesses or assets.
- 3.09 The Green Paper described the Government’s intention to expand the range of circumstances where it can intervene in order to protect national security. Most respondents to the subsequent consultation recognised that changing circumstances justified the Government reviewing and updating its powers accordingly.
- 3.10 However, some respondents raised some concerns about the specific proposals described in the Green Paper, in particular the expansion of the Government’s powers to new projects and/or sales of assets. One

---

<sup>10</sup> These mergers are covered by the Special Public Interest Regime as set out in section 59 of the Enterprise Act 2002.

<sup>11</sup> The businesses in scope of these thresholds are set out in section 23A of the Act as introduced earlier this year.

respondent, representing views held by others, raised concern that the proposed expansion would mean the Government's powers would "be very wide" and, without clear guidance, this could lead to uncertainty.

- 3.11 The Government has considered all consultation responses carefully. It has concluded that it remains an important step to expand its powers in relation to national security – for example, removing the link to businesses' turnover or share of supply, and ensuring that the acquisition of assets can trigger Government scrutiny.

## The trigger events covered by the proposed legislation

- 3.12 The Government therefore proposes to introduce legislation that would enable it to scrutinise more circumstances where acquisitions of control over entities or assets may raise national security risks. These could include:

- the acquisition of more than 25% of the votes or shares in an entity;
- the acquisition of significant influence or control over an entity;
- the acquisition of further significant influence or control over an entity beyond the above thresholds;
- the acquisition of more than 50% of an asset; and
- the acquisition of significant influence or control over an asset.

- 3.13 Collectively, these will be known in the proposed legislation as "trigger events".

- 3.14 The Government recognises that this constitutes a significant expansion in the circumstances in which it currently has powers to intervene to protect national security. However, this is necessary to provide the breadth of powers the Government needs to protect national security. It invites respondents' views about the detailed proposals for each.

- 3.15 The Government will also publish detailed guidance in the form of a [statement of policy intent](#). This will provide detail about, amongst other things, the areas of the economy where trigger events are most likely to raise national security concerns. This is discussed in more detail in the following chapter, including how the document will be subject to Parliamentary approval. A draft of the statement of policy intent is published alongside this document.

## Ensuring that control of entities cannot be used to undermine national security

- 3.16 Acquisition of entities remains a clear means by which a hostile actor may gain the capability and means to undermine national security. By shaping the

strategic and operational direction of an entity, a hostile party could therefore undermine national security risk in the manner described in Chapter 1.

- 3.17 The Enterprise Act 2002, which made reforms to the UK's regime for the control of mergers, recognised this and granted powers to ministers to intervene in 'relevant merger situations' of enterprises where specific public interests, including national security, arise.
- 3.18 The new reforms will go further in ensuring that the Government can scrutinise a broader range of means by which hostile actors can gain control over entities and assets in order to protect national security.

### **The types of entities to which the legislation will apply**

- 3.19 The Government intends to ensure that its reforms can protect national security, regardless of the form of the legal structures involved in a transaction or other trigger event.
- 3.20 Businesses can be established or re-structured in various forms and for various means – for example, to limit a founder's personal liability for its debts, or for other legal or financial reasons. Therefore, the Government proposes legislating such that its powers in this area relate to control being acquired over any "entities". The legislation would include an indicative but non-exhaustive list of the types of entities to which the reforms will apply, including private or public companies and partnerships.
- 3.21 This is also designed to ensure that the legislation could not be undermined or bypassed by a business or deal being structured so as to avoid scrutiny, while also ensuring that it keeps up-to-date with any developments in corporate law or practice.
- 3.22 The Government has concluded that the new national security-focused powers will not use any reference to an entity's turnover or share of supply. As described in the Green Paper, these are not an appropriate measure of whether a business is likely to pose national security threats should a hostile actor gain control.
- 3.23 The Government recognises that, by not including these tests, businesses will not have what have been, to date, key 'safe harbours' which provide comfort that certain transactions will not be subject to scrutiny. The Government has considered this step carefully. However, it has concluded this is a vital component of its reforms and one necessary to ensure that they cannot be deliberately undermined by hostile actors. Further, the Government considers that, by providing a clear and detailed statement of policy intent, this would

provide businesses with clarity about the transactions and other events that are most likely to be of national security interest to the Government.

### **Trigger event 1: Acquisition of ownership of more than 25% of an entity's votes or shares**

3.24 The Green Paper explained that the Government was minded to use more than 25% of a company's shares or votes as one such 'limb' of the statutory test, in line with the figure used by the CMA when assessing whether enterprises cease to be distinct. It is also the threshold set by the People with Significant Control register introduced by Schedule 1A of the Companies Act 2006.

#### *Green Paper consultation responses and the Government's decision*

3.25 As described in the summary of consultation responses published alongside this White Paper, there was a mixed response to the proposal. Some saw considerable benefit in consistency with these other statutory schemes, while some proposed that the threshold should be set at 30% in order to be aligned with the threshold used by the Takeover Panel's [Takeover Code](#) as the level at which effective control is obtained. Other respondents proposed that the threshold for a new national security-focused regime should not be set in relation to schemes designed for other purposes, but should instead be targeted at the threshold at which such threats can be realised.

3.26 The Government has considered this issue carefully. It has concluded that the acquisition of more than 25% of votes or shares remains the most appropriate threshold for this trigger event and intends to legislate to this effect.

3.27 However, a trigger event simply meeting this threshold is not enough for the Government to call it in for scrutiny. Chapter 6 describes the requirements that would need to be met in order for the Senior Minister to be able to call in a trigger event for a national security assessment. The statement of policy intent will provide clarity to business as to when this is likely to arise.

#### *The rationale for using over 25% of votes or shares as a trigger event threshold*

3.28 As a general rule, any one party requires a majority (i.e. more than 50%) of votes or shares in order to have control over the company's decisions in most matters. However, in practice and in law, parties with fewer shares or votes can exercise significant influence over its operations, policies or appointments.

3.29 For example, under the Companies Act 2006, a number of key decisions require a special resolution to be passed. This includes amending a company's articles of association or voluntarily winding up the company. A

company's articles of association can also specify any other types of decisions which require a special resolution in order to be passed. Section 283 of the same Act (which followed the approach of section 378 of the Companies Act 1985 in this regard) specifies that a company requires a majority of at least 75% of votes in order to pass a special resolution of the members. This means that a person with more than 25% of voting rights can block a special resolution from passing and therefore exert control over certain decisions relating to the company.

- 3.30 In assessing whether a transaction results in enterprises ceasing to be distinct, the CMA considers that a share of voting rights of over 25% is likely to be seen as conferring 'material influence' over the policy of, and thus control over, an enterprise, even when all the remaining shares are held by only one person, as set out in its [mergers guidance on jurisdiction and procedure](#). This is because such a shareholding generally enables the holder to block special resolutions.
- 3.31 The Government considers that there is considerable benefit from taking a consistent approach with the thresholds used by the CMA and also by the People with Significant Control register. While each focuses on a different policy objective, the Government expects that a broadly consistent approach will aid businesses and their advisers in complying with the requirements in a more efficient manner. As discussed in the next section, there will be some areas in relation to the significant influence and control limb where a more tailored approach is necessary to reflect national security-specific issues.
- 3.32 The Government also recognises that (in practice) this constitutes a substantial share, particularly in a public company. For example, based on a sample of UK-incorporated public companies, only 27% reported any one or more shareholder which separately controlled more than 25% of its shares.<sup>12</sup>
- 3.33 To ensure the breadth of the reforms' coverage and to protect against them being deliberately bypassed by a hostile actor, the Government intends to legislate so that a threshold of over 25% of votes or shares applies to all entities which have a share capital or equivalent, not just companies. Any transaction or other means by which a party crosses this threshold – whether as a single trigger event or the last of a series of acquisitions – would constitute a trigger event.

---

<sup>12</sup> Source: internal analysis based on a sample of 1,187 UK incorporated public companies, drawn from Capital IQ.

## Trigger event 2: Acquisition of significant influence or control over an entity

- 3.34 No one threshold in relation to shares or votes can be appropriate in every circumstance – entities can, in practice, be influenced or controlled by a party with votes or shares beneath any threshold that could be established in legislation. Therefore, the Government intends to legislate for a separate ‘limb’ alongside that related to the acquisition of votes or shares in an entity. This will cover other means by which a party can acquire significant influence or control over the target entity in such a way that could be used to undermine national security.
- 3.35 In assessing whether a transaction results in enterprises ceasing to be distinct, the CMA also currently considers shareholding of 25% of voting rights or below, and in particular, whether given other factors (including actual past voting patterns), the acquiring party has the ability to block special resolutions in practice (see paragraphs [4.20 – 4.22 of its guidance](#)). The CMA may also consider other sources of material influence (including Board representation).
- 3.36 The rights or abilities granted to an acquiring party would depend on a variety of other factors. In the case of [legal or contractual rights](#), for example, a company’s constitution may set specific thresholds that must be reached for shareholders to make certain decisions. Parties may also acquire certain rights as part of their share purchases – for example, the ability to appoint a Board member of their choosing.
- 3.37 Shareholders’ practical [abilities](#) of control or influence may also be determined by the type and size of other parties’ holdings. For example, a large number of parties each with only a very small number of shares will leave a large, but still minority, shareholder in a stronger position than if they were, for example, one of five equal shareholders.
- 3.38 It is for this reason that the Government also intends to legislate for there being a ‘significant influence or control’ test alongside the shares or votes threshold of over 25%. The Government recognises that some consultation respondents raised concerns that this test would be unclear and difficult for businesses to decide whether they should notify, which could lead to uncertainty. The Government does not agree with such an assessment; it believes that sufficient detail, clarity and accountability can be provided.
- 3.39 In particular, the Government proposes that the legislation would require it to publish a [statement of policy intent](#) about how “significant influence or control” should be interpreted for the purposes of this regime. The statement (or any subsequent changes to it) would be subject to debate and approval by both Houses of Parliament to provide oversight and accountability of what the

Government accepts is a key part of its reforms. More information about the statement and its content is provided in the next chapter.

- 3.40 The Government has published a draft of this statement alongside this White Paper and welcomes respondents' views about it. The statement draws from the statutory guidance on the meaning of significant influence or control published under Schedule 1A of the Companies Act 2006, but has been adapted to deliver the separate policy objectives in relation to national security.
- 3.41 The Government considers it important to have a wider concept of 'significant influence or control' for the purposes of national security because of the serious detrimental impact undermining national security could have on the UK. For instance, the statement sets out that 'significant influence or control' for the purposes of this legislation would be gained where another party acquires the right to appoint a Board member, rather than (as under the Companies Act 2006) a majority of the Board. This is because, in some circumstances, depending on the composition or size of the Board it could allow a person to influence the Board and the strategic direction of the entity. In addition, individual Board members can be responsible for particular tasks or have control over certain assets. So where a person has the right to appoint a Board member with particular important responsibilities such that the person would acquire, in effect, the ability to shape the direction and activities of an entity, that person would have significant influence or control over that entity.
- 3.42 The Government wishes to draw respondents' attention to a number of key components in this part of the draft statement:
- a party can have significant influence or control by virtue of a right and/or the practical ability;
  - that a party's influence or control is determined by an assessment of all ownerships, relationships, positions and personal connections;
  - the list of 'excepted persons' like employees and directors who, absent other circumstances, would not be considered to acquire significant influence or control.

### **Trigger event 3: Further acquisitions of significant influence or control over an entity**

- 3.43 The Government considers that there is a case for it to be able to intervene in any further or additional acquisitions of control over an entity which it considers may give rise to national security risks. This would apply whether or not the Government was notified about, or called in, the original trigger event.

- 3.44 The Government considers that there are, broadly, three main circumstances in which further acquisitions of control over an entity are likely to arise:
- the acquisition of over 50% of shares or votes (enabling a party to pass an ordinary resolution in accordance with the Companies Act 2006);
  - the acquisition of over 75% of share or votes (enabling a party to pass a special resolution in accordance with the Companies Act 2006);
  - the acquisition of further significant influence or control through new or additional rights (e.g. Board appointment rights), which may or may not relate to an acquisition of further shares or votes.
- 3.45 For example, if the Government does not call in the acquisition of 26% of a company's shares, it would be able to intervene should the acquirer gain additional shares taking them beyond 50%, provided that the additional acquisition gives rise to a national security risk.
- 3.46 This would also apply in the event that the party already had significant influence or control of an entity and then acquired another means of exerting significant influence or control. An example would be where a director who owned an asset important for the running of the company and used this to influence decisions relating to an entity, then acquired another means of exerting significant influence or control, such as a Board appointment right. By being able to appoint a Board member, depending on the composition or size of the Board or the specific Board member's role, the acquirer would have a new way of being able to shape individual Board decisions (as well as its overall direction) that could be used to undermine national security.
- 3.47 In all cases of such further acquisitions, [the Government would need to demonstrate that the further acquisition provided further significant influence or control and that the further acquisition gave rise to a risk to national security linked to that trigger event](#). Similarly, any remedy would need to apply to the further acquisition only.
- 3.48 As the draft statement of policy intent describes, the Government encourages notification about further acquisitions of significant influence or control in certain circumstances set out within the statement.
- 3.49 These provisions would apply in relation to trigger events relating to all parties – including those who may hold shares, votes or other means of influence or control before the regime comes into force. Those previous holdings would not be affected by this provision – any intervention would only relate to

those additional means of control being acquired by the party after the regime was enacted.

- 3.50 The Government considers that this approach strikes a reasonable balance in granting certainty, particularly in relation to long-held property including that held before the regime came into force, while ensuring the Government can address new threats that may emerge. The Government welcomes respondents' views on this particular component of the regime.

## Ensuring that control of assets cannot be used to undermine national security

- 3.51 The reforms described in this White Paper seek, in part, to protect businesses (and other entities) providing key services to the UK from national security-related hostile acquisitions; for example, ensuring that a hostile actor cannot acquire control over a business providing data-hosting servers to a defence contractor – this control could be used to obtain sensitive information about the country's military sites or potentially even to disrupt defence activities.
- 3.52 However, the reforms must also be designed to ensure that control over [assets](#) themselves cannot be acquired by those who wish our country harm. Without the regime covering this, a hostile party could evade the Government's oversight by buying the asset outright instead of acquiring the controlling entity.
- 3.53 In the example in the paragraph above, ownership of the servers providing the service could be a route to undermining our national security. By acquiring ownership of an asset, a hostile party could acquire the ability to direct its operations – by using, altering, destroying or manipulating the asset, they could undermine our national security.
- 3.54 National security concerns in relation to the acquisition of control over assets increasingly apply to [intellectual property](#). For example, an energy provider may use data servers which run on custom or specialist code provided by a third party. Any party acquiring control over the code (for example, buying the underlying intellectual property rather than the business that developed and maintains it) and being able to manipulate it could use this in a manner prejudicial to the UK's national security – either by monitoring or extracting the data on the server, for example, or by deliberately causing the failure of the service on which the energy providers depend.
- 3.55 In making the reforms that are the subject of this White Paper, the Government wishes to ensure it introduces a new, stable approach for the long term. Therefore, it wishes to ensure that the proposed legislation does

not permit ‘loopholes’ that could be exploited. Being able to block a hostile actor from buying a business but not being able to prevent it instead acquiring the key asset would be such a loophole.

- 3.56 Therefore, the Government will also expand its powers to scrutinise asset sales in order to ensure that its reforms in relation to entities cannot be deliberately undermined or bypassed.
- 3.57 The Government recognises that this constitutes a significant expansion in its powers. It welcomes any specific suggestions from respondents about how to ensure that its policy objectives are delivered in the most effective manner.

### **National security risks arising from land in proximity to other sites**

- 3.58 Acquisitions of land may give rise to national security risks as a result of the land’s location rather than its nature (for example, its current use). For example, the Government may well have a clear national security interest in the acquisition of land that is adjacent to or overlooks a national infrastructure site or a sensitive government facility. As such, land acquisitions of this type could be called in for national security assessment.
- 3.59 This risk may arise either by the acquisition of the land itself (as an asset) or by acquiring an entity which owns or controls the land. For example, rather than buying the land, a hostile acquirer may instead seek to buy the entity which owns the land adjacent to the sensitive site.
- 3.60 In either case, the Government expects that these ‘proximity risks’ are likely to arise only very rarely. The Government expects that the overwhelming majority of transactions relating to land in proximity to sensitive sites should not raise national security concerns.
- 3.61 In the rare event that these risks do arise, the Government will continue to consider the breadth of policy and non-legislative options open to it and seek to adopt the most proportionate option. In some circumstances, it may not be proportionate to prevent the acquisition of land in proximity to a sensitive site if, instead, the Government can increase the physical security checks at the facility which it is seeking to protect in order to address any national security risks.

### **The definition of an asset within the legislation**

- 3.62 The Government wishes to ensure that its proposed legislation is clear about the circumstances in which the transfer of control over an asset can be scrutinised for national security concerns.

3.63 The Government proposes that the legislation, recognising the broad circumstances where asset ownership can give rise to national security threats, uses a broad definition of ‘asset’ – namely, real and personal property, contractual rights and intellectual property (as defined below). This would include:

- property situated outside the United Kingdom; and
- a right arising under, or governed by, the law of a country or territory outside the United Kingdom;
- but would not include money.

3.64 The definition makes a clear distinction between physical and intangible assets.

#### *Real and personal property*

3.65 By including real and personal property the Government will be able to scrutinise the national security consequences in relation to the acquisition of ownership or significant influence or control over land and buildings and other physical assets (for example, infrastructure sites and equipment).

#### *Intellectual property*

3.66 National security threats increasingly arise in relation to intellectual property such as software code protected under copyright. It is important, therefore, that the proposed legislation permits the Government to scrutinise acquisitions of control over this type of asset. Including acquisitions of intellectual property within scope of the regime is – as is the case with other assets – a logical ‘backstop’ to ensure that the new regime cannot be circumvented.

3.67 The proposed legislation is not intended to cover, for example, the specialist knowledge or skills of employed individuals – it is important, therefore, that the draft definition provides a clear and specific list of those forms of intellectual property to which a trigger event would relate. The Government proposes using the following exhaustive list of intellectual property in the legislation:

- patents (including pending patents);
- registered designs;
- copyright;
- design rights;
- database rights; and
- any rights under the law of a country or territory outside the United Kingdom which corresponds with these rights.

3.68 The Government invites views as to whether this list is sufficient.

### *Property situated outside the UK*

- 3.69 Assets physically located outside the UK may still have the capacity to undermine our national security. For example, the supply of energy to the UK is provided, in part, by assets (such as deep-sea cables) located outside its geographical borders. Intellectual property rights may also arise outside the UK and yet be key to the provision of critical functions within the UK.
- 3.70 As described in Chapter 6, the Senior Minister could only exercise the power to call in a trigger event in relation to assets (or entities) outside the UK when it met a clear nexus test.

### **Changes in control over an asset made in the ‘ordinary course of business’**

- 3.71 The Government recognises that the proposed legal test for asset sales is broad. Notwithstanding this, [the Government expects to exercise its power to intervene into asset sales relatively rarely](#) – the power has been designed as a ‘backstop’ to prevent the new regime being bypassed. The Government’s initial analysis currently estimates that around a quarter of notifications (approximately 50) will concern asset-related trigger events each year. Like all trigger events, the Government’s initial analysis indicates that only half of these notifications would need to be called in for a national security assessment. This initial analysis indicates that around half of those that undergo that assessment would then be subject to remedies.
- 3.72 The Government does not intend that the power would be used in relation to ordinary business or consumer transactions.
- 3.73 For example, the Government may have a potential national security concern about the acquisition of control over a UK business that designs certain computer hardware components found in large numbers of electrical goods. An acquirer could gain the ability to ‘design in’ means by which it could remotely access the goods and manipulate them to undermine UK national security. Notwithstanding this risk, consumers’ purchases of the electrical goods could not, itself, raise a national security issue so it is not necessary for the reforms to cover these types of transactions.
- 3.74 The Government is continuing to consider how the call-in test could accordingly be structured to reflect the fact that it is not intended to relate to ordinary business or consumer transactions. The Government invites respondents’ views about this issue.

### **Trigger event 4: Acquisition of more than 50% of an asset**

- 3.75 The Government is examining the case for whether there is an appropriate ownership threshold that might represent a level of ownership at which a

hostile actor is more likely to be able to, on their own, control an asset or its operations or functions such that it might raise national security concerns.

- 3.76 The Government considers that acquiring a majority share (i.e. more than 50%) of an asset may, in some circumstances, provide a party with such an ability (as this may, in some cases, provide the means to control the asset or its operations or its functions without reference to others). Under this option, an acquisition of more than 50% of an asset would constitute a trigger event for the purposes of the proposed legislation.
- 3.77 The Government notes that, in some cases, majority ownership of an asset may not provide a party with the means to control the asset or its operations or its functions.
- 3.78 As a result, the Government welcomes respondents' views on this proposed trigger event and whether it offers a clear and objective threshold for where control of assets might give rise to national security concerns.
- 3.79 The Government also reiterates that it only expects to intervene into asset sales relatively rarely.

#### **Trigger event 5: Acquisition of significant influence or control over an asset**

- 3.80 In addition to the above, the Government considers that hostile actors may have the opportunity to realise national security concerns, in some circumstances, when acquiring less than the proposed threshold, if they acquire significant influence or control over an asset. By acquiring significant influence or control over an asset a hostile party may acquire decision rights over its operation, which could enable a party to use, alter, destroy or manipulate the asset in a way that could undermine our national security.
- 3.81 Therefore, in the same manner that the Government intends to legislate to cover trigger events involving 25% or less of an entity's shares or votes but nonetheless granting significant influence or control over it, the Government intends to ensure that a purchase of an interest in an asset or an entity holding the asset granting the acquirer significant influence or control over an asset can be called in for national security concerns. The Government welcomes respondents' views on this proposed trigger event.
- 3.82 A statement of policy intent will (subject to Parliament's approval) be published providing clarity and transparency as to how significant influence and control can be acquired over an asset. A draft of that statement is published alongside this White Paper. The Government invites comments about its content.

- 3.83 The Government wishes to draw respondents' attention to a number of key components in the relevant section of the draft statement, including:
- an acquirer is generally only considered to gain significant influence or control over an asset if the trigger event involves some acquisition of ownership, either of an entity owning the asset or of the asset itself;
  - preferential access to an asset, which is access that is greater than the access generally available to the public at large, does not constitute a trigger event or an indication of significant influence or control. However, where preferential access is gained as a result of a trigger event it will be relevant for the purpose of the national security risk assessment.
  - the acquisition of a licence related to an asset (including intellectual property) is a trigger event if it provides the licensee with the means of using (or manipulating) the asset in question; and
  - the list of 'excepted persons', like employees and directors who, absent other circumstances, would not be considered to acquire significant influence or control over an asset.

#### **Other statutory powers that are relevant to asset sales**

- 3.84 The UK's export control regime (set out under the Export Control Act 2002) is an important and effective tool for controlling the export of 'strategic goods'. The UK's Export Control Joint Unit (ECJU) issues licences for controlling the export of goods including military equipment and technology, dual-use items (those that can be used for both civil and military purposes), products that could be used for torture and radioactive sources.
- 3.85 After the introduction of the reforms described in this White Paper, [the export control regime will remain the key means of restricting trade in strategic goods where this might raise national security risks.](#)
- 3.86 The Government wishes to ensure that the new reforms are as proportionate as possible, and are not used instead of other, more targeted or proportionate policy levers. As such, where national security concerns relate solely or primarily to the *export* of goods, the Government expects that the export control regime would remain the primary means of protecting national security.
- 3.87 However, a hostile party's acquisition of an asset that does not leave the UK might still raise national security concerns (for example, acquiring control over parts of the UK's physical national infrastructure) and so export control would not be a viable policy response. It is important, therefore, for these reforms to sit alongside the export control regime.

## New projects

- 3.88 In its 2017 Green Paper, the Government described its intent to expand its powers to cover new projects, such as new developments and other business activities that are not yet functioning enterprises but can reasonably be expected to have national security relevance.
- 3.89 The proposed legislation would, through the proposed definitions of assets and entities and the proposed call-in test, allow the Government to intervene in new projects as and when the trigger events set out above occur. This is because the acquisition of ownership or the acquisition of significant influence or control over an asset or the acquisition of ownership or significant influence or control over an entity that is developing a new asset could, depending on the facts of the case, be a trigger event.
- 3.90 The second limb of the call-in test explained in Chapter 6 refers to the national security risks that may be raised by entities due to the “nature of their activities” and by assets due to their “nature”.
- 3.91 In the case of new projects, “nature” will be determined on a case-by-case assessment of the national security risk posed by the entity’s activities or the asset at that point time. This means that investments in half-complete national infrastructure developments, for example, could (depending on the facts of the case) be trigger events that could be called in by the Senior Minister if those developments pose a risk to national security.

### **Example of how new projects will be covered by the regime’s trigger events**

Company A is developing new technology with the potential to substantially improve the effectiveness of existing weapons systems. If Company A is acquired by a hostile party, this could undermine our national security due to the nature of Company A’s activities in developing this technology.

Company A seeks investment and Investor B offers funding in return for 40% of shares in Company A.

Because this would involve the acquisition of more than 25% of shares or votes, this would be a trigger event in which the Government could intervene if it reasonably suspected that the trigger event may give rise to national security risks at that time due to the nature of Company A’s activities in developing this technology.

### **Example of how new projects will be covered by the regime's trigger events**

Company C is building a new civil nuclear power station, which includes the development of a new nuclear reactor (Asset Z).

During construction, Company C gets into financial difficulty and abandons the project. Seeking to regain some of their losses, Company C looks to sell the half-completed Asset Z to Investor D.

This would be a trigger event in which the Government could intervene if it reasonably suspected that it may give rise to national security risks because of the nature of Asset Z. Asset Z may raise national security risks because the parts of it that have already been built were based on unique designs and may, for example, enable a hostile party to replicate these techniques, or recreate this capability. As such, even though Asset Z is not operational it still has the potential to pose a risk to national security.

### **Whether, how and when a loan may constitute a trigger event**

- 3.92 The proposed legislation will ensure that acquisitions cannot avoid scrutiny by being artificially structured as a loan. There may be particular, but **very rare**, instances where loans could give rise to national security concerns.
- 3.93 For example, a lender may extend a loan to a business with a particular asset secured as collateral in the case of default. This would not, in itself, give rise to a national security risk. However, if the lender acquired control over the asset such that the asset could be misused so as to give rise to national security concerns *and* the lender had hostile national security intent, it is important that the reforms permit the Government to intervene in such circumstances.
- 3.94 For the avoidance of doubt, **the overwhelming majority of loans raise no national security concerns**. This remains the case even in relation to businesses operating in, or supplying goods or services to, the businesses highlighted in the draft statement of policy intent as those where the Government has particular national security-related interests.
- 3.95 However, the Government must ensure that its reforms can deal with the very rare circumstances where loans may be a vehicle through which national security may be put at risk. It also aware that, absent the proposed legislation applying to loans, a determined hostile actor may be able to structure an acquisition in such a way as to avoid scrutiny by the Government.

- 3.96 There are three stages at which loans may, in certain circumstances, lead to national security concerns arising:
- **agreement**: at the point where a loan is extended;
  - **default**: where a borrower defaults such that the lender has the legal right to seize the collateral; or
  - **acquisition**: where the lender is actually acquiring ownership or significant influence or control over the collateral.
- 3.97 Only the third of these stages (acquisition) would automatically constitute a trigger event which could be called in for assessment. The first two stages (agreement and default) would only be trigger events where the lender actually exercises significant influence or control over the collateral.
- 3.98 At the first of these stages, a lender does not automatically gain significant influence or control over a collateral, whether entity or asset. **Therefore, the Government does not wish to provide that the extension of a loan, in itself, can constitute a trigger event.**
- 3.99 Significant influence or control is also not automatically gained at the point of default. In many cases, even when default theoretically permits a lender to seize an asset as collateral, parties will more likely be in negotiations about repayment structures for example. **Therefore, the Government does not consider that the point of default, in itself, can be considered a trigger event permitting an intervention.**
- 3.100 The proposed legislation, therefore, would provide that the extension of a loan or the defaulting on it are not, in themselves, trigger events where no significant influence or control is acquired.
- 3.101 However, either of these two points could involve a hostile actor acting as a lender acquiring significant influence or control in certain limited circumstances. This could apply, for example, where unusual clauses are attached to the loan at the outset requiring sensitive, non-commercial data to be provided throughout the period of the loan's repayment. Alternatively, where there has been a default on the loan but no attempt to formally seize an entity as collateral, a lender may demand that their representative attends Board meetings thus providing them a means to significantly influence its decision-making. It is these unusual instances where the Government wishes the proposed legislation to ensure that it can intervene in the lender acquiring control to protect national security.
- 3.102 Therefore, the intention is that **where significant influence or control is gained either at the point of an agreement or at the point of default on a loan, it will**

constitute a trigger event that can be called in for scrutiny. To do so, the other limbs of the call-in test (including the risk to national security) would need to be met.

3.103 The draft guidance in relation to significant influence and control included in the draft statement of policy intent published alongside this White Paper provides further details on how this term should be interpreted in relation to loans.

## Whether, how and when a conditional acquisition, such as futures or options, may constitute a trigger event

3.104 The reforms must also take a clear and proportionate approach in relation to ‘conditional acquisitions’ – that is, those agreements which would grant a party control over an entity or asset in the event that a particular condition is met. For example, two parties may sign a contract granting one the right to buy the other’s shares in a company once those shares hit a certain price.

3.105 As in the case of loans, [the vast majority of these agreements raise no national security concerns](#). However, the proposed legislation must be comprehensive in ensuring that the Government has powers to intervene whenever national security concerns might arise.

3.106 In broad terms, there are three stages involved in a conditional acquisition: agreement, a condition being met, and an acquisition occurring:

- [agreement](#): parties A and B sign a contract, permitting A to buy B’s shares in entity E when external condition C (such as E’s share price hitting a certain figure) is met;
- [condition met](#): C occurs – A now has the right to acquire B’s shares;
- [acquisition occurs](#): at any point when C is met, A decides to acquire B’s shares.

3.107 In line with any other means by which control is acquired over an entity or asset, the third stage would constitute a trigger event allowing the Government to assess whether it has any national security implications.

3.108 The first two stages, in contrast, involve no change in control over the entity or asset in question. There is also no guarantee that the condition (stage two) arises such that an acquisition (stage three) could actually take place. Given

this, the first two stages do not provide a party with control over an asset and are not considered trigger events.<sup>13</sup>

- 3.109 However, some businesses or investors may, in fact, wish to notify a conditional acquisition at the agreement stage. This may allow them to establish whether or not the Government had national security concerns in the event that the party sought to exercise its rights once the condition was met. As the signing of such an agreement is not a trigger event, no valid notification could be submitted for the Government's screening. A notification in respect of a conditional acquisition should only be considered at the stage where the actual acquisition is in progress or contemplation which is when the condition has been satisfied or is close to being satisfied.
- 3.110 An alternative approach would be to expand the types of trigger events to include conditional rights – i.e. those that would be acquired if a condition has been satisfied. However, this would significantly expand the scope of the proposed legislation.
- 3.111 On balance, the [Government considers that the better approach is not to treat the 'agreement' stage above as constituting a trigger event](#). It considers that informal dialogue with the Government may be sufficient to provide the certainty some parties may seek in this context. However, it welcomes respondents' views about this.

## The trigger events tests will take account of others' holdings

- 3.112 In order to ensure that all relevant factors are taken into account in determining whether a trigger event has occurred, and to ensure that the reforms cannot be circumvented, the proposed legislation would follow the broad approach taken by the Companies Act 2006 in looking 'across' and 'up' parties' holdings as specified below.

### Persons sharing a common purpose and connected persons

- 3.113 The proposed legislation would establish that two or more parties acting with a common purpose in relation to an asset or entity will be treated as a single person. The Government considers this a sensible and essential provision to avoid the reforms being bypassed – for example, parties A and B each acquiring 20% of a company's shares with plans to coordinate their votes should be treated as one acquiring party.

---

<sup>13</sup> The Senior Minister can intervene in the third stage in contemplation of the trigger event, which is when the condition is close to being met and (in the case of an option) there is evidence that the party intends to exercise their right. Chapter 6 provides further information about how the call-in test will operate in relation to intervention before, or after, a trigger event takes place.

3.114 Alongside this provision, the Government intends that certain connected persons, such as spouses or relatives, are to be treated as assumed to be acting with common purpose. For example, if parties A and B in the preceding paragraph were married, they would be treated as a single person for the purpose of determining whether a trigger event has, or will, occur.

### **Indirect control**

3.115 In all trigger events, the proposed legislation would be structured so as to cover both direct and indirect holdings. This is important to reflect the often complex structures employed by entities for a variety of reasons, and also to protect against the reforms being circumvented.

3.116 Part 1 of Schedule 1A of the Companies Act 2006 provides a clear basis as to how legislation can take account of indirect holdings. The Government proposes mirroring this structure and approach in relation to the new national security-related reforms.

3.117 In summary, this means that a party has indirect control over an entity if it has the means to direct or control the intermediate entity or entities via which the control is exercised. The party would need to have a majority stake in the intermediate entity or entities, for example holding more than 50% of the intermediate entity's voting rights, or satisfy any of the other requirements for holding a majority stake, in order to be considered as having indirect control over an entity or asset owned by the intermediate entity.

#### **Example of how the indirect control provisions work**

Person P owns 20% of business A which delivers an essential function on which the UK is dependent. Person P also owns 51% of business B which is a majority stake.

Business B seeks to acquire 6% of A's shares.

Because P has a majority stake in business B, once business B acquires a stake in business A, person P will acquire 6% of business A indirectly through her majority stake in business B. As a result, this transaction would take P's total holdings in business A to more than 25% and could, if it met the other limbs of the call-in test, constitute a trigger event and be called in for the national security assessment.

## When a trigger event may occur unintentionally

- 3.118 In most cases, obtaining significant influence or control over an entity or asset is a deliberate result of the acquirer's strategy and decision-making.
- 3.119 There may, however, be instances when an individual inadvertently or involuntarily acquires shares or votes that takes their collective holdings over the 25% threshold in the proposed legislation. For example, a person may inherit shares from a deceased family member that causes their holdings to increase to more than 25%.
- 3.120 Alternatively, a person may acquire significant influence or control due only to other parties' deliberate actions.

### **Example of involuntary control being acquired through other parties' actions**

Individuals A and B own 80% and 20% of a company's shares respectively.

A decides to sell their shares. These are acquired by a large number of new investor, each of whom have no more than 5% of the company's shares.

As a result of this process, B has become the largest single shareholder and has, in practice, the means to control the business's strategy.

In the event that the Senior Minister had a reasonable suspicion that B's position gave rise to national security concerns, the Senior Minister could call this in to assess these risks.

- 3.121 Chapter 8 describes the means by which the Senior Minister can prevent or mitigate risks to national security through the imposition of remedies. This includes a requirement that any remedy is both necessary and proportionate. In making this assessment in relation to control that was obtained involuntarily, the Senior Minister may conclude that it would not be proportionate to unwind a trigger event.

### **Consultation Question**

1. What are your views about the proposed tests for trigger events that could be called in for scrutiny if they met the call-in test?

# Chapter 4 – The statutory statement of policy intent

## Summary

- the Government will publish a **statement of policy intent** which will:
  - provide more information about **where trigger events may give rise to national security risks**; and
  - set out **how the Senior Minister expects to exercise the call-in power**.
- when exercising the call-in power, the Senior Minister's assessment about whether a trigger event may give rise to a national security risk will involve the consideration of the statement of policy which covers three risk assessments, all of which will be described in the statement:
  - the **target risk** – could the entity or asset subject to the trigger event be used to undermine our national security;
  - the **trigger event risk** – does the trigger event give someone the means to use the entity or asset in this manner;
  - the **acquirer risk** – might the person acquiring control over the target use this to undermine national security.
- the **statement does not limit the Government's powers** but only sets out where they are most likely to be exercised.
- the statement will also give **guidance about the meaning of significant influence and control**.
- the statement will be subject to **Parliamentary approval**.
- a **draft statement is published alongside this document**. The Government welcomes feedback about it.

## Introduction

- 4.01 In line with its principle of providing **certainty** and **transparency** wherever possible, the Government wishes to provide businesses and investors with as much clarity as possible about where and how national security risks can arise from the acquisition of control over entities or assets. This will be useful to help parties decide whether to submit a notification to the Government and/or to approach the Government for informal discussions about a trigger event.
- 4.02 The Government's initial analysis indicates, given the information provided in the statement of policy intent about the trigger events more likely to raise national security concerns, around 200 notifications will be made each year.

## The role of the statement of policy intent

- 4.03 The Government will publish a statement of policy intent setting out the areas of the economy in which it expects national security risks are more likely to occur and setting out the circumstances in which it expects national security risks to arise in relation to trigger events and where, therefore, it encourages parties to notify trigger events for screening.
- 4.04 A draft of the statement of policy intent is published alongside this White Paper. [The Government welcomes respondents' views about the statement's proposed role, as well as its draft contents.](#) The rest of this chapter only summarises its detailed content and sets out how the document will be subject to Parliamentary oversight and approval.

## The three risk factors

- 4.05 When making their national security assessment, in the context of exercising the power, the Senior Minister will have regard to the statement of policy intent which sets out the three risk factors that are relevant to that assessment. The three risk factors are:
- [the target risk](#) – the risk assessment as to whether the entity or asset that is being acquired (or over which significant influence or control is being gained) may pose a risk to the UK's national security. The statement would also provide details of the areas and sectors of the economy where the Government expects these risks are more likely to arise;
  - [the trigger event risk](#) – the risk assessment about whether the trigger event may give the acquirer the means or ability to undermine the UK's national security through disruption, espionage, inappropriate leverage or some other means;
  - [the acquirer risk](#) – the risk assessment as to whether the acquirer may seek to use their acquisition of control over the entity or asset to undermine the UK's national security.
- 4.06 [A reasonable suspicion that a trigger event may pose a risk to national security is necessary](#) in order for the Senior Minister to call in a trigger event for further scrutiny. The Senior Minister is expected to have regard to the statement, which sets out the three risk factors above in order to determine whether there is a reasonable suspicion.

### The target risk

- 4.07 The first risk factor is whether the entity or asset could be used to undermine the UK's national security. The Government considers that only certain

entities and assets have the potential to be used in this way and that these are more likely to be within the following parts of the economy which the Government terms 'core areas':

- certain parts of the national infrastructure sectors;
- certain advanced technologies;
- critical direct suppliers to the Government and the emergency service sector; and
- dual-use technologies.

4.08 The draft statement of policy intent provides detail about each of these. The Government welcomes respondents' views about whether the draft statement is helpful in indicating the areas of the economy where the Government considers trigger events are most likely to pose a national security risk.

4.09 In addition, the Government considers that there are [other key parts of the economy](#) where national security risks are more likely to arise compared to the [wider economy as a whole](#). These are:

- [critical suppliers who directly and indirectly supply the core areas](#);
- [those parts of the national infrastructure sectors not in the core areas](#);
- and
- [those advanced technologies not in the core areas](#).

4.10 The Government welcomes respondents' views about whether the draft statement is helpful in clarifying those areas of the economy, including critical suppliers, where it expects the call-in power will be more likely used.

4.11 However, given the often-changing nature of national security risks, these may arise outside those cited in the statement, that is, in the [wider economy as a whole](#). The Government may intervene in these areas, as elsewhere, where necessary and proportionate to protect national security.

4.12 In order to provide guidance to businesses as to when the Senior Minister might be most likely to intervene, the statement of policy intent provides [illustrative examples of the types of entities and assets](#) that the Government expects are more likely to raise national security concerns. For example, entities whose manufacturing technology capability could be used for defence purposes are more likely to give rise to national security concerns. This is also the case for assets which can be manipulated remotely or used to extract sensitive information from businesses.

4.13 Defence contractors are amongst the 'core areas' described above as where the Government considers it is most likely that it will call in trigger events to scrutinise any national security implications. In addition to the introduction of

the regime described in this White Paper, the Ministry of Defence will implement changes to its contractual arrangements in order to ensure that all defence contractors (and sub-contractors) are required to notify it of any plans to sell the business or particular assets. Further details will be set out in due course. These required notifications will then be assessed to establish whether the circumstances met the trigger event test and, in the event that the Government had national security concerns about such a trigger event, it could consider calling it in under the regime if the relevant legal test is met.

### **The trigger event risk**

- 4.14 The second risk factor is the trigger event risk (the acquisition) itself and whether it has the means or ability to undermine the UK's national security.
- 4.15 The draft statement sets out the key means by which acquisitions of entities or assets can give rise to national security risks, namely:
- a greater opportunity to undertake **disruptive or destructive actions** or to worsen the impact of such action;
  - an increased ability and opportunity to undertake **espionage** activities; and/or
  - the ability to exploit this acquisition to dictate or alter services or investment decisions or utilise ownership or control as **inappropriate leverage** in other negotiations.
- 4.16 In addition, the draft statement sets out that in determining whether to call in a trigger event for scrutiny, the Senior Minister will consider the entities or assets already owned by the would-be acquirer (so-called '**cumulative ownership**'). For example, the risk posed by a hostile actor's acquisition of an entity would be increased if they already had significant holdings within that sector. This could mean they may have inappropriate leverage over the Government which they could use to threaten essential services.

### **The acquirer risk**

- 4.17 The third risk factor is whether the acquirer may pose a risk to national security.
- 4.18 The draft statement sets out some indications as to the types of acquirer that may be more likely than others to pose a risk to national security. The Government considers that hostile states and other hostile parties are those most likely to pose a risk to national security, while foreign states and foreign nationals are comparatively more likely to pose a risk than UK-based or British acquirers. This is a non-exhaustive list and the case-by-case assessment in relation to a trigger event will take account of the sometimes fast-moving changes to the national security landscape.

- 4.19 The Senior Minister would make an assessment on the acquirer risk on a case-by-case basis taking into account all available information. In the case of an entity acquiring control, for example, this may involve its indirect control, other holdings, and its track record in relation to other acquisitions or holdings. In the case of an individual or individuals acquiring control, this information may include any criminal record, as well as information related to their affiliations.
- 4.20 The fact that the Senior Minister has exercised their call-in powers in relation to a certain acquirer should not be taken as a judgement that the acquirer is hostile. The Senior Minister, in reaching a decision on whether he has a reasonable suspicion that a trigger event may pose a risk to national security, would likely have had regard to a combination of all three risk factors.

## The statement does not limit the Government's powers

- 4.21 Notwithstanding the provision of additional detail and clarity as to how the power is expected to be used by the Senior Minister within the statement, it would not limit the Senior Minister's ability to call in any trigger event that met the statutory test where it is necessary and proportionate to do so. This is key given the often-changing nature of the national security landscape and the speed by which this can occur.

## Parliamentary approval

- 4.22 While the statement is not intended to limit the Government's powers to act to protect national security, the Government wishes to ensure that the document provides as much certainty and clarity about the Government's intent and its expectations as to where and how the Senior Minister might exercise the call-in power granted by the proposed legislation.
- 4.23 Given the role of the statement, the Government proposes that it should be subject to [Parliamentary approval](#). The Government proposes that this is done by way of the affirmative procedure whereby both Houses must debate and positively vote for the draft in order that it gains their consent.

## Reviewing the statement

- 4.24 To ensure the statement keeps up to date with developments in the national security landscape (for example technological advances), the Government would keep the statement under review.
- 4.25 To formalise this further, the Government proposes that the Senior Minister would be under a [statutory duty to review the statement at least once every](#)

five years. However, the Senior Minister may (of course) choose to more frequently review and update this statement. Any revised statement would be subject to the same form of Parliamentary scrutiny as described above.

## Consultation Questions

- |    |  |
|----|--|
| 2. | What are your views about the proposed role of a statement of policy intent?                                     |
| 3. | What are your views about the content of the draft statement of policy intent published alongside this document? |

# Chapter 5 – How the Government will screen notifications

## Summary

- the Government encourages notification in respect of those trigger events that might be expected to give rise to national security concerns. The [statement of policy intent](#) should provide details about where and how these are likely to arise.
- [informal discussions with the Government](#) may help to clarify when a specific trigger event may be of national security interest should parties have any doubts.
- for those trigger events notified to the Government, these will be screened in a [transparent and prescribed manner](#).
- upon receipt of a valid notification, the Government will have a [prescribed period in which to act](#) by confirming whether it will call in the trigger event or not. The Government proposes 15 working days for this period, with the possibility to extend for an additional 15 working days.
- to be valid, the [notification must include certain information that will be set out in guidance](#). It [must also be submitted by parties involved in the trigger event \(or their advisers\)](#).
- there will be [no fee](#) levied for screening notifications, nor for trigger events called in by the Government.

## Introduction

- 5.01 The Government encourages notification of those trigger events that might be expected to give rise to national security concerns. The statement of policy intent, described in Chapter 4, provides the detail and clarity about the Government's expectations as to where and how these risks are most likely to occur. Parties may also choose to engage the Government through informal discussions to establish whether the Government has these concerns in relation to a specific trigger event. The Government would welcome this form of informal discussion.
- 5.02 The Government's initial analysis indicates, given the information provided in the statement of policy intent about the trigger events more likely to raise national security concerns, around 200 notifications will be made each year.

- 5.03 The Government wishes to ensure that there is a clear and transparent process for parties to voluntarily notify those trigger events. Parties will recognise, however, that there must be a degree of flexibility afforded to the Government in regard to the timescales that it uses to scrutinise national security implications.
- 5.04 The proposals in this chapter seek to strike the right balance. The timescales proposed in the chapter are indicative for the purposes of the consultation. The Government will keep these (and other proposed prescribed time periods) under review based, in part, on the responses to this consultation – including respondents’ views about the number of trigger events that would be notified.

## Certainty and clarity in relation to notifications

- 5.05 Where parties are progressing, contemplating or have recently completed a trigger event that they consider may be of interest from a national security perspective, they are encouraged to submit a formal notification to the Government.
- 5.06 If parties wish to receive advice about whether it would be appropriate to submit a notification in respect of a specific trigger event, the Government is happy to engage with them and to provide **informal advice** (although this would not serve as a substitute for submitting a formal notification and receiving clearance under the regime).
- 5.07 Submitting a formal notification may allow parties to ensure that the national security screening process (described in Chapter 7) fits with their commercial timetable, for example.
- 5.08 In line with its principle of providing certainty and transparency wherever possible, the Government proposes to legislate for a transparent and formal process for the notification of trigger events, including a requirement that the Government responds to all notifications within a fixed period. This ensures a level playing field for all parties, and will also allow parties to plan their notifications effectively. The timescales set out in this chapter will be kept under review.

## What is needed in order to make a notification

- 5.09 Any **notification will require specific information** to be provided in writing so as to constitute a ‘valid’ notification. This should avoid limited Government resources being spent scrutinising incomplete notifications and having to request information from parties.

- 5.10 The Government will therefore publish guidance about what information will need to be provided in order to constitute a valid notification, and a template form for its submission. The intention is that online submission will be possible.
- 5.11 This is likely to include, but may not be limited to, the following categories of information:
- [factual information about the relevant trigger event](#) – for example, the entity or asset in question, and what form of control is being acquired;
  - [information about the proposed acquirer](#) – for example, the business name, the country in which it is incorporated, headquartered and has its principal of place of business, and the members of its Board;
  - [information about the purpose of the trigger event](#) – for example, what role does the acquirer expect to play in the running of the entity;
  - (for information involving multiple investors) [information about the relationship between them](#) – for example, the precise structure that a joint venture vehicle will take, and the votes afforded to each party;
  - information about the [proposed acquirer's existing holdings](#) (to the extent that it has any) – for example, what investments do they have in other UK businesses; and
  - [the expected date of the trigger event](#).
- 5.12 The Government welcomes respondents' views about these areas of information, and the costs and time involved in collating this for submission. The Government wishes to strike the right balance between minimising any burden on businesses whilst ensuring it has all the relevant information it requires to make an assessment as to whether a trigger event may give rise to a national security concern.
- 5.13 Notification of a trigger event will not be considered to be an admission by parties that they pose a risk to national security.
- 5.14 Information submitted to the Government under the new regime would be handled securely – clear information gateways would determine the other departments and agencies with whom it could be shared.

## Who can submit a valid notification

- 5.15 Given the Government will be under a duty to respond to all notifications within a fixed period, [only certain parties will be able to make a notification](#). This will ensure that only those persons who hold all of the information that is required to constitute a valid notification are able to do so. This also avoids limited resources being spent screening, for example, trigger events that are not actually occurring.

- 5.16 The parties who can voluntarily notify a trigger event are any of:
- the person acquiring the interest or otherwise activating the trigger event;
  - the seller of that interest;
  - the entity that is the subject of the trigger event; or
  - any professional adviser acting on behalf of any of the above.

5.17 The Government expects that parties will normally submit joint notifications.

## The Government's response to a notification

- 5.18 Once the Government has received a 'valid' notification (that is, one made by a relevant party and with all the necessary information), it will be under a duty to confirm receipt as soon as reasonably practicable.
- 5.19 The Government will then have a fixed period (starting on the working day after the valid notification is received) to undertake a preliminary review and inform the parties if it will be calling in the trigger event.
- 5.20 The Government proposes that the period for this preliminary review and related processes (such as gathering additional information) would be **15 working days**. It will keep this period under review, which may increase or decrease in the final proposals depending, in part, on responses to the consultation, including in relation to the likely volume of trigger events that will be notified to the Government.
- 5.21 The Government expects that, for many trigger events, this period will be sufficient to confirm that it does not need to be called in. However, there are likely to be some trigger events involving more complex considerations. As such, the proposed legislation would allow the Government to extend this period for an additional 15 working days. This would only be possible if the Government required further time to fully consider specific potential risks that it considered the trigger event may pose to national security. Given that the alternative to being able to extend this period may involve the Government publicly calling in the trigger event (if it reasonably suspected that it may raise a risk to national security) for a full assessment period of up to 30 working days, the Government considers this a more proportionate approach but invites respondents' views.
- 5.22 By the end of the prescribed period, the Government must take a decision as to whether or not to call in the trigger event, with reference to the legal test described in the following chapter. This decision will be communicated in writing to the person acquiring the interest or control and (if different) those

who submitted the notification. The Senior Minister would also have the discretion to serve notice of its decision on the seller of an interest and/or the entity that is the subject of the trigger event.

- 5.23 **A decision to call in a trigger event would be made public.** The Government considers that publishing at the point that a trigger event has been called in provides maximum transparency (a key theme of responses to the 2017 Green Paper). There may be alternatives to reduce the possible impact that this publication may have on affected businesses' interests. Chapter 7 provides further detail on this. The Government welcomes respondents' views on the timing of publication.
- 5.24 If the Government decides not to call in a notified trigger event, then the trigger event is cleared and may proceed without further scrutiny. This would be communicated in writing at this stage in the same manner and to the same persons referred to in paragraph 5.21 above but would not be made public.
- 5.25 The Government will not charge a fee for notifications, nor in relation to trigger events not notified but nonetheless called in for scrutiny.

### Consultation Question

4. Does the proposed notification process provide sufficient predictability and transparency? If not, what changes to the proposed regime would deliver this?
-

# Chapter 6 – The call-in power

## Summary

- the proposed legislation would establish a **clear test** that must be met for the Government to call in a trigger event for a national security assessment.
- the Senior Minister must have **reasonable grounds for suspecting that it is or may be the case that a trigger event has taken place or is in progress or contemplation.**
- the Senior Minister must have a **reasonable suspicion that the trigger event may give rise to a risk to national security** due to the nature of the activities of the entity or the nature of the asset (or the location of the asset if land or buildings) over which control is being acquired.
- any intervention must be both **necessary and proportionate** – this will include an assessment that no other, less intrusive, measure is available.
- when exercising the power, the Senior Minister must have regard to the **statement of policy intent, approved by Parliament**, which sets out how the power is expected to be used.
- in the event the Senior Minister intervenes after a trigger event has taken place, they must do so **as soon as reasonably practicable after becoming aware and (in any event) within a prescribed period.** The Government suggests this period could be up to six months.
- the trigger event must also relate to an entity or asset either in the UK or with a **clear, prescribed nexus** to it.

## Introduction

6.01 The proposed legislation would relate only to protecting national security. The Senior Minister must therefore be afforded sufficient flexibility to act where it is necessary and proportionate in the interests of national security. However, the Government will ensure that the proposed legislation establishes a clear and circumscribed test that must be met in order for the Senior Minister to intervene by calling in a trigger event for scrutiny.

6.02 This chapter describes the components (or 'limbs') that will make up this test.

## Structure of the call-in test

- 6.03 The Government proposes that this test should be made up of two separate conditions – each of which would need to be met in order that the Senior Minister could intervene:
- they must have reasonable grounds for suspecting that it is or may be the case that a [trigger event has taken place or is in progress or contemplation](#); and
  - they must have a reasonable suspicion that, due to the nature of the activities of the entity involved in the trigger event or the nature of the asset involved in the trigger event (or its location in the case of land), the trigger event may [give rise to a risk to national security](#).
- 6.04 In exercising this power, the Senior Minister would only act where it is [necessary and proportionate](#) to do so.
- 6.05 In addition, the proposed legislation would specify that when intervening, the Senior Minister must also:
- [have regard to a statement of policy intent](#) approved by Parliament which sets out how the call-in power is expected to be used;
  - (in the case of calling in a trigger event that has already taken place) [act as soon as reasonably practicable after becoming aware of it](#) and (in any event) within a prescribed period after the trigger event occurred; and
  - [meet the nexus test](#) established by the proposed legislation.
- 6.06 The rest of this chapter provides further detail on each of these tests.

## The Senior Minister

- 6.07 One Cabinet-level minister would be the key decision-maker for all decisions under the new regime.
- 6.08 While normally, legislation refers only to the Secretary of State, the Government proposes using “the Senior Minister” in any legislation, which would be defined as covering Secretaries of State, the Chancellor and the Prime Minister (neither of whom are Secretaries of State). The Civil Contingencies Act takes a similar approach.
- 6.09 The rest of this White Paper uses ‘the Senior Minister’ to refer to the decision-maker throughout.

## Limb 1 – reasonable suspicion that it is or may be the case that the trigger event has taken place or will do so

- 6.10 As described in Chapter 3, the proposed legislation would set out the legal tests for each of the trigger events. Some will be objective and incontrovertible matters of fact – the acquisition of shares, for example. Others may include some degree of judgement – the acquisition of significant influence or control over an entity, for example, where a statutory statement of policy will provide clear guidance.
- 6.11 In order for the Senior Minister to intervene, they must have [reasonable grounds for suspecting that it is or may be the case that a trigger event has actually taken place or is taking place](#). If this part of the call-in decision was challenged (in the manner described in Chapter 10), the Senior Minister would need to demonstrate that they had reasonable grounds for suspecting that the facts and circumstances constituted a trigger event as set out in the proposed legislation. A ‘reasonable grounds for suspecting’ test is also used in section 42(1)(a) of the Enterprise Act 2002 in relation to the Secretary of State’s powers to intervene in relevant merger situations on specified public interest grounds.
- 6.12 The proposed legislation would also ensure that, as in the case of the Secretary of State intervening in relevant merger situations on public interest grounds, the Senior Minister can intervene when the trigger event is [in progress or in contemplation](#). Given that national security risks may be realised very quickly after a trigger event has taken place (for example, intellectual property may be acquired immediately after completion of a transaction), it is vital that the Senior Minister can intervene in advance where they consider this necessary in order to protect national security.
- 6.13 [The CMA’s guidance on jurisdiction and procedure](#) sets out that the CMA will generally consider that arrangements are in progress or in contemplation “when a public announcement has been made by the parties concerned”. In the case of a public bid, this will generally mean announcement of a possible offer or of a firm intention to make an offer.
- 6.14 In cases other than public bids, this would likely mean the broad commercial terms have been agreed between the parties (for example, “heads of terms have been agreed”), or an exclusivity agreement has been made.
- 6.15 The Government considers that ‘in progress or in contemplation’ also reflects its interpretation of the point at which it would seek, where possible, to intervene in trigger events in order to protect against the realisation of national security risks. This will not be possible in relation to all trigger events – for

example, involuntary acquisitions of the sort described in Chapter 3 would not be contemplated by the acquirer.

- 6.16 In the case of share acquisitions in private companies, the Government expects to intervene where there is evidence that commercial terms have been agreed between the parties (for example, heads of terms have been agreed) or an exclusivity agreement has been made. For other trigger events, the Senior Minister would expect only to intervene when the parties to a trigger event were similarly sufficiently serious and committed in their intent, such as having instructed lawyers in relation to the trigger event or drafting and/or negotiating legal documentation relating to the trigger event.

## Limb 2 – the trigger event may give rise to a national security risk

- 6.17 The proposed legislation would ensure that the Senior Minister can only intervene in a trigger event when they have a reasonable suspicion that it may give rise to a risk to national security. This would only occur when the entity or asset over which control or influence is being gained has [the capability to undermine our national security](#) in the wrong hands.
- 6.18 In the case of entities, it is the nature of their activities (that is, the type of goods they produce or the services they offer) that the Senior Minister must have considered.
- 6.19 In the case of assets, the Senior Minister must be satisfied that their nature (such as their ability to cause a national-scale emergency) is such that they might pose a risk to national security. Separately, in the case of land, if the nature of the land does not pose any risk, the Senior Minister must be satisfied that its location is such that it might pose a risk to national security – for example, because of its close proximity to another site in which the Government has a national security interest – if acquired by a hostile party.
- 6.20 As described in Chapter 4, a statement of policy intent will be published describing, amongst other matters, how the Senior Minister expects to exercise the call-in power. It also covers the three risk assessments they would likely seek to make to determine whether they had a reasonable suspicion that the trigger event may give rise to a risk to national security. A draft of this statement is published alongside this White Paper. The Government invites comments about its contents.

## Acting only where necessary and proportionate

- 6.21 When exercising the call-in power under the proposed legislation, the Government would seek only to act when **necessary and proportionate**.
- 6.22 A key factor in determining whether to exercise the call-in power in a particular set of circumstances would be what other powers or levers the Senior Minister has available to them. The Senior Minister would need to be satisfied that their aim of protecting national security could not be achieved by other, less intrusive measures.
- 6.23 It may be, for example, that sector-specific regulations may permit the Senior Minister to take steps to ensure a trigger event could not impact national security without the need to call it in. Amending physical security measures, for example, may be sufficient in some circumstances. Alternatively, using the export controls regime may be the most suitable mitigation of national security risks related to an asset sale.

## The requirement to have regard to the statement of policy intent

- 6.24 When considering exercising the call-in power, the Senior Minister would also be required, by law, to have regard to the statement of policy intent discussed in Chapter 4.
- 6.25 While this would not limit their actions to the circumstances described by the statement (for example, the areas of the economy described as ‘core areas’), it will clearly demonstrate those areas where the Government expects these risks to arise.

## When intervening after a trigger event has taken place, the requirement to act as soon as reasonably practicable and (in any event) within a prescribed period of the trigger event taking place

- 6.26 The Government would, wherever possible and practicable, seek to act before a trigger event completes or otherwise takes legal effect. This would ensure that it could prevent or mitigate national security risks at the earliest point. The Government also anticipates that this will be in the interests of parties to a trigger event who would wish to know and take account of any potential intervention. For example, in the case of a merger, parties may wish to have certainty before databases are combined or employees’ terms are changed. It is for this reason that the Government encourages parties to notify trigger events that they think may raise national security concerns.

- 6.27 There may, however, be instances where the Government only becomes aware of a trigger event that raises national security concerns after it has taken place or has completed. In these circumstances, it is important and right that the Senior Minister is still able to exercise the call-in power to assess whether it poses any national security risks. Respondents to the 2017 Green Paper agreed with this principle.
- 6.28 The Government proposes that it can only call in a trigger event within a prescribed period of time after it has taken place, excepting the scenario covered in paragraph 6.35 below. The Government recognises that it is important that the prescribed period is not unnecessarily lengthy in order to reduce uncertainty for parties to a trigger event, while also needing sufficient flexibility to act to protect national security – particularly in relation to any parties deliberately trying to avoid Government scrutiny.
- 6.29 In the Green Paper, the Government sought views on whether three months was an appropriate period for such intervention. This is, in effect, the approximate period of time during which the Secretary of State can act in relation to a relevant merger situation on public interest grounds.<sup>14</sup>
- 6.30 A clear and detailed statement of policy intent will provide clarity to businesses about those trigger events in which the Government has national security interests and encourages notification for screening. As such, the Government considers it is likely to be notified in advance of the vast majority of relevant trigger events. However, the Government considers that there is a case for examining the merits of a longer period for calling in trigger events that have already occurred as this may be required to provide the Senior Minister with sufficient flexibility to call in those trigger events that have not been notified – especially those which the Government could not reasonably expect to know about in advance. This may be particularly important where there is limited information about such a trigger event in the public domain.
- 6.31 Further, the Government notes that similar regimes in other countries have significantly longer periods or have no such fixed period at all. The mandatory notification regime in Germany, for example, permits retrospective intervention for up to five years. The mandatory and voluntary regimes in Australia and the

---

<sup>14</sup> Under the Enterprise Act 2002, the merger must have occurred no more than four months before a reference is made to Phase 2 of the CMA's investigation. In practice, the Secretary of State would need to intervene within the four-month window but in time to allow a "Phase 1" public intervention process to complete. This would mean intervening around 60 to 80 days after a relevant merger situation takes place, to allow time for the CMA to prepare its report and for the Secretary of State to consider any undertakings offered and consult on them, although this could be expedited where necessary.

United States respectively apply no time limit for retrospective action to impose remedies or to unwind a transaction to protect national security.

- 6.32 The Government suggests that up to **six months** may be an appropriate window on the basis that it encourages parties to voluntarily notify trigger events of interest. This, it assesses, may strike the right balance between certainty for parties and a reasonable for window to provide Government with greater flexibility and means to protect national security. The Government invites respondents' views about this and the Government's position on acting retrospectively more generally.
- 6.33 Chapter 8 discusses the remedies that might be imposed in the event that the national security assessment concludes that a trigger event gives rise to a risk to national security.
- 6.34 **If following the end of this fixed period, the Government had not called in the trigger event for scrutiny, it will no longer be able to do so.** However (as described in Chapter 3), the Senior Minister will be able to call in further acquisitions of control relating to the same entity in the event that the Minister concludes that the further acquisition gives rise to a risk to national security.
- 6.35 The Government proposes to introduce legislation such that the prescribed period would not apply where false information has been provided in a notification or in response to an information request, and where that information would have made a difference to the call-in decision. Should the Government establish that this had been the case, it would be able to call in the trigger event to assess it in light of the now accurate information if, at that point, it reasonably suspected that the trigger event may raise a risk to national security.

## The trigger event's nexus to the UK

- 6.36 The proposed legislation's call-in test would also establish a clear '**nexus test**' that must be met in order that a trigger event can be called in for scrutiny in relation to potential national security implications.
- 6.37 The proposed legislation, and the powers granted to the Senior Minister by it, would be focused on protecting the UK's national security. It is UK-based entities' activities and assets that are, therefore, considerably more likely to be those with which the Government has a national security concern.
- 6.38 However, trigger events that take place outside our geographic borders may still threaten the UK's national security. This is particularly the case given the complex corporate structures that can exist. For example, a business in one

country acquiring a business in another may have national security consequences for the UK if the latter provides services to the UK upon which the country fundamentally relies.

6.39 This is also the case in relation to assets. For example, the supply of energy to the UK is provided, in part, by assets (such as deep-sea cables) located outside its geographical borders. Intellectual property may also arise outside the UK and yet be key to the provision of critical functions to the UK.

6.40 The Government considers it important, therefore, that its powers to call in a trigger event should seek to extend beyond the UK in those cases where the trigger event is connected to the UK. The proposed legislation would accordingly specify that there will be a pool of overseas entities and assets that fall within scope of the regime, namely:

- entities that are incorporated or otherwise established outside of the UK;
- assets that are either situated outside the UK; or
- (for example, in the case of intellectual property) rights that are governed by foreign law.

6.41 However, in order to call in a trigger event involving one of these entities or assets, the Senior Minister must be satisfied of the following:

- in respect of an entity that is incorporated or otherwise established under the law of a country or territory outside of the UK, **the entity must carry on activities in the UK or supply goods or services to persons in the UK;** or
- in respect of an asset that is situated outside of the UK or a right arising under, or governed by the law of, a country or territory outside of the UK, **the asset must be used in connection with activities taking place in the UK or the supply of goods or services to persons in the UK.**

## Consultation Question

5. What are your views about the proposed legal test for the exercise of the call-in power? Does it provide sufficient clarity about how it would operate?
-

# Chapter 7 – Calling in a trigger event and the subsequent assessment process

## Summary

- the Government will ‘call in’ those trigger events that raise national security concerns. It expects, for most cases, this to follow its initial screening of a notification.
- however, it reserves the right to call in trigger events not notified to the Government if they nevertheless meet the statutory test.
- the Government may request or require information in order to inform its decision as to whether to call in a trigger event.
- once it has been called in, parties must not complete the trigger event until approval has been granted but can still take preliminary or preparatory steps.
- in specific circumstances, the Government may impose specific interim restrictions on parties’ sharing of information or provision of access.
- the Government will have 30 working days to make its assessment of the national security risks. It will be able to extend this for a further 45 working days where a national security risk has been identified but the case requires more detailed scrutiny to ascertain the extent of that risk and/or the appropriate remedies. The Government will keep this period under review and it may increase or decrease in the final proposals. In exceptional circumstances, the parties can agree with the Government to further extend this timeframe.
- the Government will have powers to gather information from any party to help inform its assessment.
- the Government will publish certain details of the assessment process to ensure as much transparency as possible.
- there will be no fee levied in relation to trigger events called in by the Government.

## Introduction

7.01 This chapter sets out the process by which the Government will call in trigger events and undertake the subsequent national security assessment. The Government will use this process to determine whether to approve, approve with conditions, or (as a last resort) block or unwind the trigger event. The

type of remedy, and the legal test for their imposition, is considered in the following chapter.

- 7.02 In order to determine whether to call in a trigger event and to inform its assessment, the Government may need to gather information from parties.
- 7.03 The Government proposes to legislate to establish a clear and time-limited statutory process during which it would undertake this national security assessment.
- 7.04 The statutory process needs to strike a balance between being thorough for the purposes of protecting national security, and efficient so as not to unnecessarily delay or disrupt the trigger event. The process is designed to give certainty to businesses and investors about both the information they are required to provide in order for the Government to make its assessment, and the timeframe within which they can expect a decision. Respondents to the consultation were clear that the Government must provide sufficient clarity on these aspects to minimise costs to businesses. The Government will ensure that the reforms operate in as open and transparent a manner as is compatible with national security.
- 7.05 The Government has developed the timescales in this chapter, in part, by considering other countries' similar regimes. It considers that the proposals are reasonable but invites respondents' views, including specific evidence for alternative timescales. Respondents will be conscious about the Government's responsibility to taxpayers in ensuring that its resources are best focused and utilised. The Government will not levy fees in relation to trigger events to minimise the impact on businesses.
- 7.06 The Government's initial analysis indicates that it would "call in" around half of the 200 notifications it expects to receive each year.

## Gathering information to determine whether to call in a trigger event

- 7.07 As above, the Government encourages parties to submit notifications about those trigger events that they consider may raise national security concerns. However, it reserves the right to call in a trigger event irrespective of whether notification was made. To inform its decision as to whether to call in a trigger event, it may require information from parties.
- 7.08 The Government expects, in the first instance, to use [informal information requests](#) of persons close to the potential trigger event in order to find out more about the particular circumstances, whether a trigger event is occurring

(or has occurred) and whether it needs to be called in to be investigated more fully.

- 7.09 In the event that an informal request is not appropriate or has not provided the information required, the proposed legislation would permit the Senior Minister to exercise **formal information-gathering powers** to obtain sufficient information to determine whether to exercise the call-in power. Information could only be gathered, under this power, in order to inform the Senior Minister's decision as to whether to call in a trigger event. Those persons who receive a formal information-gathering notice would be obliged to provide the relevant information; the breach of which would lead to a civil sanction as described in Chapter 9.
- 7.10 In order to exercise the power, the Senior Minister would first need to have reasonable grounds for suspecting that it is, or may be the case, that a trigger event has taken place within a prescribed period (Chapter 6 suggests this could be up to six months) or is currently in progress or contemplation. They must also have reasonable grounds for suspecting that they require relevant parties to provide the relevant information for the purposes of informing their decision as to whether to exercise the call-in power.
- 7.11 The exercise of this information-gathering power would not be made public by the Government, although it would be open to other parties to do so. The Government would also not be under an obligation to confirm any intention as to whether to call in a trigger event having received the information.
- 7.12 Given the alternative (that is, the absence of this power) is that the Government may not be able to obtain sufficient information to meet the legal test to call in a trigger event, the Government considers that this formal information-gathering power is a proportionate and important component of the regime.
- 7.13 Knowingly providing false information, destroying information or preventing others from providing information requested under this power would attract criminal or, as an alternative, civil sanctions as described in Chapter 9. As described in the previous chapter, if the Government established that false information had been provided, it would then be able to call in the trigger event (or call it in again) to assess it in light of the now accurate information if, at that point, it reasonably suspected that the trigger event may raise a risk to national security.
- 7.14 In order to ensure it becomes aware of trigger events (or potential trigger events) that may raise national security concerns, the Government will increase its resources dedicated to 'market monitoring' and invest in the tools

and systems necessary. This additional resource will also ensure that parties, if unsure about the Government's national security interest, can engage informally with officials at an early stage in their proposed trigger event. This may enable them to understand the Government's likely interests and the likelihood of the trigger event being called in, in the event that the trigger event proceeds (although this would not serve as a substitute for submitting a formal notification and receiving clearance under the regime).

## Serving a call-in notice

- 7.15 The assessment process will begin when the Government calls in a trigger event by serving a **call-in notice**. This may follow the Government's screening of a valid notification as described in the previous chapter. However, there would be no requirement to exercise the information-gathering power before calling in a trigger event if the call-in legal test is met without the exercise of information-gathering power.
- 7.16 When serving the call-in notice, the Government may also require parties to provide information it considers necessary to inform its assessment of the national security risks. In cases where the trigger event has been notified to the Government or, in cases where the Government has used the pre-call-in information-gathering powers, it may ask for less or no information at this stage.
- 7.17 The call-in notice must be served on the person acquiring the interest or activating the trigger event. A call-in notice may also be served on the seller of the interest and/or the entity that is the subject of the trigger event. A call-in notice will include the following information:
- the name of the party on whom it is served;
  - the names of all the other parties on whom the notice is served;
  - the actual or proposed trigger event which the Government is calling in;
  - the effect of the call-in i.e. that the party on whom the call-in notice is served must not complete the trigger event (as described in the next section)
  - any interim restrictions pending the Senior Minister's final decision on the trigger event (as described later in this chapter);
  - any information required from the party in order for the Senior Minister to assess the trigger event and make a decision, and the date by which the recipient is required to provide it (the information-gathering request may be made at this stage or later by means of a separate information-gathering request);
  - the sanctions associated with breaching any of the above (see Chapter 9).

## The effect of a call-in notice being served

- 7.18 After a trigger event has been called in (but before the Government has concluded whether it can be approved), **the trigger event must not complete**. Doing so would be a breach of the call-in notice and would attract a criminal or, as an alternative, civil sanction.
- 7.19 However, the Government does not wish to unnecessarily delay parties and so **the trigger event being called in should not halt or prevent preliminary or preparatory steps being taken towards the trigger event**. For example, parties could continue to discuss contractual or commercial terms.
- 7.20 In the event that the Government is assessing a trigger event that has already taken place, once it has been called in, parties must not take any further measures that increase the acquirer's control, nor take steps that would make it more difficult for the trigger event to be unwound, should the Government reasonably conclude that this is necessary and proportionate for protecting national security and that this is the most suitable way of dealing with the risk.

## Interim restrictions

- 7.21 A trigger event, once called in, cannot complete until the Government has finished its assessment. This should (in most circumstances) be sufficient to prevent any national security risks arising before appropriate conditions can be imposed.
- 7.22 However, there may be circumstances where the Government has reason to believe that national security may be at risk at an earlier stage. This may particularly be the case when, for example, the Government has called in a trigger event that has already taken place.
- 7.23 As such, the proposed legislation would permit the Government to impose **'interim restrictions'**, in addition to the automatic stay on completion, on a trigger event while it is assessing its potential national security implications. This would only occur when a clear legal test was met, namely that the Government had reasonable grounds for suspecting that there will be a risk to national security if interim restrictions are not imposed and considered that the specific interim restrictions were reasonably necessary to protect national security while the Government considers the trigger event. A breach of an interim restriction would attract a criminal or, as an alternative, civil sanction.
- 7.24 The Government proposes that interim restrictions, in addition to the automatic stay on completion, would be limited to two forms:

- a prohibition on the release or sharing of specific **information** or specified categories of information; and/or
- a prohibition on **access** to specified sites by specified individuals or categories of individuals or their representatives.

- 7.25 The Government would be under a duty to revise or remove interim restrictions when no longer required.
- 7.26 Where the parties consider that it is necessary to take steps that are prohibited by an interim restriction in order to progress the trigger event, they may seek approval from the Senior Minister on a case-by case basis.
- 7.27 The following chapter provides more details about how interim restrictions could be amended or revoked. Chapter 10 provides details about how any decision to impose an interim restriction could be challenged by way of judicial review.

## The Government's assessment process, including timescales

- 7.28 The Government will have **up to 30 working days to assess any trigger event** which it has called in. During this period, it will assess whether the trigger event does indeed give rise to a national security risk. In the event that it concludes the trigger event does give rise to a risk, it may also begin considering what mitigations, under this proposed legislation or by other means, may be appropriate to address that risk.
- 7.29 The Government will inform parties about its assessment as soon as reasonably practicable and, in any event, within the 30 working day period. This assessment may be that the trigger event is cleared and can proceed without conditions.
- 7.30 The Government may decide that the scale or complexity of the trigger event are such that it, having determined that there will be a risk to national security, requires additional time in order to further consider the extent of the risk and decide upon appropriate remedies. Therefore, the proposed legislation would permit the Government **an additional 45 working day period** at the end of the initial 30 working day period. Again, the Government will inform parties as soon as reasonably practicable, and in any event before the end of the 30 working day period, about the fact it has identified a national security risk and any decision it makes to extend the assessment period to the total of 75 working days.
- 7.31 There may be rare circumstances where the Government is unable to reach a decision about the mitigations to address the national security risk raised by

the trigger event even within a 75 working day period. In these rare circumstances, the Government may agree an extension, or 'Voluntary Period', with the parties to the call-in notice. This would be done in writing.

## Information-gathering during the assessment process

- 7.32 While assessing a trigger event, the Government may require information or further information to inform its assessment about the national security risks and/or how these could be remedied.
- 7.33 This information may include details about the entity in question, the acquirer's other holdings or their plans for use of the asset. The parties holding this information could, therefore, include the individual acquiring control, any individual selling their interests, the entity in question, or former or other investors.
- 7.34 The specific information required will depend on the case in question, as will the party from whom it is required. The Government does not, therefore, consider it possible for the proposed legislation to limit the scope of the information that can be requested under these powers. Instead, the proposed legislation would permit the Government to seek any information it reasonably considers is relevant from any party it considers necessary whom it believes has the information necessary to inform its assessment.
- 7.35 The Government will request this information by serving an [information notice](#) on the relevant party. This may be at the point of calling in a trigger event or at any point during the assessment process. On each occasion, the notice will specify (with as much detail as possible) the information sought by the Government. The notice will also provide a deadline by which the party must provide the information. The Government will consider this time period on a case-by-case basis, setting a deadline it considers reasonable in the individual circumstances.
- 7.36 The Government considered setting out, in the Act, an overall maximum time period for providing information in order to reassure parties that deals will not be unnecessarily delayed by the Government setting long periods. However, it concluded that there may be instances where complex information was required and so any such period set out in legislation would need to be very long, perhaps three months. Given it expects the majority of information requests to be relatively straightforward and parties will be able to respond quickly, the Government considers it more reasonable and flexible that the proposed legislation does not provide a maximum time period. Each information request will be required to set out the deadline specific to that case, which could be as little as two weeks in straightforward cases. Of

course, parties could supply the information in advance of the deadline. Indeed, the Government considers that it will be in parties' interests to provide accurate information in a timely fashion to enable the Government to complete its assessment quickly. The Government welcomes respondents' view about the merits of there being a prescribed maximum time period for responding to an information request.

- 7.37 Often, the requested information will be critical to the Government's assessment. Therefore, it is not reasonable that the prescribed assessment period continues while the Government awaits information it has requested. As such, the act of requesting information from parties will 'pause the clock' until that information is supplied. In the event that the Senior Minister concluded another party's delay in responding to their information request had reached the point of unfairly harming the acquiring party's interest, they would have the ability to 'un-pause' the clock or to make a decision about the case.
- 7.38 A failure to provide the information requested by the deadline or explain why it cannot be provided, without a reasonable excuse, would attract sanctions – as would knowingly providing false information. These are detailed in Chapter 9.
- 7.39 The Government recognises that information gathered as a result of these information requests may, in many circumstances, be commercially sensitive. The proposed legislation will therefore establish clear information gateways that would limit with whom and how it could be shared. Information that was legally privileged would not, of course, need to be disclosed to the Government.

## Transparency

- 7.40 The Government also recognises the importance of providing as much transparency as possible. This was a key theme in responses to its 2017 Green Paper.
- 7.41 This transparency is particularly critical in relation to what trigger events are called in for scrutiny, and the process for their scrutiny. This is of most interest to the parties concerned, but the Government recognises that there are wider interests in relation to the volume, type and nature of trigger events which it has called in. Transparency will also permit other parties to make submissions to the Government to consider as part of its screening process.
- 7.42 Respondents will appreciate, however, that there are limits as to the extent of transparency possible in relation to a process focused solely on protecting national security.

## **What will be published in relation to a trigger event that has been called in**

- 7.43 Recognising the importance of transparency, the proposed legislation will stipulate that the Government must publish any decision to call in a trigger event.
- 7.44 The Government considers that publishing at the point that a trigger event has been called in provides maximum transparency (a key theme of responses to the 2017 Green Paper). However, the Government wishes to ensure that the regime, and transparency around it, does not harm business interests – for example, disincentivising notification of trigger events which parties do not wish to make public. It re-emphasises that informal discussions with Government officials would be an alternative or first step open to parties who wish to seek advice as to whether the Government has a national security interest in a trigger event. As an alternative to this approach, the proposed legislation could instead specify that the Government publish only when an assessment had concluded and a case had been determined. The Government welcomes respondents' views on the timing of publication.
- 7.45 Once a trigger event has been called in, the Government wishes to be as open as possible about the process of its scrutiny, even if the individual assessments must necessarily be confidential. Therefore, in relation to trigger events that have been called in, the Government will publish:
- the high-level reasons for doing so;
  - (where relevant) the fact that it has imposed, modified or removed interim restrictions, but not the details of these restrictions;
  - the timescales for its assessment process, including any 'pausing' of this because of information requests, and any decision to extend the 30 working day period or agreement to extend the 75 working day period. This will ensure that parties are clear when the assessment starts, is paused and ends.

## **Transparency in relation to trigger events not otherwise in the public domain**

- 7.46 The Government expects that, in most cases, the trigger event will be public knowledge at the point of being called in. However, there may be circumstances where this is not the case, for example deals involving private companies.
- 7.47 In these circumstances, the Government proposes that it would be able to choose not to publish the fact that it has called in a trigger event for up to five working days after the call-in notice has been served. This will give the parties on whom the notice has been served the chance to plan and prepare for the trigger event becoming public knowledge – informing employees or other

stakeholders, for example. As noted above, the Government welcomes respondents' views on the timing of publication.

- 7.48 Any decision not to disclose its calling in of a trigger event immediately would be taken on a case-by-case basis, considering all the relevant information and Government's consideration of third parties whose rights may be affected by its calling in a trigger event. The Government welcomes views about the merits of this five day 'grace period' being provided for in the proposed legislation.

## Engagement with Government during the screening and assessment process

- 7.49 During the statutory assessment period, in so far as is reasonably practicable, the Government wishes to take a flexible approach to sharing its developing thinking with the affected parties. This may speed up deliberation as the parties will be able to feed into Government's thinking about, for example, practicable remedies.
- 7.50 When calling in a trigger event, the call-in notice would provide contact details for affected parties to use if they wished to engage with Government officials. There will, however, be a limit as to the detail of the Government's views about national security that can be shared.
- 7.51 Given the Senior Minister will be acting in a quasi-judicial role, it will be important that they are not involved in the day-to-day discussion about remedies. Instead, officials acting on their behalf will conduct this role in order to inform advice to the Senior Minister who will make the final decision in line with the legal test established by the proposed legislation.
- 7.52 The Government will not charge a fee for notifications, nor for those cases that it calls in for assessment.

### Consultation Question

6. What are your views about the proposed process for how trigger events, once called in, will be assessed?

# Chapter 8 – The remedies available to protect national security

## Summary

- should the assessment process identify a national security risk, it is vital that the Government has a **range of remedies** available to enable the trigger event to complete.
- any such remedy could only be imposed subject to a clear legal test being met, namely a requirement that the specific remedy is **necessary and proportionate**, is the **most suitable way of dealing with the issue**, and follows **consideration of any representations made by affected parties**.
- the proposed legislation would allow the Senior Minister to impose a condition on **any party**.
- conditions can take any form, but the proposed legislation would provide an **indicative list** to provide as much certainty as possible, with more details set out in guidance.
- in the event that the Government concludes that no remedy is able to address or mitigate the risk to national security, it will have the power to **block a deal or unwind it** if it has already taken place (subject to the prescribed period for intervention).
- **remedies will be kept under review** and amended, revoked or added to if necessary and proportionate. Parties will be able to request a review if there has been a material change in circumstances.
- the legislation may provide for a **Government spending power** in the unlikely event that this is necessary in relation to the imposition of remedies.

## Introduction

- 8.01 This chapter sets out the steps that the proposed legislation will permit the Senior Minister to take in the event that a trigger event (which had been called in for scrutiny) raises national security concerns. The proposals have been designed in line with the Government's principle of ensuring that the new powers reflect national security concerns and are necessary and proportionate.
- 8.02 Based on its initial analysis, the Government expects that around half of the approximately 200 trigger events it expects will be notified to it each year will be called in for a full national security assessment.

- 8.03 For a trigger event to have met the statutory test for the Senior Minister calling it in, the Senior Minister must have a reasonable suspicion that the trigger event poses a risk to national security. It may be that, following his/her thorough assessment process and engagement with the parties (as described in the previous chapter), the Senior Minister concludes that no remedies need be imposed, and the Senior Minister will approve the trigger event so that it can proceed. The Government's initial analysis indicates that this is likely to be the case in relation to around half of the trigger events called in for a full national security assessment.
- 8.04 The Senior Minister may grant approval for the trigger event to proceed because:
- the assessment concludes that national security is not, in fact, undermined by the trigger event; or
  - other regulatory or legislative steps can be taken to address any such risks.
- 8.05 Should the Senior Minister conclude that they cannot approve the trigger event as proposed, the proposed legislation will grant them powers to impose remedies as a condition of the approval for the trigger event to proceed.
- 8.06 Following an introduction to the role of remedies and the Government's approach, this chapter details:
- the legal test for the imposition of remedies;
  - the type of condition that might be imposed as part of the approval process to permit the trigger event to complete;
  - the individuals and entities on whom the remedies may be imposed;
  - the approach to public disclosure around conditions;
  - how conditions and interim restrictions may be reviewed or varied;
  - when and how a trigger event may be blocked; and
  - how a trigger event may be unwound

## The role of remedies and the Government's approach

- 8.07 Remedies are designed for the Government to prevent or mitigate risks to national security that may arise from trigger events. Breach of any condition may lead to a criminal or, as an alternative, civil sanction.
- 8.08 The Enterprise Act 2002 grants the Secretary of State broad powers to mitigate or prevent national security concerns arising from relevant merger situations. In shaping these powers, Parliament recognised it is critical for all governments to have sufficient flexibility to protect national security in the most appropriate and tailored fashion – a one-size-fits-all approach would inappropriately tie the Government's hands.

- 8.09 The Government will retain this important flexibility to act in its proposed reforms.
- 8.10 The proposed legislation will permit the Senior Minister to impose **any such remedies as they consider necessary to protect national security**. This will involve a move away from the provision permitted under the Enterprise Act 2002 whereby ministers can accept undertakings made voluntarily at Phase 1 by the concerned parties.
- 8.11 As described later in this chapter, while the Government expects that parties will be involved in its deliberations about potential remedies, it considers it an important provision for a wholly national security-related regime that the Senior Minister makes a deliberate decision as to the necessary remedies on a case-by-case basis. While this may be only a relatively small distinction in practice, the Government considers this an important change in approach.

## The legal test for the imposition of remedies

- 8.12 Recognising the direct impact on parties' rights, any remedy will need to meet a clear legal test. Specifically, the Senior Minister would only be able to impose a condition if:
- they reasonably believe that a national security risk is posed by the trigger event;
  - they reasonably consider that it is necessary to impose a remedy for purposes connected with preventing or mitigating the risks to national security;
  - the remedy is proportionate to the risk identified;
  - the Senior Minister considers that there is no other more adequate and proportionate power available for them to exercise; and
  - they have considered any representations from parties.
- 8.13 Cumulatively, these 'limbs' create a **clear, rational and considerable test** that must be met for the Government to exercise what it accepts is a significant power to impose conditions on a trigger event.
- 8.14 The Government expects that, during the assessment process, its officials will engage with parties, including those on whom any remedy might be imposed. It expects that such discussions will include the potential form and detail of any remedies, and it will generally welcome parties' input as to what remedies are acceptable to them. Parties' expertise may also be useful in ensuring that remedies are practicable.

8.15 However, the final decision about the form, detail and imposition of remedies will be the Senior Minister's alone.

## The individuals and entities on whom conditions may be imposed

8.16 In the majority of cases, it is expected that any conditions would be placed upon the acquirer of that interest and/or the UK entity being acquired. However, like the type of conditions themselves, it is important that the Government is afforded sufficient flexibility to deal with any scenario. Therefore, the proposed legislation will provide that the Senior Minister may impose conditions on *any party*.

### Examples of the individuals on whom conditions may be imposed

Investor A is acquiring Entity B which is a telecommunications provider.

The Senior Minister calls in the trigger event for scrutiny. They conclude that A presents a national security risk and therefore the trigger event would impact the UK's national security if it proceeded as proposed. This is because, if A possessed unconditional and unescorted access to a particular operational site, they could use this to monitor or manipulate these communications and therefore affect the national security of the UK.

The Senior Minister concludes that it is both proportionate and necessary to mitigate the national security risk so that the trigger event can only proceed subject to the condition that A does not access the site in question.

However, they may also conclude that this condition alone is not sufficient – for example, because of the risk that A would not comply with the condition and would obtain access nonetheless.

As a result, the Senior Minister may also require entity B to not permit access to A and/or to alert the Senior Minister should A seek to do so.

## The type of condition permitted by the proposed legislation and envisaged by the Government

8.17 As described above, it is crucial that (in protecting national security) the Government is provided sufficient flexibility in the remedies that can be imposed to deal with the broad and unforeseeable range of circumstances where trigger events may give rise to national security concerns. Remedies would only relate to the national security concerns identified by the

Government's assessment of a trigger event. Remedies could not relate, for example, to wider considerations such as protecting jobs.

- 8.18 The conditions would be used to protect confidential or sensitive information, ensure the maintenance of strategic capability, or otherwise protect national security. Annex B provides further details about the purpose of conditions that could be imposed.
- 8.19 While requiring flexibility, at the same time, the Government wishes to provide as much clarity as to its likely intentions as possible. It is in all parties' interests that parties to a trigger event are aware of the potential form of remedies which the Senior Minister may impose in the event that they consider this necessary and proportionate to prevent or mitigate national security concerns.
- 8.20 One option to provide this certainty would be for the proposed legislation to establish an exhaustive statutory list of conditions from which the Senior Minister could choose on a case-by-case basis. However, such an approach would unacceptably limit the Government's ability to adequately protect national security. Further, any such exhaustive list would have to be so broad and vague as to provide no certainty or clarity to parties.
- 8.21 The lack of flexibility afforded to the Government by an exhaustive list would also apply to parties to a trigger event who may have more practicable suggestions than those permitted in any fixed list.
- 8.22 Therefore, the Government has determined that the proposed legislation will include an **indicative but non-exhaustive list** of the type of conditions available to the Senior Minister.
- 8.23 Annex B includes an indicative list of conditions that the Government envisages being included in an indicative but non-exhaustive list within the proposed legislation. This includes conditions related to the structure of transactions, physical security measures, or the appointment of monitors.
- 8.24 Such a list will not limit the breadth of conditions that might be imposed but will provide parties with a clear indication of the conditions that the Government would expect to impose in most cases. This may help parties determine the structure of deals, for example, by building in the Government's likely concerns at the outset. However, even in the event that a trigger event is structured such as to anticipate its concerns, the Government may still call it in and impose binding conditions. This would mean that relevant criminal or, as an alternative, civil sanctions would be available for non-compliance.

### **The broad forms conditions can take**

- 8.25 In broad terms, the types of conditions described in the indicative list take two forms – behavioural and structural. The former relate to parties doing, or not doing, certain activities to protect national security and the latter relate to the organisational structure of enterprises or the merger.
- 8.26 An example of behavioural conditions in relation to national security could include limiting access to certain physical sites, or access to other tangible or non-tangible assets of the acquired entity to those with appropriate UK security clearances.
- 8.27 Structural conditions could include a requirement that control over a particular division or asset is not part of a wider merger. This might be the case where the acquired entity undertakes a broad range of economic activity in addition to the activity which the Government considers raises national security concerns. A suitable remedy in these circumstances might be to require that that activity is not part of the merger so that control does not change hands.

### **Requiring prior approval for further acquisitions of significant influence or control over an entity**

- 8.28 The Government considers that there may be instances where it is able to approve a trigger event (without or without conditions) but would want to have prior notice ahead of the party acquiring a specific further means of control, in the manner described in Chapter 3.
- 8.29 For example, a party acquiring 30% of shares in a business may not give rise to a risk to national security if such a shareholding only provided economic benefits to the party. However, the assessment process may lead the Senior Minister to reasonably suspect that, on the basis of the available evidence, a specific further acquisition (for example, acquiring more than 50% of total shares) would give rise to a new or further national security risk. If this risk could be materialised quickly, only having the ability to call in this further acquisition may be too late to prevent the harm being realised.
- 8.30 In such a scenario, the Government considers it may be appropriate for the Senior Minister to have the power to, following full assessment of the initial trigger event, place a mandatory requirement on the party to seek the Senior Minister's prior approval for a specific further acquisition relating to the same entity. The Government considers that such a requirement would need to be backed by criminal or, as an alternative, civil sanctions.
- 8.31 The Government considers that it could only be appropriate to require prior approval where the Senior Minister believed it was reasonable and

proportionate. As such, the Government considers that it could only require prior approval for further acquisitions of control where a party was actively acquiring further control, rather than through involuntary acquisitions of control arising as a result of third party actions (for example, the divestment of shares by another shareholder).

- 8.32 The Government welcomes respondents' views on this possible component of the new regime.

## The approach to public disclosure around conditions

- 8.33 As throughout these reforms, the Government wishes to ensure that there is as much transparency as is possible for a wholly national security-focused regime in respect of what conditions it has imposed on a trigger event.

- 8.34 Therefore, as soon as practicable after determining that a trigger event can proceed subject to certain conditions, the Senior Minister would be under a duty to publish the approval notice with high-level details about any conditions attached to that approval. The Government considers that this approach provides sufficient transparency and accountability about individual decisions in such a manner that ensures national security is not undermined by public disclosure of sensitive information that could undermine our national security.

- 8.35 Parties subject to conditions would, of course, receive more detailed information about the conditions.

## Appeal against the imposition of remedies

- 8.36 The Government recognises that imposing a remedy on a trigger event would constitute a significant interference with parties' rights. It would only do so when necessary and proportionate.

- 8.37 In the event that a party considered that any condition imposed upon a trigger event had been imposed in an unfair manner, they would have the right to seek a judicial review of the decision. The means and process for this are described in Chapter 10.

## How and when interim restrictions and conditions may be reviewed or varied

- 8.38 Both interim restrictions and remedies should only be in place as long as is necessary and proportionate to protect national security. The proposed legislation, therefore, will make provision for them to be reviewed, varied or revoked whenever this is no longer the case.

## Interim restrictions

- 8.39 Interim restrictions, by definition and design, are to be focused and short-lived. They would automatically cease to apply at the end of the statutory assessment period when the trigger event has been approved (potentially with conditions which supersede the interim restrictions) or as a last resort blocked.<sup>15</sup>
- 8.40 However, the proposed legislation will permit the Senior Minister to review or revoke interim restrictions in light of a request to vary them. They would be required to act “without undue delay” in considering any request made by a party subject to an interim restriction. The Senior Minister need not await such a request – if at any point they consider that the interim restrictions are no longer required, they would be required to remove or amend them accordingly, informing the relevant parties and publishing that decision.

## Conditions

- 8.41 Conditions will only be imposed following a rigorous assessment by the Senior Minister of a trigger event. *The Senior Minister will keep any and all remedies under regular review. Should they conclude that they are no longer appropriate, the Senior Minister will promptly amend or revoke them.* This may result in further conditions being imposed, including upon new parties, when there has been a breach of conditions or the conditions imposed are insufficient to address the national security risk because of a change in circumstances or additional information coming to light.
- 8.42 While there will be means for parties to request a variation of any condition, this will only be permitted following a *material change in circumstances* as set out in the proposed legislation. This is to ensure that vexatious requests cannot impose an administrative burden on the Government.
- 8.43 Upon receipt of a valid request, the Senior Minister will be required to carry out an assessment as to whether the condition still meets the standard test for their imposition. The fact that the Senior Minister is undertaking such an assessment, and the outcome of it, will be published so as to maintain the same high degree of transparency and accountability provided for by all relevant aspects of the reforms.

---

<sup>15</sup> As described in Chapter 7, this period is 30 days and may be extended by a further 45 working days if the Senior Minister needs more time to ascertain the extent of the national security risk and/or consider appropriate remedies, or for a longer period should the Senior Minister and all parties to the call-in notice agree.

## How and when a trigger event may be blocked

- 8.44 There may be circumstances in which the threat to national security is such that consent to proceed with the trigger event, even with conditions, cannot be given. It is anticipated that these would be very rare circumstances.
- 8.45 The proposed legislation, therefore, will provide that the Senior Minister can declare that the trigger event cannot proceed in its current form and is blocked.
- 8.46 Notwithstanding its expectation that these will be very rare circumstances, the Government recognises that blocking a trigger event from taking place would constitute a significant step. The various limbs included in the remedies test in paragraph 8.12 would require the Senior Minister to meet a number of conditions in order to be satisfied that blocking a trigger event was the appropriate way forward.
- 8.47 Any party who considered that the Senior Minister had acted unlawfully in coming to such a conclusion would be able to challenge this decision through judicial appeal as described in Chapter 10.

## How a trigger event may be unwound

- 8.48 As described in Chapter 6, the Senior Minister may call in and scrutinise a trigger event after it takes place.
- 8.49 The Government would only expect to call in a trigger event retrospectively in the event that it was not notified, or otherwise aware of, a trigger event in advance of it completing or otherwise taking effect. The Government expects this to be a relatively rare occurrence. The proposed legislation will also place a duty on the Senior Minister to call in a trigger event as soon as reasonably possible after they become aware of it. There will also be a maximum period in which such an intervention could take place – Chapter 6 suggests this could be up to six months.
- 8.50 If, following their assessment, the Senior Minister concludes that there is no other means of protecting national security other than unwinding the trigger event, they will be able to require the parties to do so by serving an Unwind Order on them. This would have the effect of requiring the recipients to take all such steps as necessary to undo the trigger event.
- 8.51 The Government has concluded this part of the proposed legislation is necessary following careful consideration, recognising the impact it would have on the parties concerned. However, it has concluded that the risks to

national security that might be realised means this is an important option that must be made available to the Senior Minister.

- 8.52 The Government notes that the Enterprise Act 2002 includes similar powers, within specified time limits, for the Competition and Markets Authority to unwind completed relevant merger situations which it considers give rise to a substantial lessening of competition. The CMA's [guidance](#) cites examples of the types of measures it has imposed to unwind integration, including the removal and replacement of key staff.
- 8.53 The Unwind Order will be made only in so far as the Senior Minister considers this is necessary to be able to address the national security risk. This would essentially be a partial unwind of the trigger event. A partial unwind is required only to the point where the imposition of conditions can sufficiently mitigate the on-going national security risk. This avoids the need for a full unwind order. The Government expects a full unwind order to be necessary only where conditions cannot be designed to adequately address the on-going national security risk. A full unwind would be a measure of last resort as is the case with blocking a trigger event.
- 8.54 As in the case of imposing any kind of remedy, the Senior Minister must have considered representations made to them by affected parties when proposing an Unwind Order or a partial Unwind Order. Again, as with all remedies, interested parties could pursue an appeal of the Senior Minister's decision in the manner described in Chapter 10.

## Following breach of conditions, when a trigger event may be unwound

- 8.55 The Government invites views about how the reforms might ensure that it can protect national security in the event that conditions are found to have been breached.
- 8.56 As described above, the Government will keep conditions under a review and may determine, in light of non-compliance with any conditions, that revised or additional conditions are required to protect national security.
- 8.57 However, if conditions (including revised or additional conditions) have been breached, the Senior Minister might conclude that conditions are unable to protect national security in the case of a particular trigger event.
- 8.58 The Government welcomes respondents' views about the appropriateness of the Senior Minister being granted the power to impose a condition (as part of the approval of the trigger event) allowing them to unwind a trigger event

following a breach of certain specified conditions. There would be no time limit on this. If there was a breach of a condition (where unwind had been specified as the consequence of a breach) years after its imposition and the Senior Minister concluded that unwinding the trigger event was a necessary and proportionate step to protect national security, they could compel this.

- 8.59 This power is entirely separate from the sanctions regime designed to punish non-compliance. It would be focused only on protecting national security. It would require the Senior Minister to have carefully considered the damage that would be caused to national security if the trigger event is not unwound, and that it was necessary and proportionate to unwind it. They would also be required to act promptly, having considered the passage of time between the breach of the specific condition or conditions and the date that it came to their attention. As with all remedies, the action would follow consideration of any representations made by interested parties. Also, as in relation to any decision made under the proposed legislation, any such decision could be challenged by judicial appeal.
- 8.60 The Government does not expect that such a condition would be regularly imposed. However, there may be circumstances where this would be an important provision. It invites respondents' views about this and how any such provision could be best designed.

### Information-gathering powers in relation to remedies

- 8.61 Once the Government has imposed a remedy, it must have the means to monitor compliance with it, or to investigate suspected breaches.
- 8.62 Therefore, the proposed legislation will grant the Government the ability to require information from any person for the purposes of monitoring compliance. In the majority of cases, the Government anticipates that these information-gathering notices will be served on the parties acquiring influence or control through the trigger event, or the entity over which this was being acquired. However, this may not always be the case and Government will be able to require information from any third parties whom it considers may have relevant information.
- 8.63 The information-gathering powers proposed in this section would be used for the purpose of carrying out functions under the proposed legislation, including ensuring compliance and reviewing the continued appropriateness of conditions. Interested parties could seek a judicial review of their exercise in the manner described in Chapter 10. As with other information-gathering powers, a failure to provide the information requested with this power would attract sanctions as described in Chapter 9.

8.64 Information submitted to the Government under the new regime would be handled securely – clear information gateways would determine the other departments and agencies with whom it could be shared.

## A Government spending power

8.65 There may be instances where the Government concludes that it must spend public money in order to discharge its functions, for example in relation to remedies, under the proposed legislation. Therefore, the legislation will ensure that, **if and where necessary to protect national security, the Senior Minister is legally able to spend public money.** Any such step would be a last resort, pursued only when no other practicable or effective option was available, and approval for the power to spend would be sought from HM Treasury on a case-by-case basis. Government will continue to explore the most appropriate way of ensuring this, including whether a new spending power is required.

### Consultation Questions

- |    |   |
|----|---|
| 7. | What are your views about the proposed remedies available to the Senior Minister in order to protect national security risks raised by a trigger event?   |
| 8. | What are your views about the proposed powers within the regime for the Senior Minister to gather information to inform a decision whether to call in a trigger event, to inform their national security assessment, and to monitor compliance with remedies? |

# Chapter 9 – The potential sanctions for non-compliance

## Summary

- the Government will ensure that **strong and clear sanctions** are available to incentivise compliance and punish breaches of a regime designed to protect national security.
- sanctions will take the form of **criminal offences or civil financial penalties**.
- a **maximum custodial sentence of five years** will be available for most offences. Breaches of some information-gathering powers will attract lesser sanctions.
- the Government will be able to **impose financial penalties** on both individuals and businesses as an alternative to pursuing criminal convictions.
- the Government will also be able to apply for **director disqualification** instead of, or in addition to, any other sanction.

## Introduction

- 9.01 The proposed legislation, as described above, will require strong and clear sanctions to ensure compliance in order to protect our national security. This chapter describes the Government’s proposals for these.
- 9.02 Annex C includes a detailed table of all the proposed sanctions including setting out potential mitigations.

## Breaches of notices or conditions

- 9.03 The proposed legislation will establish a number of instances where parties would be required by the Senior Minister to take, or not to take, various steps. These are:
- **breach of a call-in notice:** if a trigger event is called in, the Senior Minister will send a call-in notice to the parties which will set out the process. The notice will set out that any person on whom the call-in notice has been served is liable to sanctions for breaching the call-in notice.
  - **breach of interim restrictions:** when a trigger event is called in, the Government will serve a call-in notice which will set out (if relevant) any interim restrictions. The notice will set out that any person on whom the

call-notice has been served is liable to be sanctioned for breaching the call-in notice, including any interim restrictions.

- **breach of a condition:** the Senior Minister may decide to impose conditions (remedies) on a trigger event to prevent or mitigate the national security risks. When a condition is imposed, the notice will set out that any breach of the condition is an offence.
- **breach of a compliance notice:** where there is a breach of an interim restriction or a condition the Senior Minister may serve a compliance notice as a preliminary step. The compliance notice will also inform the party that any breach of the compliance notice is in itself an additional and further breach.
- **breach of an order blocking the trigger event:** the Senior Minister may decide that the only way to mitigate the national security risk is to block it. The relevant order will inform the party that any breach of the order is an offence.
- **information-gathering breaches:** the Senior Minister will have the power to request information and, therefore, there are various sanctions for non-compliance with information requests or obstruction. Some of these breaches are considered to be of a more serious nature and therefore have a higher penalty. For instance, not providing information is considered to be a lesser breach than intentionally or recklessly providing false information.

9.04 The Government would always seek to act proportionately – this also applies in the event that it becomes aware of a potential breach of any notice or condition. It may be, in the first instance, that the Government would informally raise it with the parties concerned – potentially to draw a minor breach to their attention.

9.05 In the event that this approach was not successful or appropriate, the proposed legislation will permit the Senior Minister to serve a **compliance notice** on the party in breach. This notice would specify the breach of notice or condition which the Senior Minister considers has occurred and would specify what action the recipient should take as a result. The compliance notice should ensure that parties are in no doubt as to the seriousness of the action and are given the opportunity to take remedial action. Breach of the compliance notice would attract a sanction of itself – this may include a daily penalty to incentivise a quick response.

9.06 The Senior Minister could choose to serve a compliance notice instead of, or in addition to, commencing criminal proceedings or, as an alternative, imposing an administrative penalty as described below.

## The types of sanctions

- 9.07 The Government intends to legislate to introduce new criminal offences and civil sanctions for any breaches of requirements imposed under the reforms described in previous chapters.
- 9.08 Given its national security focus, it is appropriate that individuals committing a breach face the risk of significant sanctions. Therefore, criminal sanctions are appropriate.
- 9.09 However, the Government will have the flexibility to determine whether to pursue a criminal sanction or to take a more nimble, quicker approach through the imposition of administrative penalties. The proposed legislation will also provide the option for the Government to apply for director disqualification instead of, or in addition to, any other sanction.
- 9.10 The proposed legislation will set the maximum sentence and/or financial penalty for breaches, but this does not mean that the maximum sanction will be utilised in every case. There will be a defence where a person has a reasonable excuse or mitigating circumstances for permitting or allowing the breach.
- 9.11 The full list of breaches under the regime and the maximum criminal and civil sanctions is set out in Annex C. The table also sets out potential mitigating circumstances that would provide a defence.

## Criminal offences

- 9.12 The Government considers that the reforms' national security focus necessitates a significant custodial sentence being available to courts to act as a suitable deterrence to breaching, for example, conditions imposed or failure to unwind a transaction. In this context, it believes that a maximum sentence of five years' imprisonment is appropriate on indictment and/or an unlimited fine.
- 9.13 Therefore, with the exception of some of the information-gathering breaches, the Government intends to legislate so that criminal offences committed under the reforms will attract maximum penalties of:
- **summary:** statutory maximum fine and/or imprisonment of up to six months; or
  - **indictment:** unlimited fines and/or imprisonment for up to five years.
- 9.14 The Government has concluded that lower maximum sanctions should apply in relation to failures to comply with some information-gathering powers where

the consequences of non-compliance are considered to be lower risk to national security. Specifically, for failing to provide information, documents or to attend as a witness for the purposes of an investigation into a suspected breach of the regime, the Government proposes that the regime will attract maximum penalties of:

- **summary**: statutory maximum fine and/or imprisonment of six months; or
- **indictment**: unlimited fines and/or imprisonment for up to two years.

9.15 Parties may also fail to provide information, documents or to attend as a witness in circumstances other than an investigation into a suspected breach; for example, when the Senior Minister has requested information to inform a decision whether to call in a trigger event for a national security assessment. This type of failure to comply will attract only a civil penalty as described in the next section. However, knowingly providing false information or altering or suppressing information will remain a more serious offence (whether for the purposes of an investigation or not) and be subject to the higher sanctions detailed above. As described in Chapter 6, the Government proposes that where false information has been provided, it may be able to call in a trigger event to assess it in light of the now accurate information if, given this information, at that point, it reasonably suspected that the trigger event may raise a risk to national security.

## Civil financial penalties

9.16 The proposed legislation will also create new civil financial penalties as an alternative to criminal sanctions. This will ensure the sanctions available are flexible and appropriate. The Senior Minister could only pursue civil or criminal sanctions – not both.

9.17 Civil financial penalties are designed to be quick and proportionate responses to any breaches committed. To reflect this, the proposed legislation will require that they can only be imposed by the Senior Minister within 56 days of the breach coming to their attention.

9.18 Dependent on the individual case, the Government will be able to impose the penalty on the relevant entity(s) or individual(s). For breaches other than those related to failure to provide information, the maximum financial penalty will be either:

- **for a business**: up to 10% of worldwide turnover; or
- **for an individual**: up to 10% of total income or £500,000 (whichever is the higher).

- 9.19 For offences committed in relation to any failure to provide information, the maximum civil penalty will be:
- maximum one-off fine for business or individual: up to £30,000; or
  - maximum daily fine for a business or an individual: up to £15,000.
- 9.20 These maximum fines align with the equivalent penalties available to the CMA in relation to its information-gathering powers under Part 3 of the Enterprise Act 2002. However, the Government is considering whether these should be increased in order to ensure compliance with what is a national security-focused regime.

## Director disqualification

- 9.21 The Government will also have the power to apply for a director disqualification order as a sanction following breaches. The disqualification can be for up to 15 years. This can be imposed alongside criminal or civil sanctions, or can be imposed independently.
- 9.22 This will ensure that, where a breach is committed by a corporate body, those directors responsible for its actions can also be held to account. It will also ensure that where directors are not resident in, or a citizen of, the UK and therefore potentially could evade criminal or civil penalties, the Government has the ability to impose robust sanctions.
- 9.23 These sanctions could be applied to not only those who authorised the breach, but also those directors or senior officials who permitted the breach and failed to take action to prevent it, as well as those who ought to have known in their official capacity but failed to take action to prevent the breach. The Government does not wish those who were reckless to escape sanction.
- 9.24 It is important that Government is able to rigorously enforce the reforms and that people, including foreign investors, who commit a breach will face the full criminal and civil penalties available under the law. UK law regularly extends outside our shores. The CMA, for example, also has practical powers to intervene should a party not comply with its decisions. We intend for the regime to be similarly enforced and for sanctions and penalties to be imposed on both UK and foreign entities.

## Consultation Question

9. What are your views about the proposed range of sanctions that would be available in order to protect national security?

# Chapter 10 – Judicial oversight

## Summary

- the Government's powers under the new regime will be subject to **robust and transparent oversight**. A specific appeals process will be created for the regime.
- the appeals process will not be by means of a judicial review but will be based on and aligned with **judicial review principles** whereby appeals are made against the lawfulness of a decision (save for appeals against the imposition of financial penalties).
- appeals against **financial civil penalties** imposed by the Senior Minister will be on the basis of a full merits appeal.
- appeals against decisions under the regime will be heard by the **High Court**.
- appeals can be brought by anyone who can demonstrate 'sufficient **interest**' in the matter.
- an appeal will have to be brought **within 28 days** of the decision or action that is being challenged.
- the Government will be able to use **Closed Material Proceedings** to protect information harmful to national security.

## Introduction

- 10.01 The Government recognises the importance of ensuring proper robust and transparent oversight of the powers that will be granted by the proposed legislation.
- 10.02 This applies to all forms of executive powers, including those related to national security for which the Government has ultimate responsibility. While transparency is an important feature of our judicial system, the proposed legislation will need to take account of the fact that some information related to decisions cannot be disclosed publicly without undermining national security, even where that decision is appealed to court.
- 10.03 This chapter does not cover appeals against criminal sanctions – as any such appeal would follow the normal criminal appeals process.

## Appeals against decisions made by the Senior Minister

10.04 Domestic and international courts have long and rightly recognised successive governments' rights and responsibility in relation to protecting national security. It is right that decisions made to protect our national security are made by those directly accountable to Parliament. It would not be appropriate for courts to supplant ministers' decisions.

### What decisions should be subject to potential appeal

10.05 In the case of the proposed legislation, these decisions would include:

- a decision to call in a trigger event for scrutiny;
- a decision to impose a particular interim restriction at the point of, or following, calling in a trigger event;
- a decision to impose a particular remedy on a trigger event;
- a request to provide a particular piece of information to Government in order (for example) to inform its assessment of a trigger event it has called in;
- a decision to serve a compliance notice; or
- a decision to impose an administrative penalty.

### The grounds of appeal

10.06 Notwithstanding courts' recognition of the Government's role as guarantor of national security, it is essential that any decisions made by the Senior Minister are subject to rigorous judicial oversight to ensure their rationality.

10.07 The appeals process will be set out in statute and will be based on judicial review principles. This means that **appeals can only be made against the lawfulness of a decision** and the appeal will review the way in which a decision has been made. In line with the courts' and governments' respective roles in relation to protecting national security, the appeal should not review the merits of the decision reached. The only exception to this relates to the imposition of a financial penalty where the court would consider the merits and level of the penalty, as well as the process by which it was imposed.<sup>16</sup>

### Where the appeal will be heard

10.08 The Government considered the merits of establishing a dedicated appeals court for hearing appeals against decisions made under the proposed legislation. This would mirror the approach, for example, of the Special Immigration Appeals Commission or the Competition Appeal Tribunal, both of which are specialist courts established by legislation.

---

<sup>16</sup> In respect of appeals against criminal sanctions, the standard criminal procedure will apply.

10.09 However, the Government concluded that this would not be the appropriate way forward. The low volume of cases would not justify the costs associated with establishing and maintaining a separate judicial body. In addition, the Government considers that the matters likely to be assessed by the courts in relation to an appeal made under this proposed legislation are not so specialist as to require a dedicated court or tribunal. Therefore, any appeals against decisions made under the proposed legislation will be heard by the [High Court](#).

### **Who can appeal and when**

10.10 The Government is keen not to unduly limit who is able challenge a decision and plans to enable any person and/or organisation to be able to appeal if they can demonstrate a “sufficient interest in the matter” as is the case for judicial reviews. Appeal will not be restricted to the entities or individuals involved in the trigger event.

10.11 An appeal will have to be brought within 28 days of the decision or action that is being challenged. Having a 28 day time limit is to ensure certainty and speed for everyone. The Government understands that businesses, shareholders and individuals do not want decisions prolonged for a significant period. This process aligns with other statutory appeals processes which allow for 28 days, such as appeals under the Terrorism Prevention and Investigation Measures Act 2011.

10.12 Appeals will only be considered if they are brought through the statutory process, and all decisions will remain in force unless and until the appeal is successful.

### **How national security-related material will be protected during an appeal**

10.13 In any issue related to national security, there must be a balance between transparency and ensuring that sensitive material is not improperly disclosed. As such, the proposed legislation will permit the use of [Closed Material Proceedings \(CMPs\)](#) to protect material which, if disclosed, would undermine our national security.

10.14 The Government will mirror similar procedures as provided for under the Terrorism Prevention and Investigation Measures Act 2011. The Government intends that appeals against its decisions under the proposed legislation will follow a similar process. However, there will be a separate appeals process set out in the proposed legislation. The key difference to the appeals process under the Terrorism Prevention and Investigation Measures Act 2011 is that the Senior Minister will not be required to make an application for the use of

CMPs to the court at the outset of every appeal made under the legislation. This is because the Government expects that, by definition, any appeal of these decisions will involve sensitive material, and will require the use of CMPs.

10.15 This does not mean that any and all documents will be automatically covered by CMPs. The Government will, as is always the case, only seek to prevent public disclosure where not doing so would undermine national security. It would be for independent courts to assess the Senior Minister's request. Expert Special Advocates (appointed independently by the Attorney General) will represent claimants' interests in hearings to determine what material could be disclosed. They will also appear in any subsequent hearings considering material which the courts agreed should be protected in order to protect national security.

### Consultation Question

10. | What are your views about the proposed means of ensuring judicial oversight of the new regime?

---

# Chapter 11 – How the proposed reforms will interact with other regimes

## Summary

- in amending the Enterprise Act 2002 to implement this regime, the Government will create a [clear separation between competition- and national security-related assessments](#).
- it will retain the [independence of the Competition and Markets Authority \(CMA\)](#).
- the Government will design and implement its proposed national security reforms so that they [interface effectively](#) with the wider competition and public interest regime (for example, for deals that could jointly raise national security, competition and financial stability concerns).
- until the UK leaves the European Union, the Government will continue to be bound by, and comply with, its framework of directives and regulations including [EU Merger Regulations](#) and forthcoming [EU Foreign Direct Investment Screening Regulation](#).
- the Government intends to legislate so that the new assessment process sits as [efficiently as possible alongside other regimes and processes](#).

## Introduction

11.01 The Government recognises that the proposals covered in the preceding chapters, when implemented, will constitute a significant reform to its powers. It has proposed processes and time periods that are designed to be as predictable, transparent and reasonable as possible, while ensuring that the Government can take such steps as necessary to protect national security.

11.02 In line with the principles it established throughout this review, the Government wishes to ensure that these processes are implemented in as efficient a manner as possible. This includes ensuring that trigger events that are also relevant merger situations under the Enterprise Act 2002 are assessed in a co-ordinated fashion, while preserving the independence of the CMA. This efficient co-ordination must also apply to other domestic schemes and (until the UK leaves the European Union) EU-related legislation.

## Removing national security-related considerations from the public interest considerations in the UK competition regime

- 11.03 Certain trigger events covered by the proposed reforms will also be relevant merger situations as defined by section 23 of the Enterprise Act 2002. Therefore, as well as potentially being assessed by the new national security-focused regime, trigger events may also be scrutinised in relation to their impact on competition and other specified public interest grounds.
- 11.04 By introducing the proposed reforms described in this White Paper, there will no longer be a need for the public interest or the special public interest regimes insofar as they relate to matters of national security. They will still be required in relation to the protection they provide for the specified public interest grounds of financial stability and media plurality. Therefore, the Government will remove national security considerations from the public interest and special public interest regimes under the Enterprise Act 2002.
- 11.05 The Government has recently amended the turnover and share of supply thresholds set out in section 23 of the Enterprise Act 2002 in relation to specific areas of the economy that pose a particular risk to national security interests. These measures are a temporary step until primary legislation can be enacted, at which point they will no longer be needed as the Government will be able to scrutinise trigger events which raise national security concerns in these specific areas of the economy using its new powers. The Government will then reverse the above changes to section 23.

## The new regime's interaction with the merger regime

- 11.06 Once the proposed legislation is enacted, a trigger event may constitute a relevant merger situation and therefore need to be assessed in relation to its impact on competition by the CMA. A trigger event may need to be assessed in relation to:
- its national security risks – under the new regime; and
  - its impact on competition and/or another specific public interest ground– under the public interest regime in the Enterprise Act 2002.
- 11.07 The CMA will remain the independent and expert authority responsible for competition assessments (and its role in public interest interventions related to media plurality and financial stability will remain unchanged). National security matters are for the Government to assess.
- 11.08 The Government will ensure that any such cases are considered and processed in an efficient manner, and any decisions made by it and the CMA are implemented in an effective manner.

- 11.09 This will include measures to deal with the rare situations where decisions made under a national security assessment run contrary to the outcome of a CMA competition assessment.
- 11.10 In developing the precise legislative arrangements, the Government intends to design a process that:
- is **efficient** – ensuring a trigger event passes through both the national security and competition assessments as quickly as possible. This includes allowing information to be shared between the Government and CMA at appropriate times;
  - is **transparent** – providing predictability and certainty for all parties; and
  - maintains the operational **independence of the CMA** – the Senior Minister will have no powers to intervene directly in the CMA’s assessment of competitive impact. However (as below) the proposed legislation will ensure that the Senior Minister can take all necessary steps to protect national security, including when this may be at odds with the CMA’s assessment as to the best outcome for competition.
- 11.11 The Government welcomes respondents’ views about the specific arrangements and processes proposed in the remainder of this chapter.

### **How the proposed reforms and competition regime will interact in practice**

- 11.12 In most cases, the Government considers that relevant merger situations can be effectively scrutinised by the CMA and under the new regime in parallel. Where a national security assessment is ongoing, the Senior Minister could require the CMA to pause its competition assessment pending the outcome of the Senior Minister’s national security assessment. The proposed legislation will therefore establish new procedure for interaction when a national security issue has been identified with a trigger event also being scrutinised (as a relevant merger situation) by the CMA.

#### *When the Government blocks a merger on national security grounds while it is being assessed in relation to its impact on competition*

- 11.13 In the rare circumstances where it is necessary and proportionate for the Government to block a trigger event on the basis of national security considerations, the trigger event will stop. In this event, the CMA would likely end its competition assessment of the relevant merger situation, given it will no longer be proceeding. As set out in Chapter 7, completion of a trigger event which has been called in before approval has been given would be a breach and subject to sanctions.

*When the Government and the CMA's decision or proposed remedies are incompatible*

- 11.14 There may be instances where the Government's and the CMA's decisions or proposed remedies run contrary to each other. For example, the CMA may be happy to accept undertakings involving the divestment of a specific part of a target's business, while the Government is considering the imposition of a remedy that would restructure it in a wholly different fashion.
- 11.15 Under these scenarios, the Government will need to ensure that the outcome of a competition assessment should not undermine its national security-related decision (including any remedies it may have attached).
- 11.16 If the CMA's competition assessment has not yet been completed at the point that the Senior Minister reaches a decision about a trigger event which is also a relevant merger situation, the Government intends that the Senior Minister should have the power to issue a notice to the CMA to enable the Senior Minister to consider how the competition- and national security-related factors interact, at the end of a Phase 1 or Phase 2 assessment and to decide how to proceed. This may mean, in effect, overruling the CMA (for instance on any proposed undertakings) when the Senior Minister judges this necessary to protect national security. This is, in effect, the position as currently provided for in relation to merger situations that are subject to a Public Interest Intervention Notice and a Special Public Interest Intervention notice in the Enterprise Act 2002.
- 11.17 In practice, this will mean that the Government will apply adapted timings for competition assessments to be completed and undertakings to be agreed. The Government will not interfere in the CMA's deliberations on establishing a trigger event's merits on competition grounds.
- 11.18 The Government intends that a similar adapted process could be applied to merger situations that undergo both a national security assessment and that are also subject to a Public Interest Intervention Notice and/or a Special Public Interest Intervention Notice in relation to media plurality or financial stability grounds.
- 11.19 As now, any Government decision under the Enterprise Act 2002 public interest regime would be bound by the CMA's decision as to whether a relevant merger situation has arisen. In contrast, the CMA (nor any other body) would not be the arbiter as to whether a trigger event established by the proposed legislation had arisen.

## **When the CMA recommends a relevant merger situation should not go ahead on competition grounds, but the Senior Minister disagrees on national security grounds**

11.20 It may also be the case that the Government concludes that a merger should go ahead notwithstanding the CMA's conclusion that it would be harmful to competition. For example, where the Government wishes a takeover to take place (regardless of its impact on competition) to ensure that a UK-based entity continues to produce components critical to our Armed Forces. The Government will ensure that the Senior Minister should be able to consider the competition and national security aspects of the trigger event in the round at the end of the CMA's assessment and overrule the CMA if necessary to ensure that it takes place, even if the Senior Minister had not previously intervened under the new national security regime. This also replicates, in substance, the current position as provided for in the Enterprise Act 2002.

### **Remedies previously imposed by the CMA**

11.21 The Government also intends that the Senior Minister will (following a national security assessment of a trigger event) have the power to vary any undertakings or orders that have previously been put in place by the CMA where they are considered to be inconsistent with the interests of national security. This may arise where, for example, the CMA accepts an undertaking for divestment of part of the business but, following a national security assessment, the trigger event is blocked outright under the new national security regime.

11.22 The Senior Minister would have the power to give notice to the CMA to request that the CMA reconsiders the remedies in place and propose a solution which deals with the substantial lessening of competition in a way which avoids damaging national security. The final decision will be the Senior Minister's which may differ from any recommendation made by the CMA. The Government will take a similar approach to remedies that have previously been imposed through public interest or special public interest intervention cases but only in respect of remedies imposed after the commencement of the new regime.

11.23 The Government will not set any time limitation to the use of these new powers. However, they could not apply retroactively – **the Government could not intervene in remedies imposed before the new regime came into force.** The Government is clear that these powers are focused only to deal with situations where previous remedies are incompatible with the outcome of a specific national security assessment and could damage national security.

## **Information-sharing with the CMA**

- 11.24 There may be instances when the CMA is made aware of a trigger event in which it considers the Government may have a national security interest. The trigger event may be a relevant merger situation (as defined by the Enterprise Act 2002) or not.
- 11.25 The Government, therefore, proposes that the legislation would impose a duty on the CMA to provide information gathered in the course of its exercise of its functions to the Senior Minister, where it reasonably believes that the information it has collected would be relevant to a national security assessment. This would retain the purpose of section 105(6) of the Enterprise Act 2002 but would apply this duty to the broader range of trigger events covered by the new regime, not just the relevant merger situations defined by that Act.
- 11.26 The Government also intends to bring forward powers to allow it to share relevant information on individual trigger events with the CMA to ensure the national security assessment interacts effectively with the competition assessment. The Government will seek the consent of the relevant parties to share information where this information is unrelated to the specific national security assessment.

## **The Takeover Code**

- 11.27 The Takeover Code applies, broadly speaking, to offers for the shares of UK public companies whose securities are traded on the Main Market of the London Stock Exchange or on the Alternative Investment Market. The Takeover Code requires those making an offer for a company subject to the Code to set out their plans in relation to how they will handle the target company in the event of a successful takeover. The Takeover Code also sets out timetables for the completion of takeovers, including for the main stages of making and securing acceptance of an offer. The Takeover Panel is not, however, responsible for determining the merits of a takeover bid, nor does it have any authority to intervene in a takeover.
- 11.28 The Government will work closely with the Takeover Panel to consider how the proposed reforms would interact with the Takeover Code. This will include exploring with the Panel whether it judges any updates are needed to the timetable and process for the completion of takeovers to ensure that the new regime works effectively with the Takeover Code.

## Appeals in relation to trigger events involving grounds other than just national security

- 11.29 The protections and safeguards described in Chapter 10 in relation to judicial oversight of decision-making under the regime apply equally, of course, in relation to decisions made about trigger events which also have competition or other specified public interest considerations.
- 11.30 The issues related to the protection of sensitive information relating to national security also similarly apply – therefore the proposed legislation will permit that Closed Material Proceedings will be available in relation to appeals related to all of the Government’s national security decisions about trigger events, including those that also raise competition or other specific public interest considerations.

## EU Merger Regulation and forthcoming EU FDI Screening Regulation

- 11.31 The proposed reforms will need to also work effectively and efficiently alongside EU-related law so long as the UK is bound by it. The EU Merger Regulation (EUMR) is the current key regulation.
- 11.32 Under the EUMR, where a relevant merger situation is also a concentration with an EU dimension, the European Commission (the Commission) has exclusive competence to investigate the merger and will apply EU competition law.<sup>17</sup> In certain circumstances, the investigation can be returned to national competition authorities, which will apply national competition law instead.
- 11.33 Member States are able to take appropriate measures to protect their legitimate interests, in respect to the Commission’s investigation on competition grounds. Under the EUMR, the definition of legitimate interests is limited to public security, media plurality and prudential rules. Under the Enterprise Act 2002, the Secretary of State can give a notice to the CMA if he or she believes that it is, or may be the case, that a public interest

---

<sup>17</sup> The European Commission will look at cases which exceed certain turnover thresholds, namely a) where the combined worldwide turnover of all undertakings concerned is over €5 billion, and the aggregate EU-wide turnover of at least two undertakings is over €250 million, or b) where the combined worldwide turnover of all undertakings concerned is over €2.5m, the aggregate EU-wide turnover of each of at least two of the undertakings concerned is over €100 million, and the combined aggregate turnover of all the undertakings concerned is over €100 million in at least three Member States (MSs), and in each of at least three of these MSs, the aggregate turnover of at least two of the undertakings concerned is over €25 million. But the Commission will not look at cases if the all the undertakings concerned achieve more than two-thirds of their aggregate EU-wide turnover within one and the same MS.

consideration is relevant to a consideration of the relevant merger situation concerned, and it is appropriate to protect the UK's legitimate interest. This is known as a European Intervention Notice.

- 11.34 Where a European Intervention Notice has been given, the Government can take action with a view to remedy, mitigate or prevent effects adverse to the public interest which have resulted from, or may be expected to result from, the creation of the European relevant merger situation. The action may include requiring the CMA, acting through a Phase 2 Inquiry Group, to investigate and report on public interest issues, and the taking of interim and final enforcement action required to resolve such issues.
- 11.35 These existing powers mean that, in effect, if the Commission was to clear a transaction on competition grounds under the EUMR, it would still be open to the Government to intervene on the basis of national security and impose its own conditions. However, if the Commission was to block a transaction which the Government considered to be in the interests of the UK's national security, it is understood that the Government would not be able to override the block imposed by the Commission. This will necessarily continue to be the case while the EUMR continues to apply in the UK.
- 11.36 The proposed legislation, removing the national security components of the public interest regime within the Enterprise Act 2002, will make similar provision to ensure that the Government's scrutiny of a trigger event interacts efficiently with the EUMR.
- 11.37 Additionally, the European Commission has proposed an [EU-wide FDI screening regulation](#) to provide a cooperation mechanism between Member States, to mitigate against potential security risks posed by FDI from third countries into the EU. The proposal sets out procedural requirements for Member States both with and without a formal national security screening mechanism, as well as annual reporting obligations. This cooperation mechanism also obliges Member States to share information on their screening activity, including live cases, in order for other Member States to provide comments. There is also the facility for the European Commission to provide non-binding opinions.
- 11.38 If the proposed EU Regulation comes into force before the end of the Implementation Period, the UK will become subject to it until the Implementation Period concludes in December 2020. The Government will carefully consider what the EU Regulation means for both its existing powers under the Enterprise Act 2002 and the proposed legislation set out in this White Paper.

## The new regime's interaction with other statutory and regulatory regimes

- 11.39 The Government is aware that the national security assessment process introduced by the proposed legislation may take place alongside other statutory or regulatory regimes or processes. For example, the Government may call in a trigger event involving the takeover of a business or an asset sale in a specific sector, where an existing regulator already has powers to provide licences to businesses to operate in the sector. This is the case in the water sector (for example), where water supply and sewerage licenses are granted by Ofwat based on an assessment of a potential operator's managerial, financial and technical competencies.
- 11.40 The Government intends that the new system interacts effectively with other existing regimes. Independent regulators operate across a number of sectors, many of which are also national infrastructure sectors where (as described in the draft statement of policy intent) it is more likely that the call-in power will be exercised. This includes the communications, water, nuclear and aviation sectors – regulated by Ofcom, Ofwat, the Office for Nuclear Regulation and the UK Civil Aviation Authority respectively. The scope of existing powers for intervention varies across sectors and regulators – such as licensing schemes for ongoing enterprises, or prior approval being required before a new infrastructure project is commenced. The precise processes and timescales varies considerably across these regimes.
- 11.41 It is conceivable that a decision made under the proposed national security regime could run contrary to that of another regime. Measures that might be suitable for addressing a negative market impact in a specific sector could run contrary to those that would mitigate the national security risks. When this arises, the Government is clear that the operational independence of existing regimes must be maintained. However, the Government will ensure that any action to address national security risks must take precedence.
- 11.42 To mitigate situations where the outcome of a national security assessment runs contrary to that of other existing regimes, the Government will consider if bespoke, adapted procedures are necessary to ensure Ministers have the opportunity to consider the national security implications of sector-specific regulatory decisions. This includes considering if it would be appropriate to pause other regimes or apply adapted timelines to ensure that the Government can consider both the sector specific issues and national security risks in the round. Such powers could be similar to those proposed earlier in this chapter in relation to interactions between the national security assessment process and the competition regime.

11.43 The Government intends to bring forward powers to allow it to share relevant information on individual trigger events with other departments, regulators and agencies to ensure the proposed reforms interact effectively with other assessments. The Government will seek the consent of the relevant parties to share information where this information is unrelated to the specific national security assessment. This is similar to the Government's proposed approach to information-sharing with the CMA. The Government will examine how to deal retrospectively with historic decisions through other regimes that may be incompatible with the outcome of a national security assessment.

11.44 The Government welcomes views from respondents about the proposals in this chapter and the precise means by which the new regime should be designed and implemented in the most efficient manner for businesses, investors and regulators alike.

### Consultation Question

11. | What are your views about the proposed manner in which the new regime will interact with the UK competition regime, EU legislation and other statutory processes?
-

## Annex A – List of consultation questions

1. What are your views about the proposed tests for trigger events that could be called in for scrutiny if they met the call-in test?
2. What are your views about the proposed role of a statement of policy intent?
3. What are your views about the content of the draft statement of policy intent published alongside this document?
4. Does the proposed notification process provide sufficient predictability and transparency? If not, what changes to the proposed regime would deliver this?
5. What are your views about the proposed legal test for the exercise of the call-in power? Does it provide sufficient clarity about how it would operate?
6. What are your views about the proposed process for how trigger events, once called in, will be assessed?
7. What are your views about the proposed remedies available to the Senior Minister in order to protect national security risks raised by a trigger event?
8. What are your views about the proposed powers within the regime for the Senior Minister to gather information to inform a decision whether to call in a trigger event, to inform their national security assessment, and to monitor compliance with remedies?
9. What are your views about the proposed range of sanctions that would be available in order to protect national security?
10. What are your views about the proposed means of ensuring judicial oversight of the new regime?
11. What are your views about the proposed manner in which the new regime will interact with the UK competition regime, EU legislation and other statutory processes?

# Annex B – Indicative list of potential conditions

- B.01 As described in Chapter 8, the Senior Minister will have the power to impose any remedy that they considered necessary and proportionate to protect national security.
- B.02 The Government proposes that the legislation would provide an indicative, but not exhaustive, list of the types of conditions that the Senior Minister may impose, including the purpose of each condition. Further details will be provided in non-statutory guidance. It is hoped that this will provide clarity and certainty to businesses and may help parties develop potential undertakings to propose, and that the Government could then accept by imposing on the trigger event.
- B.03 Below are, firstly, a non-exhaustive list of the [purposes](#) that conditions may seek to have, and secondly, a non-exhaustive list of the [types of conditions](#) that the Senior Minister may impose, linking each to one of these purposes.

## The purposes of conditions

- [ensure the maintenance of strategic capability](#): this might include a condition to continue to procure a product in respect of a component critical to national infrastructure, or that a foreign entity continue to retain the entity's existing supply company to address a threat to national security.
- [protect confidential/sensitive information](#): this might include ensuring that all matters/ information in relation to a programme be maintained in line with UK national security regulations, or that only personnel with appropriate UK clearances have access to confidential material or that only such personnel should be a part of the operational management of the business.
- [protect intellectual property](#): this would restrict the transfer, sale or use of any intellectual property rights relevant to national security. Such conditions may require that intellectual property is not used for certain purposes in certain locations.
- [ensure compliance](#): this might include imposing measures as to supervisory or other actions that should be taken to ensure compliance with UK regulatory regimes.
- [ensure economic viability and financial health](#): this may be in the shape of a condition requiring the investor to demonstrate that they are able to sustain the on-going operation of the entity to continue to provide the essential service. There are examples of financial health requirements within the

regulation sphere. In relation to the regulation of financial services, for example, the Financial Services and Markets Act 2002 includes financial health requirements.<sup>18</sup> There are also financial viability tests in respect of the granting of licences under the EU Council Regulation Licensing Regulation where applicants for certain types of licences to operate commercial air travel must pass a financial test and the Civil Aviation Authority will continue to monitor their financial health.<sup>19</sup>

## Types of conditions

### Access condition

- a condition limiting access to a particular site operated by the acquired entity to certain named individuals.

### Information/operations condition

- a condition that only personnel with appropriate UK security clearances have access to confidential information or that only such personnel should be part of the operational management of the business.

### Supply chain condition

- condition that a new acquirer retains an acquired entity's existing supply chain for a set period.

### Intellectual Property condition

- a condition restricting the transfer or sale of IP rights (to be tailored to the individual circumstances of the case and the national security risks identified).

### Access condition

- a condition requiring that access to dual use technologies and information about their design, materials, uses or supply chains be restricted to certain named individuals within the investor company or a third party associated with them.

### Compliance condition

- a condition imposing supervisory measures, periodic reporting or other actions (to be decided on a case-by-case basis) that should be taken to ensure compliance with UK regulatory regimes.

---

<sup>18</sup> See Schedule 6, Part 1B Part 4A, paragraph 2D.

<sup>19</sup> EU Council Regulation Licensing Regulation 1008/2008

### **Monitoring condition**

- a condition requiring that Senior Minister (or their representative) be given access to information on the company's activities.

### **Personnel condition**

- a condition requiring the acquirer to secure the Senior Minister's approval for appointments of any Directors and other key personnel.

### **Structural condition**

- a condition requiring the retention of UK staff in key roles at a particular sensitive site.

### **Proximity condition**

- a condition requiring the relevant person (most likely a person with title, control or interest over the proximate site) to maintain such measures as the Senior Minister may specify e.g. physical or personnel security, restrictions on access.

## Annex C – List of sanctions and offences created by the regime

- C.01 This Annex sets out the list of potential breaches that would be established by the introduction of the new regime described in this White Paper. For each, it describes the proposed sanctions that would apply.
- C.02 The sanctions set out the maximum criminal or civil penalty the Government is proposing would be applicable to each breach. We do not envisage that the maximum penalty would be imposed in every case, the precise level would depend on the circumstances of the individual case. In any event, only one of a criminal offence or civil penalty could be sought.
- C.03 As described in Chapter 9, the Senior Minister would have the power to seek a director disqualification order either alongside other sanctions or as a standalone penalty.

Breach	Details	Sanction
<b>Breach of a call-in notice</b>	<p>The Government will have ability to call in a trigger event for screening in the event it is not notified (this is set out in Chapter 6). If a trigger event is notified it will go through the screening process and the Senior Minister will decide whether it should be called in for further scrutiny.</p> <p>If a trigger event is called in, the Senior Minister will send a call-in notice to the parties which will set out the process. The effect of a call-in notice being served is to place a ban on all those on whom the call-in notice has been served from completing the trigger event or, where the trigger event has already taken place, to prevent further steps as set out in the notice.</p> <p>The notice will set out that any person on whom the call-notice has been served or is liable to criminal and/or civil sanctions for breaching the call-in notice. Breaching a call-in notice is an offence as it could undermine national security and it undermines the ability of the Government to protect national security.</p> <p>A potential mitigation could be if a party had a reasonable belief that the interim restrictions were being complied with.</p>	<p><b>Criminal Offence</b>            Summary: fine – statutory maximum            Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b>            Company: 10% of worldwide turnover;            Individual: 10% of total income or £500,000 (whichever is higher).</p>

Breach	Details	Sanction
<p style="text-align: center;"><b>Breach of interim restrictions</b></p>	<p>When a trigger event is called in, the Government will serve a call-in notice notifying relevant parties about this.</p> <p>The call-in notice will set out any interim restrictions that have been imposed whilst the Senior Minister is scrutinising the trigger event. Interim restrictions can also be imposed subsequent to the call-in notice being served.</p> <p>These interim restrictions may prevent the transfer of specified information or access to specified sites. They are imposed to prevent a trigger event posing a risk to national security before the Senior Minister can scrutinise and consider the trigger event.</p> <p>Breaching a call-in notice is an offence as it could undermine national security and it undermines the ability of the Government to protect national security. However, the Government can also impose sanctions for the breach immediately depending on the nature and the severity of the breach.</p> <p>A potential mitigation could be if a party had a reasonable belief that the interim restrictions were being complied with.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Company: 10% of worldwide turnover; Individual: 10% of total income or £500,000 (whichever is higher).</p>
<p style="text-align: center;"><b>Breach of a condition</b></p>	<p>Following scrutiny, the Senior Minister may decide to impose conditions on a trigger event to prevent or mitigate the national security risks. These are set out in Chapter 8 and Annex B which provides an indicative list of the potential conditions.</p> <p>When a condition is imposed, it will be set out that any breach of this condition is an offence. As these conditions have been imposed to protect UK national security, any breach could potentially undermine national security. Depending on the circumstances and the breach, the Senior Minister could firstly issue a compliance notice – setting out there has been a breach of interim restrictions – before imposing sanctions for the breach. However, the Senior Minister can also impose sanctions for the breach immediately depending on the nature and the severity of the breach.</p> <p>A potential mitigation could be if a party had a reasonable belief that the conditions were being complied with.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Company: 10% of worldwide turnover; Individual: 10% of total income or £500,000 (whichever is higher).</p>

Breach	Details	Sanction
<p style="text-align: center;"><b>Breach of a compliance notice</b></p>	<p>Where there is a suggested breach of an interim restriction or a condition, the Senior Minister can serve a compliance notice to inform the party that they are in breach and to request that they stop the breach or do not repeat the breach, as appropriate. However, the Senior Minister can also impose sanctions for the breach immediately depending on the nature and the severity of the breach.</p> <p>A potential mitigation could be if a party had a reasonable belief that the compliance notice was being complied with.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Company: 10% of worldwide turnover; Individual: 10% of total income or £500,000 (whichever is higher).</p>
<p style="text-align: center;"><b>Breach of a blocking order</b></p>	<p>The Senior Minister may decide that the only way to mitigate the national security risks from the trigger event is to block the trigger event. In this case the Senior Minister will impose a blocking order on the trigger event. If it has already occurred this may be done in conjunction with an unwind order (i.e. the trigger event would have to be unwound and a blocking order would be placed preventing the trigger event from occurring again).</p> <p>Breach of a blocking order is a serious offence. The Government expects that blocking a trigger event would only be done as a last resort and when it is the only method to safeguard national security. We do not envisage there would be potential mitigations to this or that someone could break a blocking order and remain unaware. More details on when a trigger event could be blocked are set out in Chapter 8.</p> <p>The Government does not consider there are any potential mitigating circumstances as a breach of a blocking order requires clear action in contravention of the blocking notice.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Company: 10% of worldwide turnover; Individual: 10% of total income or £500,000 (whichever is higher).</p>
<p style="text-align: center;"><b>Failure to comply with requirement to provide information, documents or attend as a witness in accordance with the notice</b></p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness. It is an important part of the screening and scrutiny process to ensure that the Senior Minister is able to access the necessary information in order to review the trigger event and potential national security risks. The Senior Minister will have the power to request this information either before call-in, following call-in or in connection with monitoring or reviewing the regime.</p> <p>Failure to comply hinders the Senior Minister in making a reasonable assessment.</p>	<p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>

Breach	Details	Sanction
<p>For the purposes of an investigation, failure to comply with requirement to provide information, documents or attend as a witness in accordance with the notice</p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness. It is an important part of the screening and scrutiny process to ensure that the Senior Minister is able to access the necessary information in order review the trigger event and potential national security risks.</p> <p>Failure to comply for the purposes of an investigation is a more serious breach than failure to provide information for other purposes. This is because the use to which the information may be put is different given it is for the purpose of conducting an investigation into a potential breach of the legislation which could lead to higher sanctions. This aligns with CMA powers under section 193 of the Enterprise Act 2002.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum and/or imprisonment of up to six months; Indictment: unlimited fine and/or imprisonment up to two years.</p> <p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>
<p>Intentionally altering, suppressing or destroying a document following service of a notice to produce it</p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness (information-gathering powers). It is an important part of the screening and scrutiny process to ensure that the Senior Minister is able to access the necessary information in order review the trigger event and potential national security risks.</p> <p>Failure to comply hinders the senior Minister in making a reasonable assessment.</p> <p>The Government does not consider there are any potential mitigating circumstances as intentionally altering, suppressing or destroying documents requires clear action with intent to undermine the ability of the Government to make a reasonable assessment.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum and/or imprisonment of up to six months; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>
<p>Intentionally obstructing or delaying another from complying with an information-gathering notice</p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness. It is an important part of the screening and assessment process to ensure that the Senior Minister is able to access the necessary information in order review the trigger event and potential national security risks.</p> <p>Failure to comply hinders the Senior Minister in making a reasonable assessment.</p> <p>The Government does not consider there are any potential mitigating circumstances as intentionally obstructing or delaying another with complying requires a clear action with intent to undermine the ability of the Government to make a reasonable assessment.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum and/or imprisonment of up to six months; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>

Breach	Details	Sanction
<p>Supplying information or documents or providing evidence that a person knows to be false or misleading or being reckless in doing so</p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness. It is a important part of the screening and assessment process to ensure that the Senior Minister is able to access the necessary information in order review the trigger event and potential national security risks.</p> <p>Failure to comply hinders the Senior Minister in making a reasonable assessment.</p> <p>The Government does not consider there are any potential mitigating circumstances as knowingly supplying false or misleading information requires a clear action with intent to undermine the ability of the Government to make a reasonable assessment.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum and/or imprisonment of up to six months; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>
<p>Intentionally or recklessly providing evidence that the person knows to be false</p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness. It is an important part of the screening and assessment process to ensure that the Senior Minister is able to access the necessary information in order review the trigger event and potential national security risks.</p> <p>Failure to comply hinders the Senior Minister in making a reasonable assessment.</p> <p>The Government does not consider there are any potential mitigating circumstances as intentionally providing false information requires a clear action and intent to undermine the ability of the Government to make a reasonable assessment.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum and/or imprisonment of up to six months; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>
<p>Supplying information, documents or providing evidence that a person knows to be false or misleading or being reckless in doing so</p>	<p>The Senior Minister will have the power to request information, documents or for a person to attend as witness. It is an important part of the screening and assessment process to ensure that the Senior Minister is able to access the necessary information in order review the trigger event and potential national security risks.</p> <p>Failure to comply is hinders the Senior Minister in making a reasonable assessment.</p> <p>The Government does not consider there are any potential mitigating circumstances as intentionally providing false information requires a clear action and intent to undermine the ability of the Government to make a reasonable assessment.</p>	<p><b>Criminal Offence</b> Summary: fine – statutory maximum; Indictment: unlimited fine and/or imprisonment up to five years.</p> <p><b>Civil Penalty</b> Maximum: £30,000; Maximum daily rate: £15,000.</p>





© Crown copyright 2018

**Department for Business, Energy & Industrial Strategy**

[www.gov.uk/beis](http://www.gov.uk/beis)