Home Office

Legislation to Counter State Threats (Hostile State Activity)

Government Consultation

This consultation begins on **Thursday 13th May 2021**

This consultation ends on **Thursday 22nd July 2021**

About this consultation

To:	This consultation is open to the public. We will be particularly interested to hear from those who may be impacted by the proposals, should they form legislation, including those in Industry and Research as well the general public.
Duration:	From Thursday 13th May 2021 to Thursday 22nd July 2021
Enquiries to:	State Threats Consultation Homeland Security Group Home Office 5th Floor, Peel Building 2 Marsham Street London SW1P 4DF CST.Consultation@homeoffice.gov.uk
How to respond:	Please provide your response by 17:00 on Thursday 22nd July 2021 at: https://www.homeofficesurveys.homeoffice.gov.uk/s/2RJAKB/ If you are unable to use the online system, for example because you use specialist accessibility software that is not compatible with the system, you may download a word document version of the form and email or post it to the above contact details. Please also contact the above details if you require information in any other format, such as Braille, audio or another language. We may not be able to analyse responses not submitted in these provided formats.
Response paper:	A response to this consultation exercise is due to be published at https://www.gov.uk/government/consultations/legislation-to-counter-state-threats

Ministerial Foreword

The threat from hostile activity by states is a growing, diversifying and evolving one, manifesting itself in a number of different forms: from cyber-attacks, attempts to steal intellectual property and sensitive government information, threats to critical national infrastructure, and attempts to interfere in democratic processes. We continue to face this very real and serious threat from those who seek to undermine and destabilise our country to pursue their own agendas.

The UK will always defend its people and its interests, and we have a record of responding robustly to hostile activity by states alongside our international partners. Together with our allies, the UK is taking steps to safeguard our open and democratic societies and promote the international rules-based system that underpins our stability, security and prosperity.

As part of our Manifesto we made two commitments that are relevant to this work:

> *We will invest in the police and security services and give them the powers they need to combat new threats;* and
>
> *We will protect the integrity of our democracy, by introducing identification to vote at polling stations, stopping postal vote harvesting and measures to prevent any foreign interference in elections.*

We are already making the UK safer by strengthening our ability to deter, withstand and respond to hostile activity by states. Under this Government, my department has:

- brought into force a new power under Schedule 3 to the Counter-Terrorism and Border Security Act 2019 to help protect public safety by allowing an examining officer to stop, question and, when necessary, detain and search, individuals and goods travelling through UK ports and the border area for the purpose of determining whether the person appears to be someone who is, or has been, engaged in hostile activity. This Government continues to bring together all the tools at its disposal, because evolving threats and new technologies make doing so more vital than ever.
- made public the Joint State Threats Assessment Team (JSTAT) which were established in 2017 to better understand the threat and inform the Government's response. Publicly avowing their work will support them in maximising their utility to the national security community, enabling them to reach out to all parts of the Government, as well as stakeholders across a number of sectors offering the opportunity to gain a better understanding of

state threats and enabling greater analytic challenge. This also allows broader communication of the threats across Government and agencies, as well as partners across the private and charitable sector, ensuring they have access to information to better protect themselves.

- continued to use existing tools and powers, including immigration powers, to protect the country from this threat.
- supported our intelligence and law enforcement agencies in their work to counter these threats.

But I recognise there is more we can do and this consultation forms part of our continuing efforts to empower the whole national security community to counter the insidious threat we face today by introducing new legislation.

I welcome the work of the Law Commission in their Review on the Protection of Official Data, which closely analysed the Official Secrets Acts, and recognise that the proposals contained in this consultation are of interest across a range of sectors. It will be vital that the tools and powers we legislate for work in harmony with our commitments to keep Britain an open and vibrant society to do business in and with; our strong record on academic and press freedoms; and on retaining our position as a leading global destination for research and development.

This country is fortunate to have the best security services in the world. I stand shoulder to shoulder with them, just as I do with our police. I am committed to ensuring we have the tools in place to keep this country safe and welcome your input to ensure we make the UK a more challenging environment for states to conduct hostile activity in and increase the cost to them of doing so.

The Rt. Hon. Priti Patel MP

Home Secretary

Contents

Glossary of Key Terms

State Threats (ST) – Is a term used to describe overt or covert action orchestrated by foreign governments which falls short of general armed conflict between states but nevertheless seeks to undermine or threaten the safety and interests of the UK, including: the integrity of its democracy, its public safety, its military advantage and its reputation or economic prosperity. While the term hostile state activity (HSA) has generally been used to describe the threat, it is often read as being activity conducted by hostile states rather than hostile activity by states as intended. In this consultation and through to the legislation the Government is adopting new terminology to describe the threat.

Espionage – Is the covert process of obtaining sensitive confidential information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems).

Joint State Threats Assessment Team (JSTAT) - Is a cross-departmental assessment organisation that provides analysis on the hybrid state threats to the UK and UK interests. It assesses the national security threat posed by activities such as espionage, assassination, interference in our democracy, threats to the UK's economic security and the UK's people and assets overseas.

National Cyber Security Centre (NCSC) - The NCSC provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments on issues relating to cyber security. When incidents do occur, they provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

Foreign Direct Investment (FDI) - Whilst often beneficial to the UK economy, FDI through acquisitions, mergers, joint ventures and other financial relationships can also pose a national security risk. For example, it can be used by foreign states to gain control or influence over, or access, to a business and its assets in a way causes or for the purpose of causing damage to UK national security.

Unauthorised Disclosure – A disclosure of official information (from specific categories listed under the Official Secrets Act 1989) without lawful authority.

Primary Disclosure – A disclosure of official information by an individual who – most often by virtue of their profession – has access to the primary source of the material and discloses or publishes it.

Onward Disclosure – A disclosure of official information (from specific categories listed under the Official Secrets Act 1989) by an individual who does not have access to the primary source of the material, but discloses or publishes it further, once it has been shared with them by a primary discloser, without authorisation or shared in confidence.

Introduction

Background

In 2018 the then Prime Minister announced that the Government would be taking a number of steps to address the threat posed to the UK by the hostile activities of foreign states. This included introducing a new power to allow police to stop those suspected of conducting hostile activity on behalf of a foreign state at the border and, in slower time, conducting a comprehensive review of the tools and powers available to counter the threat. The former was delivered through the Counter Terrorism and Border Security Act 2019 and came into force in 2020.

In March 2019, the former Home Secretary announced that the Home Office was working towards introducing new legislation and the Queen's speech in December 2019 announced that 'measures will be developed to tackle hostile activity conducted by foreign states'[1]. Although this work was instigated following the attack in Salisbury in 2018, the Government has been considering potential legislative changes to address the full range of state threats and this consultation is the next step in this phase of work. This work is also being informed by the Law Commission Review of the Protection of Official Data (see the section on Official Secrets Acts reform for further detail).

In considering this consultation, consultees may also wish to be aware of the wider national security and legislative context, set out at Annex A. This section sets out a number of tools and programmes that already exist across Government to address the threat and will be supplemented by new legislation in this area.

Separately, the Intelligence and Security Committee of Parliament (ISC) have published a report following their inquiry into Russian Interference. While this consultation does not specifically respond to that work and while the proposals set out in this document are not targeted at any specific country, consultees may wish to consider the content of the Russia report[2] and the formal Government response,[3] when considering the proposals set out below.

The Threat

The Nature of the Threat[4]

States engage in and orchestrate overt and covert action which falls short of general armed conflict but nevertheless seeks to undermine or threaten the safety and interests of the UK, including: the integrity of its democracy, its public safety, its military advantage and its reputation or economic prosperity. Although often referred

[1]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853886/Queen_s_Speech_December_2019_-_background_briefing_notes.pdf
[2] http://isc.independent.gov.uk/news-archive/21july2020
[3]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf
[4] This assessment has been informed by the work of the Joint State Threats Assessment Team (JSTAT) and they agree this is an accurate reflection of the threat in the UK. JSTAT are an independent assessment body. As such, while their work has informed the threat assessment they are not involved in, nor do they take a view on, the policies and responses proposed in this consultation.

to as Hostile State Activity (HSA) it is important to recognise that this term refers to hostile activity undertaken by states, as opposed to activity undertaken by hostile states.

This is a growing, diversifying and evolving threat, which manifests itself in a number of different forms. States who engage in hostile activity in or against the UK are becoming increasingly emboldened, asserting themselves more aggressively, to advance their geo-political objectives and undermine our own.

At a strategic level, this activity seeks to undermine the UK's security, prosperity, social cohesion, resilience, democracy, values, institutions and strategic advantage, as well as the rules based international system and associated organisations that underpin all of the above.

Broadly speaking the threat can be broken down into 5 categories:

1. Physical threat to people - This includes any physical harms directed towards individuals; including assassination, forced repatriation and harassment. A small number of states present a physical threat to UK interests, citizens and residents at home and abroad, as well as third-country nationals in the UK.
2. Physical threat to things – a sabotage risk where states might seek to cause damage or disruption to infrastructure physically and/or by cyber means. While the primary concern relates to UK infrastructure in the UK or abroad, this threat can manifest itself in attacks on foreign infrastructure that has a downstream impact in the UK – such as attacks on oil or gas pipelines affecting fuel prices for UK business, or attacks on infrastructure, which forms part of critical UK supply chains abroad.
3. Espionage – which is the covert seeking of sensitive confidential information across a range of areas by means of human intelligence (including spies or other human sources), signals intelligence (the intercepting of communications), technical intelligence (eavesdropping and other close access methods) and penetration and disruption of computer networks. The UK Government, industry, academia, defence and business sectors are routinely targeted by foreign states seeking sensitive information and the UK economy is a significant vector for espionage activity. Some states have advanced espionage capabilities both technical (including online) and using human sources.
4. Interference – which covers a wide range of activity through which states seek to further their aims by use of covert means or by obfuscation of intent and originator, including disinformation[5], bribery and coercion. This also includes attempts to interfere in our democracy or Government policy making, including through interference in national, regional or local elections and referenda, as well as attempts to undermine academic freedoms. A number of states conduct persistent activity which attempts to distort UK and international information environments through the use of information operations which often play on existing divisions.

[5] Disinformation is defined here as the deliberate creation and/or sharing of false or manipulated information with the intention to deceive or mislead audiences.

5. Threats to geostrategic interests – states can use covert means and intelligence techniques rather than legitimate diplomatic engagement to seek to challenge the rules-based international order, challenging the UK's interests and seeking to undermine the UK's existing alliances. States also use these techniques to seek to influence international standards, particularly for new and emerging technologies, for their own interests or to the detriment of our own.

The threats above can be delivered in a range of ways including directly by foreign governments or foreign intelligence services or indirectly through firms or individuals working for or on behalf of foreign governments or foreign intelligence services. In the latter cases, such co-operation may be intentionally done in the support of the state, or it could be incidental to other work, or completely unwitting.

One vector through which the espionage threat can manifest itself is through foreign direct investment (FDI), where we are seeing novel means to undermine the UK's national interests that go beyond traditional mergers and acquisitions, such as; structuring deals to obscure who is behind them and acquiring sensitive assets such as intellectual property. Such behaviour left unchecked can leave sensitive UK businesses vulnerable to disruption and espionage.

The UK is one of the best places to engage in collaborative research and collaboration and engagement within the UK, where open and transparent, will continue to be welcome. However, states can use academic co-operation to enable them to work with experts in fields of cutting-edge research and innovation, and obtain the resulting output of that work, all without having to steal it (through traditional cyber espionage, for example). It provides those with hostile intent overt access to expertise, IT networks and research.

It is crucial that the Government is able to fully combat these threats coming from an ever more determined set of hostile actors. Hostile involvement in UK research and businesses can provide a vehicle for other forms of hostile activity such as interference.

The impact of State Threats

The impact and cost of hostile activity by states can be difficult to measure and quantify. In most cases the hostile activities are intended and designed to be invisible while they are happening, and for a long time after. Even where the activity is identified, the cost may not be visible to the victims of the activity or to the public at large for some time, if at all. It may be years, or only in a time of national crisis or war, before the full impact of those actions are realised.

The physical threat to people is a more visible form of state threat, particularly when it results in deaths or serious injuries to people, as we have seen in recent times in both the UK and beyond. The links between the physical and espionage threats are clear. The acquiring of data through espionage could identify British operatives abroad or individuals under the UK's protection, which could therefore directly or indirectly lead to them coming to harm.

The physical threat to locations can also have a significant impact, from affecting critical services such as gas or electricity, to affecting supply chains and therefore the price and supply of goods in the UK.

The National Cyber Security Centre's annual report for 2020[6] notes some of the cyber threats that exist, assessing, for example, that there have been state linked attempts to acquire Intellectual Property (IP) relating to COVID vaccine research and noting that hostile actors have almost certainly sought to interfere in recent elections.

In monetary terms the impact of hostile activity by states can be difficult to measure and quantify. The US estimates that economic espionage costs the US economy $400bn[7] per year and that the overall cost of hostile activity by states to the US to be hundreds of billions of dollars[8]; no similar figure has yet been calculated for the UK, but we believe that it is likely to be very significant. The fundamental impact of the public losing confidence in Parliamentary democracy or the loss of the UK's strategic advantage would be priceless, and it can be hard to assign values to the cost of an official passing intelligence to a foreign state – costs could include the loss of investment in capabilities which are undermined as well as remedial costs that seek to mitigate the impact of that harm.

The evolution of the threat

The threat has evolved since the last time the UK substantively legislated on this issue. The Official Secrets Act 1911 and subsequent acts in 1920 and 1939 were primarily focussed on the threat posed by early 20th Century Germany. Since then the global landscape has changed significantly, with collaboration between states offering benefits in a wide range of areas. The traditional way of viewing states as hostile and non-hostile, therefore, often overlooks the complexity of modern international relations in an interconnected world, including complex international trade and supply chains. The focus, first and foremost, needs to be on the activity being conducted and the UK's ability to counter it.

In addition, new technologies and their widespread commercial availability has created new opportunities and significant vectors for attack, lowering the cost and risk to states to conduct espionage. Accordingly, while only a small number of states show the full range of capabilities and a willingness to use them, a large number of countries have both the capability and intent to conduct hostile activity against the UK, in some form.

There are a number of current and future trends that impact on both the threat and our response:

COVID 19 – The Government assessment is that while there have been a number of changes to the nature of the threat as a result of COVID 19 (for example a reduction in physical threat but an increase in the cyber threat) the overall level of risk has not

[6] https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf
[7] Update to the IP Commission Report-The theft of American Intellectual Property: Reassessments of the Challenge and United States Policy, National Bureau of Asian Research 2017
[8] National Counterintelligence Strategy of the United States of America 2020- 2022

changed significantly. However, interconnected societies are particularly vulnerable to the threat of global pandemics and the economic downturn and volatility caused by COVID has increased the risk of hostile foreign investment in UK business, and has reiterated the importance of protecting certain sectors, such as medical research. Increased home working has also increased the risks of espionage against Government and businesses alike.

Data – Technological innovation has transformed our lives, changing the way we live, work and play. At the same time, this innovation has brought with it an exponential growth in data: in its generation and use, and in the world's increasing reliance upon it. The significant amount of government, business, academic research and citizens' data stored online can be an invaluable resource but also poses risks. While the UK Government and its agencies use data to detect national security threats and keep citizens safe, the increasingly international nature of data collection, storage and transfer can present data security risks. In addition, foreign states can use the information to seek to conduct hostile activity against the UK, including by using the data to target individuals or entities in the UK, or gain information to be used as leverage.

Disinformation and information operations – increasingly, these have become core tools for state and non-state actors alike to sow discord, attempt to interfere in UK democracy, and disrupt the fabric of UK society through division and polarisation. This has become an evolving threat due to the fast and wide nature in which information can spread online, and the increased speed at which actors can produce and legitimise damaging narratives

Scope and objectives of the legislation

As set out in detail at Annex A, there is a significant volume of work ongoing within Government to counter state threats. This includes the Defending Democracy Programme which is a cross-Government initiative taking forward a co-ordinated programme of work to maintain the integrity of our democracy and electoral processes.

However, through its work, and taking into account the relevant independent reviews in this area, the Government has concluded that there is a compelling case for new legislation to address the threat. It is the Government's ambition to now create a modern and comprehensive legislative framework similar to that which has developed for counter terrorism (CT).

The Terrorism Act 2000 repealed previous CT legislation to become a modern baseline of tools and powers to counter terrorism. As the terrorism threat has evolved in the years since, and as legal standards and case law have developed, the legislative framework has, in turn, been updated and amended. However, the Terrorism Act 2000 remains to this day the centre of the UK's legislative CT response.

It is the Government's intention that this legislation will perform a similar role to TACT 2000, replacing outdated law and, sitting alongside modern tools such as the port examination power in Schedule 3 to the Counter-Terrorism and Security Act 2019 and the National Security and Investment Act, providing a new modern baseline of tools and powers. While our ambition is for the legislation to be comprehensive and future proofed, we also recognise that as the threat evolves, the legislation may need to be updated, amended or complemented with new tools and powers. This would mirror the approach taken on CT over the past 20 years.

Further to an assessment of existing national security legislation and following the Law Commission's findings, the Government is also clear on the importance of ensuring certain official information is protected adequately. As set out above, significant technological advances continue to transform the ways in which information and data can be stored and shared worldwide, as well as the ways in which hostile activity can be conducted for, or on behalf of, states; all factors which existing legislation does not reflect.

The legislative proposals being developed by the Government will therefore include, at a minimum:

- Reform of the Official Secrets Acts 1911, 1920 and 1939 – these Acts contain the core espionage offences which, as set out in more detail further through this consultation, have failed to keep pace with the threat and modern legal standards;
- Reform of the Official Secrets Act 1989 – which governs the law around the unauthorised disclosure of official material and its onward disclosure; and
- The creation of a Foreign Influence Registration Scheme – an important new tool to help combat espionage, interference, and to protect research in sensitive subject areas, as well as to provide a greater awareness of foreign influence currently being exerted in the UK.

We are also considering whether there is the case for new tools and powers to criminalise other harmful activity conducted by, and on behalf of states.

At their core these legislative proposals seek to do 3 things:

- Modernise existing counter espionage laws to reflect the modern threat and modern legislative standards;
- Create new offences, tools and powers to detect, deter and disrupt hostile activity in and targeted at the UK
- Improve our ability to protect official data and ensure the associated offences reflect the greater ease at which significant harm can be done.

The tools and powers proposed in this consultation will make the UK a more challenging environment for states to conduct hostile activity in and increase the cost to them of doing so. It will ensure that the police and security services have the powers they need to keep the country safe, disrupt hostile activity and punish those who conduct hostile acts against the UK.

It is important to note that the tools and powers proposed here alone do not seek to address every aspect of the threat set out above rather, they will form part of the existing and developing legislative and non-legislative toolkit for countering the threat. Further detail on other tools and measures can be found in Annex A.

At the same time, measures adopted must respect the human rights framework; recognising, in particular, the need to protect privacy, press freedoms and freedom of expression, which are the core foundations on which our democracy and society are built. We consider it important to make clear, at this early stage, that ensuring the right balance is struck between this and adopting measures which adequately protect the UK from state threats will remain a priority as we develop this new legislation.

When considering the objectives for the legislation, it is important to note that in a large number of cases, hostile activity will be carried out through highly sophisticated covert means and is intended to steal some of the UK's most sensitive information. These factors combine to pose inherent challenges in prosecuting those seeking to carry out hostile activity, and while the reforms proposed in this consultation will enhance our ability to detect, deter, disrupt and prosecute those acting against the UK and its interests, it is important to acknowledge that some of these challenges will inevitably remain.

Purpose of this consultation

This consultation sets out the Government's proposals and seeks input to inform the final policy and legislative proposals to counter state threats. Responses will help shape those tools and powers to ensure they are comprehensive, effective, workable and balance the protection of national security with the important rights and values we all enjoy in the UK.

The policy proposals in this consultation are split into 3 sections as follows:

Reform of the Official Secrets Acts

This part of the consultation responds to the Law Commission's Review of the Protection of Official Data, highlighting where the Government agrees with their recommendations, as well as highlighting those we intend to consider further and seek input on. In the main body of this consultation, the Government is seeking further input in relation to a number of these recommendations, to inform final policy development. The Government's response to all of the recommendations made by the Law Commission in their Review can be found at Annex B. These proposals, and in particular those which relate to reform of the Official Secrets Act 1989, will be of interest to legal, media, civil liberties and employment rights groups.

In this part of the consultation, the Government also considers the case for potential new offences, including whether, in addition to reform of the core espionage offences in the Official Secrets Acts 1911-1939, there is a case for new standalone offences to cover hostile activity including; sabotage, economic espionage and foreign interference. We particularly welcome views from legal groups and businesses on these proposals.

As part of its proposals, the Government considers there is also a strong case for aggravating sentences in cases where other forms of criminality have been committed, during the process of an actor conducting hostile activity on the behalf of a state.

Foreign Influence Registration Scheme

Having reflected on the value and lessons of the legislation of some international partners, and on the conclusions and recommendations set out by the Intelligence and Security Committee (ISC) in its recent 'Russia Report', the consultation includes an outline proposal for a UK Foreign Influence Registration Scheme. In essence, the creation of a government-managed register of declared activities that are undertaken for, or on behalf of, a foreign state. We intend to engage directly with these individuals, organisations and sectors most likely to be in scope of the scheme as part of the consultation process as we seek to ensure the scheme delivers the most value for them, is practical and accessible, and protects their interests.

Civil Orders

In recognition of the fact that there may be cases where it is not possible to prosecute or otherwise disrupt individuals considered to be involved in hostile activity on the behalf of states, the Government is also considering the case for inclusion of a power of last resort that would enable it to impose a range of restrictions on particular individuals. These proposals will be of particular interest to legal and citizens' rights groups.

In addition to the legislative proposals to counter state threats, this consultation seeks input on any other additional tools and measures that consultees consider could be useful to counter the threats.

Consultation Proposal – Official Secrets Acts Reform

The Official Secrets Acts

The Official Secrets Acts 1911[9],1920[10] & 1939[11] are the core pieces of legislation providing criminal offences to protect the UK from espionage and hostile activity by states. **The Official Secrets Act 1989[12]** is supporting legislation, which constitutes the core legal framework to protect specific categories of sensitive official information, by making its unauthorised disclosure a criminal offence.

What does each Act cover?

The Official Secrets Act 1911 was enacted to strengthen and repeal existing provisions in the first Official Secrets Act of 1889. The 1911 Act created criminal offences for two different types of espionage, described by the Law Commission as 'espionage by trespass/proximity' and 'espionage by information gathering and communication'. It also contains a series of broader measures related to spying and sabotage.[13]

The Official Secrets Act 1920 improved and amended existing provisions in the Official Secrets Act 1911, to reflect more modernised methods of spying and introduced a number of new offences, including making several wartime provisions permanent.

The Official Secrets Act 1939 was enacted to create a legal duty for individuals to provide information on the commission of espionage offences under the 1911 Act.

The Official Secrets Act 1989 creates criminal offences for the unauthorised disclosure of sensitive official information in six categories by; former and existing Crown servants, government contractors, members of the security and intelligence agencies, and those notified that they are subject to provisions under section 1 of the Act, and members of the public more generally. The categories of protected information include; information relating to security and intelligence, defence and international relations, amongst others. This Act, unlike the 1911-39 Acts, was not introduced to directly tackle espionage or other state threats, but rather, to prevent the compromise of official data from harming the UK or its citizens.

How many prosecutions are there under the Acts?

While there has been a recent successful prosecution,[14] the Official Secrets Acts, (particularly in the case of the 1911-39 Acts) are not commonly used to bring prosecutions. This is primarily due to the sensitive nature of the evidence that would typically be required to be disclosed in order to bring prosecutions, but also because of the age of the legislation, which means many of the offences are not designed for the modern world. Prosecutions as a result are challenging and rare.

9 https://www.legislation.gov.uk/ukpga/Geo5/1-2/28
10 https://www.legislation.gov.uk/ukpga/Geo5/10-11/75
11 https://www.legislation.gov.uk/ukpga/Geo6/2-3/121
12 https://www.legislation.gov.uk/ukpga/1989/6
13 https://commonslibrary.parliament.uk/research-briefings/cbp-7422/
14 http://news.met.police.uk/news/man-convicted-of-offences-under-the-official-secrets-act-414654

Why reform the Official Secrets Acts?

As noted above, the scale and potential impact of espionage and unauthorised disclosures has changed significantly since the Official Secrets Acts 1911-89 first became law. The Government is of the view that the existing legislation does not sufficiently capture the discernible and very real threat posed by state threats and therefore, reform of all of the Official Secrets Acts is central to the UK's ability to tackle it.

Reform of the Official Secrets Act 1989 is essential to strengthen the UK's ability to tackle hostile activity by states, by ensuring official information (which can significantly harm the nation and its citizens if it falls into the wrong hands) is better protected, by legislation that enables offenders to be prosecuted and punished appropriately.

The Law Commission's Review on the Protection of Official Data - September 2020

In 2015, the Cabinet Office and the Ministry of Justice commissioned the Law Commission to examine the Official Secrets Acts as part of a wider review of the Protection of Official Data[15]. The genesis of this Review was prompted by increased concern over the impact of unauthorised disclosures of official information, and the speed and scale of global communications enabled by the internet. The Cabinet Office Minister at the time, when inviting the Law Commission to conduct its Review of the criminal law provisions that protect official information, reaffirmed the Government's commitment to transparency, and expressed the need for clearer boundaries so that those responsible for handling official information know what is expected of them, and what the consequences are, if official information is disclosed without authorisation.

During their Review, the Law Commission consulted widely on potential legislative proposals. The Government engaged with the Law Commission during their consultation process in 2017, as did a wide number of interested parties, including; media and legal organisations, academics, non-governmental organisations, and individual members of the public.

The Commission's final Review was published on 1 September 2020. The Government would like to thank the Law Commission for the hard work, time and effort spent on developing the Review and we encourage people to read their extensive report, for in depth and expert analysis.

The Government's response

The Law Commission's Review makes a number of recommendations for reform of the Official Secrets Acts, both legislative and non-legislative. In the following section, the Government responds to several core recommendations on legislative reform, where we seek further input. Our full response to all recommendations can be found in Annex B. Given the wide range of strong views expressed at the time, we are particularly interested in hearing from those who contributed to the Law

[15] https://www.lawcom.gov.uk/project/protection-of-official-data/

Commission's consultation and may have further views on their final recommendations, or the Government's views in this document.

Reform of the Official Secrets Acts 1911-1939

This section focuses on the Law Commission's recommendations relating to the core espionage offences in the Official Secrets Acts 1911-39.

Acts Preparatory to Espionage

The Law Commission, in recommendation 9 of their Review, propose that the offence of doing an act preparatory to espionage should be retained.

We welcome this recommendation. It is important that law enforcement can arrest those looking to conduct espionage at a preparatory stage, as this is the best means of ensuring that sensitive information remains secure. We are also considering the case for broadening the offence to apply to acts preparatory to other types of hostile activity by states, outside of espionage, such as sabotage or foreign interference. By maintaining and broadening an offence of this type, we would seek to criminalise relevant acts carried out in the lead up to hostile activity, which would enable the police to intervene at an early stage before these preparatory acts can culminate into serious harm.

Questions to consultees:

1) Do you think an acts preparatory to hostile activity by states offence could be a valuable addition to modern criminal law, in light of the threat?

2) Do you have any comments about how an offence of this nature could work in practice?

The territorial ambit of Official Secrets Acts 1911-39 offences

In recommendation 10 of their Review, the Law Commission propose that the territorial ambit of offences in the Official Secrets Acts 1911-39 be expanded so they can be committed irrespective of the offending individual's nationality. The Commission goes further to suggest a 'significant link' model, between the individual's behaviour and the interests of the United Kingdom, which is not limited by reference to the nationality or official role of the individual involved. The Commission suggest "significant link" should be defined to include not only the case where the defendant is a Crown employee or contractor, but also the case where the conduct relates to a site or data owned or controlled by the UK Government (irrespective of the nationality of the defendant).

We broadly welcome the recommendation that the territorial scope of offences under the 1911-39 Acts be updated and agree that the current legal position, which only applies to British citizens or subjects abroad, is insufficient to protect British assets at home and elsewhere. The nature of the threat and HMG's global footprint, as well as the movement of individuals around the world and developments in cyber technology, has changed the way espionage is carried out. Therefore, the Government agrees that the territorial application of espionage offences should be expanded, so they can be committed irrespective of the offending individual's nationality or location and applies when the UK's interests are damaged by espionage, or UK assets, sites or information are subject to espionage.

The Government is considering whether the 'significant link' model (as seen in other UK legislation) is the correct model to cover espionage against assets in the UK from overseas, or upon a UK site or information based overseas.

Questions to consultees:

3) Do you think there would be merit in considering a 'significant link' formula, as described above, to bring into scope espionage against assets in the UK from overseas? How do you think this could work in practice?

4) Is there anything that you consider this model would miss that ought to be captured?

Reform of the Official Secrets Act 1989

This section focusses on the Law Commission's recommendations relating to provisions which criminalise individuals for disclosing official information without authorisation, under the Official Secrets Act 1989. The 1989 Act contains a number of different offences that apply to the disclosure of certain categories of information, including; information relating to security and intelligence, defence and international relations.

The offences in sections 1 to 4 of the Act can only be committed by Crown servants (including members of the security and intelligence agencies), government contractors, or those notified under section 1 that they are subject to its provisions. Offences committed in these sections are often referred to as primary disclosures. The offences in sections 5 and 6 can be committed by anyone and cover disclosures by those who do not have access to the primary source of the material, but disclose or publish it further, once it has been shared with them by a primary discloser, without authorisation or in confidence. Offences committed in these sections are often referred to as 'onward' disclosures.

The Government recognises that the Law Commission considered and presented their recommendations on the Official Secrets Act 1989 as a package of proposed reforms. For the purposes of this response, we have considered the merits of each recommendation individually. We are, however, conscious of the interaction between the recommendations and will consider this further, when developing proposals for reforming the 1989 Act, taking into account responses to this consultation.

The requirement to prove damage

In recommendation 11 of their Review, the Law Commission suggest that the unauthorised disclosure offences in sections 1 to 4 of the Act – applicable only to former or existing Crown servants, government contractors or those notified – should no longer require proof or likelihood of damage. Instead, they suggest the introduction of an explicit subjective fault element that could be modelled around whether the defendant knew, believed, or was reckless as to whether the disclosure would, was likely to, risked causing, or was capable of causing damage. The Commission also recommend that offences in sections 5 and 6 of the Act should continue to be based on proof or likelihood of damage.

In addition, in recommendation 12, the Commission propose that the unauthorised disclosure offence in section 1(1) of the Act – concerning individuals notified that they are subject to its provisions (most commonly Crown servants and contractors) should not be amended to require proof that disclosures were damaging. They also propose that the defence in section 1(5) of an individual not knowing and having no reasonable grounds to believe that the material disclosed related to security or intelligence, should continue to apply.

The Government welcomes the Commission's recommendations that offences in sections 1 to 4 of the Act - relating to Crown servants, government contractors and those notified - should no longer require the prosecution to evidence proof or likelihood of damage, and that offences contrary to section 1(1) of the Official Secrets Act 1989 should not be amended to require proof of damage. We agree with the Commission that this requirement is wrong in principle and creates real practical issues, acting as a barrier to potential prosecutions. In practice, proving damage in an open judicial system would likely require the disclosure of additional confidential information, which in turn could cause further material damage, meaning there is often a reluctance to pursue prosecutions. We note, however, that whilst the removal of the damage requirement would, for this reason, remove one barrier to the prosecution of offences in sections 1 to 4 of the Act, existing challenges surrounding the requirement to disclose (often highly sensitive) information as evidence, through usual criminal disclosure in open court, would still remain. We will consider the merits of this recommendation further when developing legislation.

We also accept the recommendation that the 'defence' of not knowing or having reasonable grounds to believe that material disclosed related to security or intelligence (and thus in scope of section 1(1)), should continue to apply.

In addition, the Government notes the additional recommendations that for sections 1 to 4, there should be an explicit, subjective fault element and that the offences in sections 5 and 6 should continue to include the requirement to evidence proof or likelihood of damage. We will explore both of these suggestions further, but we do consider that both primary and onward disclosures have the potential to cause equal amounts of harm.

Questions for consultees:

5) Do you agree with the Law Commission's proposals with regards to introducing a subjective fault element, as part of offences in sections 1 to 4 of the existing Act, instead of a damage requirement?

6) Do you agree that the requirement to prove damage should remain for offences under sections 5 and 6 of the existing Act? If so, why?

Sentencing for unauthorised disclosure offences

The Law Commission, in recommendation 14 of their Review, suggest that a maximum sentence of two years' imprisonment does not provide the court with adequate powers in really serious cases of unauthorised disclosure, and that Parliament should consider increased maximum sentences for some offences under the 1989 Act. The Commission also recommend that consideration be given to whether a distinction should be drawn in sentencing, between the offences in sections 1 to 4 and 5 and 6 of the Act.

The Government welcomes the recommendation that a maximum sentence of two years does not provide the court with adequate powers in the most serious cases of unauthorised disclosure. Since the passage of the Act in 1989, there have been unprecedented developments in communications technology (including data storage and rapid data transfer tools) which in our view, means that unauthorised disclosures are now capable of causing far more serious damage than would have been possible previously.

As a result, we do not consider that there is necessarily a distinction in severity between espionage and the most serious unauthorised disclosures, in the same way that there was in 1989. Although there are differences in the mechanics of and motivations behind espionage and unauthorised disclosure offences, there are cases where an unauthorised disclosure may be as or more serious, in terms of intent and/or damage. For example, documents made available online can now be accessed and utilised by a wide range of hostile actors simultaneously, whereas espionage will often only be to the benefit of a single state or actor. In severe cases, the unauthorised disclosure of the identities of agents working for the UK intelligence community, for example, could directly lead to imminent and serious threat to life. In addition, the unauthorised disclosure of information could also provide multiple hostile actors with critical information relating to core UK defence capabilities, for example, which could ultimately render these capabilities ineffective as a result.

Questions for consultees:

7) Do you agree that maximum sentences for some offences under the Official Secrets Act 1989 should be increased?

8) Do you think there should be a distinction in sentencing between primary disclosure offences - committed by members of the security and intelligence agencies, Crown servants, government contractors and those notified - and onward disclosure offences - which can be committed by members of the public?

The vetting of lawyers to protect official information

The Law Commission provide a package of recommendations in their Review, relating to the vetting and security practices of lawyers dealing with official information, in recommendations 15-17.

In recommendation 15, the Commission suggests that professional bodies responsible for the Codes of Conduct for practising lawyers – the Solicitors Regulation Authority and Bar Standards Board – consider including explicit guidance on the importance of maintaining confidentiality in cases involving the Official Secrets Acts, and the obligation not to receive disclosures unless they have the appropriate security clearance and premises assurance for practising lawyers.

In addition, recommendation 16 proposes that - where an individual who is not 'notified' that they are subject to section 1(1) provisions (and is not a subject of a relevant criminal investigation) makes a disclosure to a qualified lawyer for the purpose of obtaining legal advice - that disclosure should constitute an authorised disclosure, subject to specific safeguards being met. The safeguards the Commission propose are; (i). the legal adviser must be subject to professional obligations, either through the Bar Standards Board or the Solicitors Regulation Authority; and (ii) the lawyer to whom the disclosure is made must have undergone security vetting to the appropriate level and systems/premises assurance.

The Commission also propose, in recommendation 17, that where a Crown servant, government contractor or notified person is a suspect in a criminal investigation, and makes a disclosure to a qualified legal adviser for the purposes of legal advice, that disclosure should be authorised for the purposes of sections 1 to 4 of the Official Secrets Act 1989, if the legal adviser has security clearance to the appropriate level and has undergone systems/premises assurance.

The Government welcomes the Law Commission's package of recommendations in relation to security and vetting requirements upon lawyers. Access to legal representation is a core part of the UK legal system and we fully support all attempts to ensure access, when seeking advice in this complex and sensitive area. However, such access must be balanced with the requirement to safeguard sensitive official material, the release of which could cause a threat to life, and/or significant damage to national security. We will consider options when developing legislation, which balance these requirements with the importance of people being able to seek independent legal advice and will draw on the views advanced in the Review accordingly.

Questions for consultees:

9) Do you agree with the Law Commission's proposed recommendations on how sensitive official material could be better protected during the process of obtaining legal advice?

10) Do you have any other suggestions on how it can be assured that sensitive official information is adequately protected during the process of obtaining legal advice?

Categories of information protected under the Act

In recommendations 19 and 20 of their Review, the Law Commission propose that the categories of information currently protected in the 1989 Act should not be narrowed, and that if reform of the Act is undertaken, the possibility of defining the categories of information with greater precision ought to be explored as a priority. They also recommend that the categories of information should not be expanded to include economic information in so far as it relates to national security.

As part of legislative reform, we will consider whether to amend the categories of information protected[16], to reflect technological and national security developments since the legislation was enacted, and to ensure new legislation is futureproofed.

Questions for consultees:

11) Do you have a view on whether the categories of protected information should be reformed?

12) In your view, is there a type of sensitive official information that is not currently protected by the existing Act, but should be in reformed legislation?

The territorial ambit of Official Secrets Act 1989 offences

In recommendation 21 of their Review, the Law Commission propose that the territorial ambit of offences in sections 1 to 4 of the 1989 Act should be amended, so that a government contractor or notified person commits an offence when he or she makes an unauthorised disclosure abroad, irrespective of whether he or she is a British citizen.

The Government agrees that there is a need to change the territorial extent of the offences in the 1989 Act and we will consider adopting a version of the formulation proposed by the Commission, as part of legislative reform. We will also consider

[16] The categories of information protected by the Official Secrets Act 1989 include; Security and Intelligence; Defence; International Relations; Crime and Special Investigation Powers; and Security, Intelligence, Defence or International Relations information communicated in confidence to another State or international organisation.

whether the territorial scope for the offences under sections 5 and 6 (onward disclosures by a third party) should be extended, to bring into scope British citizens and those with a right to remain in the UK, when overseas.

The serious threat posed to UK interests by those who commit damaging unauthorised disclosures exists not solely in the case of British citizens, but also in the case of those who benefit from resident and settled status. We note that the Review is not explicit on whether this should also apply to formerly notified persons, government contractors and Crown servants, which is something we would also seek to consider, in more detail.

In addition, the 1989 Act offences exclude the prosecution of other individuals overseas, even in cases where the individual would have known (or indeed intended) for the disclosure to cause damage. There may be circumstances in which the Crown should be able to consider prosecution against non-British citizens for unauthorised disclosure, who have caused damage through their disclosure, which we will consider further.

Questions for consultees:

13) Do you think the extraterritorial ambit of offences in sections 1 to 4 should apply to formerly notified persons, Crown servants and contractors, as well as those currently employed?

14) Do you think the extraterritorial ambit of offences in sections 5 and 6 should be extended to bring into scope British citizens, residents and those with settled status (including those located overseas) when committed abroad?

15) Do you think there is a case for extending the extraterritorial ambit of offences in sections 5 and 6 to all, regardless of nationality?

Disclosure of information in the "public interest"

The Law Commission's final recommendations relate to disclosures of information potentially in the "public interest".

In recommendation 32 of their Review, the Commission propose that an independent, Statutory Commissioner should be established with the purpose of receiving and investigating allegations of wrongdoing or criminality, where otherwise the disclosure of those concerns would constitute an offence under the Official Secrets Act 1989.

They propose that such a Commissioner would have to constitute an effective investigative mechanism and therefore have to not only be independent, but also be able to act expeditiously, and have the legal authority to compel cooperation with its investigations. The Commission also recommends that there should be a right of appeal by the complainant against decisions of the Statutory Commissioner and that the jurisdiction of the Investigatory Powers

Tribunal should be expanded, such that it can hear appeals against decisions of the Statutory Commissioner.

To support this function, the Commission also recommend the introduction of a Public Interest Defence, outlining in recommendation 33 of their Review that; a person should not be guilty of an offence under the Official Secrets Act 1989 if that person proves, on the balance of probabilities, that: (a) it was in the public interest for the information disclosed to be known by the recipient; and (b) the manner of the disclosure was in the public interest.

We note these recommendations and will consider in further detail proposals relating to a Statutory Commissioner and a Public Interest Defence. As part of these considerations, we will also reflect on the Commission's comments regarding the compatibility of the Act with Article 10 of the European Convention on Human Rights – the right to freedom of expression. From our initial considerations, the Government believes that existing offences are compatible with Article 10 and that these proposals could in fact undermine our efforts to prevent damaging unauthorised disclosures, which would not be in the public interest.

Safeguards already exist (including existing processes for Government whistleblowers) which allow them to raise concerns without needing to undertake an unauthorised disclosure. These processes include; the possibility of raising a concern inside their own organisation, with the Cabinet Office, the Civil Service Commission, and even the chair of the Intelligence and Security Committee of Parliament. For former and current members of the security and intelligence agencies, there are additional offices to which disclosures can be made, creating a further set of safeguards for that group. Any decision to prosecute will be subject to the public interest test by the Crown Prosecution Service, and in most cases, requires the consent of the Attorney General to prosecute. The efficacy of existing mechanisms and safeguards across Government is key to the operation of these offences, and the Government will review their operation, in order to assess the Commission's recommendations for a Statutory Commissioner, when exploring options for Official Secrets Act 1989 reform.

Press freedom is an integral part of the UK's democratic processes, as is the ability for individuals to whistleblow and hold organisations to account, when there are serious allegations of wrongdoing. However, a balance must be struck with safeguarding official information (including national security information), where its compromise could harm the UK, its citizens or interests, given the unlawful disclosure and/or subsequent publishing of sensitive documents can lead to serious harm in many cases. We are not convinced that the Law Commission's recommendations strike the right balance in this area.

Our fundamental concern is that a person seeking to make an unauthorised disclosure, whether in Government or otherwise in possession of official material, will rarely (if ever) be able to accurately judge whether the public interest in disclosing the information outweighs the risks against disclosure. Even if the case is subsequently made that the disclosure was not in the public interest, and the person who published the information has committed a criminal offence, this does not undo the potential damage caused by the disclosure.

Questions for consultees:

16) Do you support the potential creation of a Statutory Commissioner to support whistleblowing processes? If so, why?

17) Do you have any evidence for why existing government whistleblowing processes would necessitate the creation of a Statutory Commissioner?

18) Do you have a view on whether a Public Interest Defence should be a necessary part of future legislation?

Summary of questions for consultees on Official Secrets Acts reform

Official Secrets Acts 1911-39 reform

1. Do you think an acts preparatory to hostile activity by states offence could be a valuable addition to modern criminal law, in light of the threat?
2. Do you have any comments about how an offence of this nature could work in practice?
3. Do you think there would be merit in considering a ‘significant link’ formula to bring into scope espionage against assets in the UK from overseas? How do you think this could work in practice?
4. Is there anything that you consider this model would miss that ought to be captured?

Official Secrets Act 1989 reform

5. Do you agree with the Law Commission’s proposals with regards to introducing a subjective fault element, as part of offences in sections 1 to 4 of the existing Act, instead of a damage requirement?
6. Do you agree that the requirement to prove damage should remain for offences under sections 5 and 6 of the existing Act? If so, why?
7. Do you agree that maximum sentences for some offences under the Official Secrets Act 1989 should be increased?
8. Do you think there should be a distinction in sentencing between primary disclosure offences - committed by members of the security and intelligence agencies, Crown servants, government contractors and those notified - and onward disclosure offences - which can be committed by members of the public?
9. Do you agree with the Law Commission’s proposed recommendations on how sensitive official material could be better protected during the process of obtaining legal advice?
10. Do you have any other suggestions on how it can be assured that sensitive official information is adequately protected during the process of obtaining legal advice?
11. Do you have a view on whether the categories of protected information should be reformed?
12. In your view, is there a type of sensitive official information that is not currently protected by the existing Act, but should be in reformed legislation?
13. Do you think the extraterritorial ambit of offences in sections 1 to 4 should apply to formerly notified persons, Crown servants and contractors, as well as those currently employed?
14. Do you think the extraterritorial ambit of offences in sections 5 and 6 should be extended to bring into scope British citizens, residents and those with settled status (including those located overseas) when committed abroad?
15. Do you think there is a case for extending the extraterritorial ambit of offences in sections 5 and 6 to all, regardless of nationality?

16. Do you support the potential creation of a Statutory Commissioner to support whistleblowing processes? If so, why?
17. Do you have any evidence for why existing government whistleblowing processes would necessitate the creation of a Statutory Commissioner?
18. Do you have a view on whether a Public Interest Defence should be a necessary part of future legislation?
19. Do you have any views or evidence you'd like to provide on any of the other final Law Commission recommendations, or the Government's response, in Annex B?

Strengthening Official Secrets Acts reform to tackle the threat of hostile activity by states

Separate to the Law Commission's recommendations, we are considering whether there is justification to create additional offences and provisions as part of Official Secrets Acts 1911-1939 reform, to tackle state threats.

Economic espionage, sabotage and foreign interference

We are conscious that there may be a need to address additional harms relating to hostile activity by states, which may not be captured by Official Secrets Acts reform alone.

These harms include:

- **Sabotage -** which incorporates a number of potential activities that are carried out to; destroy, damage, modify or obstruct critical infrastructure, functions or organisations, for political or military advantage.
- **Economic espionage -** or activity by states to enable the theft of trade secrets; and
- **Foreign interference –** which, as noted in the introduction, covers a wide range of activity through which states seek to further their aims by use of covert means, or by obfuscation of intent and originator, including; disinformation, bribery and coercion.

We consider that some of these harms are already captured, to an extent, by existing Official Secrets Acts offences or will be through reform. For instance; espionage-related offences under the 1911 Act may already cover the theft of trade secrets, or trespass by a hostile actor entering a prohibited place to commit sabotage. Foreign interference activity may also already be captured by the Official Secrets Acts in the form of hacking and the disclosure of stolen information.

In addition, some of this activity and resulting harms may also be addressed by other offences in the statute book, particularly with regards to acts of sabotage, which may already be captured by a plethora of common law offences, such as; criminal damage, computer misuse and theft. Other, more general offences, may also be committed in the course of carrying out economic espionage, including; misconduct in public office (if committed by a public office holder), conspiracy to defraud, and offences under the Computer Misuse Act 1990, Fraud Act 2006, or Bribery Act 2010, amongst others.

As we develop legislative proposals, we will consider whether there is a requirement to create standalone offences for sabotage, economic espionage and foreign interference, to specifically address these harms, subject to whether they are sufficiently covered by; Official Secrets Acts reform, a new Foreign Influence Registration Scheme, and other relevant legislation.

Questions for consultees:

20) Are there any harms which fall under these broad headings (sabotage, economic espionage, and foreign interference) that are not currently captured in existing legislation?

21) Do you think that there is a case for standalone offences for sabotage, economic espionage, and foreign interference?

Search warrants under the Official Secrets Act 1911

Under section 9 of the Official Secrets Act 1911, a court can authorise a search warrant to the police where there are reasonable grounds for suspecting that an offence under the Act has been, or is about to be, committed. The warrant will allow the police to; enter and search any place named in the warrant, and to search every person found therein, and to seize any relevant material. Where there is "great emergency" for which immediate action is required, a Superintendent may authorise a warrant.[17]

Other search powers provided under the Police and Criminal Evidence Act 1984 (PACE), have not been found to adequately provide the police in England and Wales with the swift preventative powers they require to address the espionage threat. This is because:

- PACE requires reasonable grounds for "believing" that an indictable offence *has* been committed. The Official Secrets Acts allow for searches where there are reasonable grounds for "suspecting" that an offence is, *or is about to be*, committed;
- PACE powers alone do not allow for a search for excluded or special procedure material, when an offence is not yet believed to have been committed, without a provision in another Act to allow for this; and
- PACE alone does not allow for search warrants to be issued by a superintendent in urgent cases.

As noted above, hostile activity by states pose significant challenges, owing to capable and well-resourced actors, who use covert methods. Accordingly, it may often not be possible to produce the necessary evidence to meet the requirements for obtaining a search warrant under PACE. Further, excluded material under PACE (such as personal records related to a suspect's occupation, for instance) is often particularly relevant in Official Secrets Acts investigations, where such material may form the central evidence in an offence. The additional power to search for this in Official Secrets Acts cases is crucial to the effectiveness of investigations.

The existing section 9 search power therefore enables the police to effectively respond to the threat and disrupt, investigate and obtain evidence of hostile activity by states, when required. This comes with the safeguard of the Court needing to be

[17] https://www.legislation.gov.uk/ukpga/Geo5/1-2/28/section/9

persuaded in each case to issue a warrant. Accordingly, we seek to carry over the section 9 provision into reformed legislation. In addition, we will also consider whether there is a need for other enhanced investigative tools to support the new offences and powers in the legislation.

Questions for consultees:

22) Do you have any concerns about the continuation of this power? If so, what kind of mitigating actions could be put in place to address these concerns?

Hostile activity by states as an aggravating factor in sentencing

The Government intends to make a connection to hostile activity by states an aggravating factor in sentencing.

Aggravating factors are used during sentencing to increase the seriousness of an offence and assist the court in deciding the most appropriate sentence for an offender. When determining a sentence, the court considers both aggravating factors that make the offence more serious, and factors which may reduce seriousness, or reflect personal mitigation. It is for the court to independently determine how much weight should be assigned to any aggravating or mitigating factors and increase or reduce a sentence accordingly.

Aggravating factors enable the courts to recognise wider conduct that may support increased criminal penalties. For example, individuals committing offences of theft or property damage may also be committing hostile activity on behalf of a state, when committing those offences.

The measure would mean that if a hostile actor is prosecuted and found guilty of an offence outside of our proposed legislation, but a connection to hostile activity by states can be proven, the court must take into account this connection when determining the offender’s penalty. We consider that such an aggravating factor should apply to all offences in UK legislation, outside of this legislation, to accommodate the broad and evolving threat, which is likely to change and advance rapidly over the coming years. Reflecting this threat in UK criminal law in this way will additionally send a strong message to other states that the UK will not tolerate hostile activity by states.

Consultation Proposal – Foreign Influence Registration (FIR) scheme

Introduction

As set out at the beginning of this consultation document, the UK faces a range of state threats. The Government has proposed a comprehensive package of measures to strengthen existing legislation to disrupt, deter and prevent such activity. We consider that an important part of this package, and one of the key tools in delivering on those objectives, would be a Foreign Influence Registration (FIR) scheme – the creation of a government-managed register of declared activities that are undertaken for, or on behalf of, a foreign state. Having reflected on the value and lessons of similar schemes in the United States[18] and Australia[19], and on the conclusions and recommendations set out by the Intelligence and Security Committee (ISC) in its recent 'Russia Report'[20], this section outlines why a UK scheme could make an important contribution to mitigating the threats from states.

Principles of this consultation proposal

This consultation seeks your input to help develop the design of the FIR scheme and, in particular, **to ensure its requirements are proportionate, clear and practical.** The proposal that follows provides an overview of the specific threats to the UK that this scheme could help to address. It considers how a UK scheme could be constructed to maximise its utility against the threat, and to the extent possible, mitigate any unintended consequences from it. We anticipate that there will be individuals, organisations and sectors that are more likely to be impacted by the scheme's requirements due to their exposure to threats that are of most concern (see 'which threats could the Foreign Influence Registration scheme help to address?' below). We intend to engage directly with these individuals, organisations and sectors as part of the consultation process. We seek to ensure the scheme delivers the most value for them, is practical and accessible, and protects their interests. We do, however, welcome input from all other interested respondents.

It is important to be clear that the Government does not intend for this scheme to create any barriers or deterrence to those acting for, or on behalf of, a foreign state, to engage in legitimate activities in the UK. The Government also does not intend for this scheme to halt or obstruct collaboration. The UK prides itself on being one of the most open, fair and inclusive societies. It is in this spirit that the Government emphasises that collaboration and engagement within the UK, where open and transparent, will continue to be welcome. The

---

[18] The US Foreign Agent Registration Act (FARA) 1938 - Department of Justice, *'Foreign Agent Registration Act'* (https://www.justice.gov/nsd-fara) and US 18 Code US Section 951 - Department of Justice, *'FARA related statutes'* (https://www.justice.gov/nsd-fara/fara-related-statutes)

[19] Australian Foreign Influence Transparency Scheme Act (FITS) 2018 - The Attorney General's Department. *'Foreign Influence Transparency Scheme'* (https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme)

[20] Intelligence and Security Committee, *'Russia Report'* (July 2020, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFI), p34.

scheme intends to ensure that certain activities undertaken for, or on behalf of, a foreign state are openly declared and not concealed.

In developing the FIR scheme we recognise that the Belfast (Good Friday) Agreement and the unique circumstances of Northern Ireland demand particular care and attention. The Government is clear that the legislation is not intended to interfere with the underlying principles and spirit of the Agreement. It recognises that individuals and political parties legitimately operate in both jurisdictions on the island of Ireland and will develop and implement these proposals in a way that does not interfere with their ability to do so. We would welcome input, as part of the consultation, on how the FIR scheme, or wider legislative proposals can be developed in accordance with that intention.

How could a scheme like this work?

A UK scheme would require individuals in scope of the requirements to register activity within the UK that is being undertaken for, or on behalf of, a foreign state. This could include activities that have been directly commissioned by a foreign state, as well as activities that have been directed by an individual or entity that is subject to foreign state influence or control (referred to in this document as a foreign state-related actor). For any activity that has been registered, the individual would also need to declare the underpinning arrangement with a foreign state or foreign state-related actor. If the individual fails to register or provides false information, they could face enforcement action.

A register of activity undertaken on behalf of a foreign state would provide the Government with an important tool to disrupt hostile activity. An individual would risk committing a criminal offence by not registering or registering false information. The associated penalties for non-compliance would provide an alternative means to prosecute hostile actors. Such a scheme would increase the risk to foreign states seeking to conduct hostile activity and help to build resilience against being unwittingly drawn into interference[21]. Through greater transparency, the scheme would also increase understanding of the level of foreign influence in UK affairs, including Government and areas of national security interest.

The success of state threats against the UK depends on the activity remaining hidden. It also often relies on relationships with individuals in, or working on behalf of, the UK to support and facilitate the activity. A UK scheme would increase the risk to hostile actors that are intent on concealing their activity, as well as those who agree to covertly facilitate such activity.

[21] For the purpose of this consultation (see section on the threat at page 7), 'interference' is understood to cover a wide range of activity through which states seek to further their aims by use of covert means or by obfuscation of intent and originator, including disinformation, bribery and coercion. This also includes attempts to interfere in our democracy or Government policy making, including through interference in national, regional or local elections and referenda, as well as attempts to undermine academic freedoms. A number of states conduct persistent activity which attempts to distort UK and international information environments through the use of information operations, which often play on existing divisions.

Which threats could the Foreign Influence Registration scheme help to address?

The Government considers that a UK scheme might provide a versatile tool that could be used to support efforts to combat espionage, interference, and to protect research in sensitive subject areas that is essential to UK national security and prosperity.

- **Espionage.** Which is the covert seeking of sensitive confidential information across a range of areas by means of human intelligence, signals intelligence, technical intelligence and penetration and disruption of computer networks. The UK Government, industry, academia, defence and business sectors are routinely targeted by foreign states seeking sensitive information.

- **Interference.** Examples of interference have been reported on in multiple contexts, including the targeting of democratic events domestically and overseas through information operations and the distribution of funding (as described in the ISC 'Russia Report').[22]

- **Transfer of data related to research in sensitive subject areas.** The UK enjoys research leadership in many important areas. It is one of the best places to engage in collaborative research. Because of this our research sector is targeted by hostile actors seeking to acquire sensitive information that would be of benefit to foreign states and to the detriment of UK national security and prosperity. They do this by attempting to gain access to the research, or to individuals who work on research in sensitive subject areas and possess relevant expertise and 'know how'.

How could a UK scheme help address these threats?

A UK scheme could help the Government to combat espionage, interference and protect research in sensitive subject areas in the following ways:

- **Enabling disruption of hostile activity by states.** The scheme would impose penalties for non-compliance with the registration requirements (including for not registering an eligible activity or providing false or misleading information). It is anticipated that many of the individuals engaged in hostile activity or interference on behalf of a foreign state would not declare this by registering with the scheme or would register false or misleading information. If they sought to engage in this activity without properly registering, they would be liable to prosecution. If an individual did register their hostile or interference activity with the scheme, they would risk exposing their potentially harmful activities to those with access to the register, which would undermine their objectives and allow protective measures to be taken.

[22] Intelligence and Security Committee, *'Russia Report',* p.9

- **Increasing the risk of conducting hostile activity.** We consider that the requirements and penalties for non-compliance associated with the scheme would also increase the risk to those seeking to engage in hostile or interference activities for, or on behalf of, foreign states. There would be both practical and reputational costs to states in conducting covert interference activity imposed through the threat of, or actual, prosecution for non-registration. It could make individuals think twice before seeking to undertake such activity if there is an increased risk of that activity and its links to foreign states being exposed, or by attracting the attention of the criminal justice system.

- **Building resilience to state threats and increasing transparency.** We also consider that the scheme could help protect individuals from unwittingly being used by foreign states to undertake hostile activity, particularly those who might work in areas likely to be subject to influence such as the UK's political processes. The scheme is intended to encourage individuals to undertake due diligence before entering into a relationship with, or undertaking activity for, another individual or organisation. This would be especially important in areas of national security concern. As an additional benefit, increasing transparency through the information on the register would provide Government decision makers, sensitive sectors in the national security community and, if parts of the register are published (see below), the general public, with a greater awareness of foreign influence currently being exerted in the UK.

What benefits would a UK scheme offer in addition to other Government tools?

The main difference between a UK registration scheme and other government tools, both those available today and those being considered as part of this package of measures, is that a UK scheme would allow for the prosecution of individuals engaged in hostile activity based on a failure to register when conducting certain activities, rather than for committing the hostile act. This offers two main benefits:

- **An alternative means of prosecution**. Traditionally, offences relating to state threats have been difficult to evidence, and therefore prosecute. One of the reasons is that providing evidence of espionage often involves information of the highest sensitivity and can present risks to national security if disclosed in court proceedings. The scheme would provide a means of prosecuting known hostile actors without necessarily having to disclose the most sensitive evidence. For example, by prosecuting for a failure to register under the scheme rather than an espionage offence, the prosecution need only disclose evidence of carrying out a registerable activity for or on behalf of a foreign state or foreign state actor.

- **A means of disrupting hostile activity at an earlier stage**. Most of the tools that the Government has to counter hostile activity are focused on creating offences for harmful activity that has been carried out by hostile actors. This requires an offence and damage to HMG to have been committed, or a provable preparatory act to have taken place, before an individual can be prosecuted. Whilst this can provide some deterrent effect, its utility is limited – it does not provide the Government with options for disrupting harmful activity before damage to the UK has occurred. By requiring an individual to declare their engagement in activity that has been directed by a foreign state or foreign state-related actor, with offences for non-compliance, the scheme could provide a means to intervene at an earlier stage of the activity and before it results in a damaging hostile act.

Should registered activity be visible to wider government and the general public?

The resilience and transparency benefits of the scheme would be amplified if both the Government and the general public have visibility of certain information that has been registered. The Government is therefore considering making certain information about registrants, registerable activities and their relationships to a foreign state or foreign state-related actor, available to the public. Access to information registered with the scheme by those involved in the relevant sectors may also increase the risk to those who continue to conceal their activities. This is because wider accessibility of registered information would likely result in greater scrutiny of who has, and importantly who has not, registered their activity with the scheme. This could be a valuable tool to certain sectors who have a strong incentive to protect their work or the integrity of their functions. A public register would enable those working in the sector to continue to engage in important international collaboration with state linked individuals and organisations with greater confidence.

In considering making certain information publicly accessible, we are also aware that there may be situations in which it would be necessary for information on the register to remain private. For example, where the information would threaten the interests of national security, could put an individual's safety at risk, or is commercially sensitive. In these situations, publication of the individual's name and their activity may not always be appropriate and could even make them an attractive recruitment target for hostile actors. This would run contrary to the purposes of the scheme. This is an area that we would like to explore further through the consultation to determine how a process to evaluate such cases could work in practice.

Questions for consultees:

23) What do you think the implications would be for you, your employer, or your sector in making certain information about registrants, their registerable activity and their registerable links to a foreign state available to the public?

(Very negative – Negative – No impact – Positive – Very positive)

Comments: ______________________________

Who would be required to register their activity?

The aim of this consultation process is to support development of a scheme that will bolster efforts to combat espionage, interference, and to protect research in sensitive subject areas that is essential to UK national security and prosperity. To deliver the benefits described above, the scheme would require the declaration of certain activities that are being undertaken for, or on behalf of, a foreign state. The registration requirements would therefore need to reflect three key considerations: i) activity that is undertaken directly and indirectly for a foreign state; ii) the form of direction given by a foreign state or foreign state-related actor; and iii) the type of activities that are to be registered.

The benefits of the scheme are dependent on the requirements being practical, but also enforceable where non-compliance has been identified. It is the Government's view, therefore, that making registration of an activity the responsibility of the individual, rather than an organisation, is likely to be more effective from a compliance and enforcement perspective.

- **Activity undertaken directly and indirectly for a foreign state.** Hostile activity continues to be commissioned directly by foreign states through their operatives and agents. Such hostile activity can however, also be undertaken on behalf of foreign states by seemingly private or independent actors that are subject to foreign state influence or control (foreign state-related actors). To ensure the scheme is effective against both manifestations of hostile activity, and to avoid creating a loophole that could be exploited, the requirement to register certain activities should not only apply to individuals acting directly for a foreign state, but it should also apply to those acting for the state indirectly through a foreign state-related actor. We welcome views on how these terms should be defined.

- **Direction given by a foreign state or foreign state-related actor.** Another key consideration is what it means to be undertaking an activity 'for, or on behalf of, a foreign state'. It is the Government's view that an individual should not be required to register under the scheme simply because they have a link to a foreign state or foreign state-related actor. Rather, the relationship to a foreign state or foreign state-related actor should include an element of direction. For example, an order or request. We would welcome feedback on the various forms of direction that could be included within the requirements.

- **Activities that may be registerable under the scheme.** To increase the risk to those seeking to engage in espionage, interference, or the theft of research in sensitive subject areas, the scheme would need to require the registration of activities that relate to particular areas of threat. The types of activity that we are currently considering could include lobbying, the funding of political campaigning, the work of think tanks, political communications and public relations; or the acquisition of ideas, information or techniques where produced by certain sensitive science and technology sectors. Engagement through the consultation will be vital in assisting the Government to test and refine its thinking. We intend to use this consultation process to determine the types of activities that the requirements should include, and conversely should not include, and work with impacted individuals, organisations and sectors to define them in the most effective and practical way. As this has been a point of concern in other countries, we want to be clear from the outset that the scheme would only require an individual to register if they are being directed by a foreign state or foreign state-related actor. This is unlikely to include, for example, foreign students, or students on scholarships from other countries.

A further consideration is how the scheme deals with hostile activity conducted from abroad. As a starting point, we intend to design the scheme to apply to activity conducted within the UK. We are aware however, of the increasing activities of those engaged in hostile activity that do not require an individual to be physically present within the UK. We are therefore considering whether the requirements of the scheme could be extended to certain activity conducted from outside of the UK, but where the effects of that activity occurs within the UK. We would welcome the views of respondents on this issue.

Questions for consultees:

24) Do you think the scheme's requirements should apply to individuals, organisations, or both? What advantages or disadvantages do you foresee?

25) Which actors do you think should be included within the definition of 'foreign state' or 'foreign state-related actor' for the purposes of the scheme's requirements?

26) This Government's manifesto committed to protecting the integrity of our democracy by preventing foreign interference in elections. With this in mind, are there any other categories of foreign actors that you would suggest including within scope of the scheme to support the Government's commitment, and to counter foreign interference in domestic politics and our democratic processes?

27) How do you think the 'direction' should be defined, where it is given by the foreign state or foreign state-related actor in relation to the registerable activity?

28) What activities do you think should be registerable under the scheme and how do you think this would contribute to tackling the key areas of threat (espionage, interference, transfer of research in sensitive subject areas)?

29) Do you think that the scheme's requirements should extend to certain activity conducted from outside of the UK, where the effects of that activity occur within the UK? What benefits or issues do you foresee with such an approach?

How could those impacted be made aware of the requirements?

We consider that a dedicated unit within a government department would be needed to provide day-to-day support of the scheme. We are considering a number of ways to ensure members of the general public, impacted sectors and international stakeholders are aware of any new requirements that may be introduced through a UK scheme. Many of these activities could fall to the dedicated unit, including through targeted communications, creation of a dedicated scheme website and day-to-day responsibility for enquiries and correspondence.

The Government will look for opportunities to use existing mechanisms to communicate the scheme's requirements and support its enforcement. For example, using the immigration system to inform visitors to the UK from overseas of the registration requirements or by integrating registration requirements into other tools and systems.

We are also considering the inclusion of a notification power[23], which could be used by the Government, if necessary, to clarify to an individual or entity that they (either in whole or in part) meet the definition of a foreign state or a foreign state-related actor for the purposes of the scheme. This could support the scheme in two ways: firstly, it would help clarify beyond doubt that an individual or entity is considered to be working for a foreign state actor or is a foreign state-related actor, ensuring those individuals working for them are fully aware of their obligations to register their activity; secondly, it would make it more difficult for those who seek to conceal or obfuscate their links to a foreign state or foreign state-related actor to do so. We aim to use this consultation process to determine how such a power could function in practice and identify any necessary safeguards (e.g. a clear decision-making process, reviews and appeals).

Questions for consultees:

30) What channels are available to your sector to communicate any registration requirements to individuals? How can these be best utilised?

31) Do you think there would be benefit in legislating for a notification power that could be used to clarify the status of an individual or entity as a foreign state or foreign state-related actor? What implications do you think there would be for the notified individual or entity?

How would an individual register their activity with the scheme?

We are particularly concerned to ensure the process of registration is simple, user-friendly and rapid. For many people, the most straightforward means of registering would be through a dedicated online portal or service. We welcome feedback on

[23] A key point to note is that this power would not designate or brand an individual or entity as a hostile actor. Rather, it would provide clarity to support compliance with the scheme.

whether alternative means of registering should be made available, including suggestions on where the registration requirements could be integrated with other government tools and processes which require similar information.

Questions for consultees:

32) Do you consider that there is a need to provide an alternative means for registration in addition to online registration (e.g. printable forms that can be posted)?

33) Are there existing government mechanisms that your sector relies on, which you think the scheme could integrate its requirements with? What are these mechanisms?

When would an individual be required to register their activity and what information would they be required to provide?

The question of when an individual should be required to register their activity has practical implications as well as implications for the utility of the scheme. One of the potential benefits of the scheme is to enable the disruption of hostile activity before the activity has resulted in damage to the UK. We are therefore considering whether the requirement to register should apply before the activity undertaken for a foreign state or foreign state-related actor commences. This could be particularly important where the registration concerns an activity that takes place at short notice, is very short in duration or involves an individual travelling into the UK for a very limited amount of time. We would welcome feedback from respondents on the practical implications of applying the requirements in such a way. We also recognise the need to consider timeframes for providing information and how this would impact on those who have already begun registerable activity prior to the requirements of the scheme coming into force– as noted above it is not the intention of the scheme to act as a barrier to, or otherwise impede, those engaging in legitimate activities.

As part of registration process, we would expect a UK scheme to require a combination of personal details (e.g. names, address, date of birth, passport/national ID number and employer) and key details of the activity being registered (e.g. purpose, duration and links to a foreign state or principal). Only such data as is necessary to differentiate one registrant from another would be made public (to include name and employer at a minimum).

It will be important for the requirement to register to be as clear and straightforward as possible, as this will be integral to its effectiveness and the delivery of the scheme's objectives. We would, therefore, welcome feedback on how this could be achieved and what challenges this may create. We would particularly welcome feedback on the information the scheme could require from the registrant and any risks or challenges in providing this prior to the activity taking place.

Questions for consultees:

34) What do you think the implications would be for you, your employer, or your sector of a requirement to register activity (where undertaken for a foreign state or foreign state-related actor) before it commences?

(Very negative – Negative – No impact – Positive – Very positive)

Comments: ________________________________

Would there be a requirement to keep registration information up to date?

The ongoing effectiveness of the scheme in delivering its objectives will depend on accurate and up-to-date information. Therefore, if a registrant becomes aware that information about their current activity or relationship with a foreign state or state-related actor has changed, it is proposed that they should be responsible for updating the registration accordingly. For persistent activity, or activity that takes place over a significant period of time, we are considering whether periodic supplemental statements would be required. We would welcome feedback on these examples and options to help us determine the most straightforward and efficient approach.

Questions for consultees:

35) What do you consider to be the most straightforward and efficient approach to ensuring that registered information remains accurate and up-to-date?

What may the consequences be for non-compliance with the scheme's requirements?

We consider that **for an activity to be registerable under the scheme, it should require a form of direction or request from a foreign state or foreign state-related actor**. The Government therefore anticipates that the vast majority of engagement with a foreign state or foreign state-related actors would <u>not</u> require individuals to register under the scheme. In order however, to ensure the effectiveness of the scheme, and in line with similar schemes in the US and Australia, we propose that an individual is liable to have committed an offence if they have not complied with or fulfilled an obligation in accordance with the scheme's requirements.

The Government is of the view that this would increase the risk to individuals who would seek to avoid their registration obligations. Offences could include an individual undertaking registerable activity without registering that activity with the scheme, or an individual purposely providing false or misleading information in their registration.

We consider, therefore, that the proposed penalties must reflect the potentially significant implications of activities that are conducted for, or on behalf of, foreign states and which are hostile in nature. Given financial penalties alone are unlikely to provide the necessary deterrent to those who seek to engage in hostile activity, we propose that non-compliance with the scheme should be capable of attracting a custodial sentence. We also consider that there may be merit in providing for financial penalties that could be used in combination with or instead of a custodial penalty where appropriate. We also recognise that there may be incidences of non-compliance which come about as a result of genuine error, and we intend for the offences to be designed so as to accommodate such circumstances. We welcome your feedback on this proposed approach and the range of possible penalties available.

Questions for consultees:

36) Do you consider that offences and penalties for non-compliance should be formulated to accommodate a range of circumstances, including intentional and unintentional non-compliance?

37) What do you think the implications of this scheme would be for your sector? Where do you see it helping and creating barriers?

(Very negative – Negative – No impact – Positive – Very positive)

Comments: ________________________________

Summary of questions for consultees on FIRS

23. What do you think the implications would be for you, your employer, or your sector in making certain information about registrants, their registerable activity and their registerable links to a foreign state available to the public?

24. Do you think the scheme's requirements should apply to individuals, organisations, or both? What advantages or disadvantages do you foresee?

25. Which actors do you think should be included within the definition of 'foreign state' or 'foreign state-related actor' for the purposes of the scheme's requirements?

26. This Government's manifesto committed to protecting the integrity of our democracy by preventing foreign interference in elections. With this in mind, are there any other categories of foreign actors that you would suggest including within scope of the scheme to support the Government's commitment, and to counter foreign interference in domestic politics and our democratic processes?

27. How do you think the 'direction' should be defined, where it is given by the foreign state or foreign state-related actor in relation to the registerable activity?

28. What activities do you think should be registerable under the scheme and how do you think this would contribute to tackling the key areas of threat (espionage, interference, transfer of research in sensitive subject areas)?

29. Do you think that the scheme's requirements should extend to certain activity conducted from outside of the UK, where the effects of that activity occur within the UK? What benefits or issues do you foresee with such an approach?

30. What channels are available to your sector to communicate any registration requirements to individuals? How can these be best utilised?

31. Do you think there would be benefit in legislating for a notification power that could be used to clarify the status of an individual or entity as a foreign state or foreign state-related actor? What implications do you think there would be for the notified individual or entity?

32. Do you consider that there is a need to provide an alternative means for registration in addition to online registration (e.g. printable forms that can be posted)?

33. Are there existing government mechanisms that your sector relies on, which you think the scheme could integrate its requirements with? What are these mechanisms?

34. What do you think the implications would be for you, your employer, or your sector of a requirement to register activity (where undertaken for a foreign state or foreign state-related actor) before it commences?

35. What do you consider to be the most straightforward and efficient approach to ensuring that registered information remains accurate and up-to-date?

36. Do you consider that offences and penalties for non-compliance should be formulated to accommodate a range of circumstances, including intentional and unintentional non-compliance?

37. What do you think the implications of this scheme would be for your sector? Where do you see it helping and creating barriers?

Consultation Proposal - Civil Orders

While the Government's preferred approach will always be to seek criminal prosecution where an individual is found to be engaged in an activity that constitutes an offence, it is recognised that there may be circumstances where it is not possible to adduce evidence to support a prosecution, or to take immigration action against an individual where they are not a UK national. For example, there may be a strong intelligence case to suggest that an individual is engaged in hostile activity, but with limited evidence that could be openly used to support criminal prosecution.

In the absence of prosecution these individuals could continue to act in ways that cause significant harm to the UK and its interests. While the police can, and would, continue to investigate individuals with a view to building an evidence base for prosecution it is in these circumstances that the introduction of preventative and restrictive measures, through a Civil Order, could be a useful tool to mitigate the risks posed by those who may be engaged in such activity. A Civil Order would complement the other measures being introduced as part of the legislation, providing operational partners with a full suite of measures to use.

We are therefore considering the creation of a new Civil Order to mitigate the risk posed by individuals engaged in hostile activity. For example, where an individual is engaged in espionage, sabotage, physical harms, interference or activity which enables any of these. The order could include a range of restrictive and preventative measures, including measures to prevent an individual associating with certain people or from visiting specified sensitive locations. We consider that these restrictions could be used to make it more difficult for an individual to engage in such activity, as well as providing a significant deterrent against those who may be vulnerable and susceptible to foreign state coercion and influence.

Although the Government is still considering what such a model could look like, including the test for imposing the order, our initial view is that the preventative nature of these measures would lend themselves to this being an order that could be imposed by the executive rather than the courts.

Questions for consultees:

38) Do you think preventative and restrictive measures are a desirable way of addressing the threat posed by those engaged in hostile activity where prosecution isn't viable?

Additional question for consultees

Given the evolving nature of the threat and ongoing debates in Parliament and beyond, both on the threat and the Government's response, we would welcome input from consultees on whether there are any additional measures which could be introduced or whether there is any existing legislation which could be amended or updated to address the threat.

Questions to consultees:

39) In addition to the policy proposals set out above, are there any other additional or reformed tools or powers that could be utilised to address the threats set out in this consultation, such as treason reform?

Contact details and how to respond

Please respond using the online system available at: https://www.homeofficesurveys.homeoffice.gov.uk/s/2RJAKB/

Please submit your response by Thursday 22nd July 2021 at 17:00

If you are unable to use the online system, for example because you use specialist accessibility software that is not compatible with the system, you may download a word document version of the form and email it or post it to:

State Threats Consultation.
Homeland Security Group
Home Office
5th Floor, Peel Building
2 Marsham Street
LONDON SW1P 4DF

Email: CST.Consultation@homeoffice.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Home Office using the e-mail address above or the address under 'Contact details and how to respond'.

Extra copies

Further paper copies of this consultation can be obtained from this address and it is also available online at https://www.gov.uk/government/consultations/legislation-to-counter-state-threats

Alternative format versions of this publication can be requested from: CST.Consultation@homeoffice.gov.uk

Publication of response

A paper summarising the responses to this consultation will be published alongside the introduction of legislation to Parliament. The legislation will be introduced as soon as Parliamentary time permits once responses from the consultation have been taken into account. The response paper will be available online at https://www.gov.uk/government/consultations/legislation-to-counter-state-threats

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004). If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this 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 as binding on the Home Office. The Home Office will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

Impact of Proposals

Impact Assessment

The Home Office acknowledges that these proposals, and in particular the creation of the FIR Scheme, may impact on business, charities and voluntary bodies. Impact of Official Secrets Acts reform and new and amended criminal offences on the public sector, such as the police and the Crown Prosecution Service (in England and Wales) is expected to be relatively minor. There will be costs associated with the creation and implementation of the FIR Scheme. These will be costed and set out in more detail as the scope and nature of the scheme is finalised. Outlined below are some of the different costs and benefits that we expect to be associated with the proposals outlined in this document.

Stakeholder group	Potential benefits
Businesses / organisations	Reduced risk to businesses/organisations from hostile activity and influence
Public sector	Benefit of avoiding potential costs of hostile activity, e.g. those borne by the emergency services in the event of an attack
Society	Benefit of deterring hostile activity, i.e. avoiding economic and social costs of a potential attack
	Increased transparency in political and business activity
	Benefit of disrupting hostile activity, e.g. identifying and penalising perpetrators
	Potential unintended consequences as a result of the proposals

Stakeholder group	Potential costs
Businesses / organisations	Costs of familiarisation with changes to legislation
	Potential loss of business activity due to the FIR Scheme
	Administrative costs of record keeping
Public Sector	Enforcement costs: associated with greater number of prosecutable offences under the reform of the Official Secrets Acts
	Legal Vetting - Solicitors Regulation Authority and Bar Standards Board would be responsible for organising appropriate security clearance for lawyers involved in applicable cases
	Costs of implementation and running the FIR Scheme
	Enforcement costs
	Criminal justice costs associated with non-compliance
Society / individuals	Registration costs to individuals, including a registration fee (if applicable) and time taken to register and provide supporting information

A full impact assessment will be published alongside the legislation on its introduction to Parliament.

When responding to the questions in this document we would welcome any feedback on the social and economic impacts of the proposals to inform our analysis.

Equalities Statement

Section 149 of the Equality Act 2010 places a duty on Ministers and Departments, when exercising their functions, to have 'due regard' to the need to eliminate conduct which is unlawful under the 2010 Act, advance equality of opportunity between different groups, and foster good relationships between different groups. The Home Office will conduct a full assessment of the equalities impact of the proposals as it develops the legislation in more detail.

We welcome any feedback on the impact of these proposals to inform our analysis.

Devolution

The proposals in this document relate to national security which is a reserved matter. Nevertheless, the Government is conscious that certain proposed provisions for this legislation touch on a number of devolved areas of competence. For instance, a provision to create an aggravating factor in sentencing for hostile activity by states would impact on devolved areas with regards to offences and sentencing. The Government will work with closely the Devolved Administrations as it prepares the legislation.

As noted, in relation to the FIR scheme, we recognise that the Belfast (Good Friday) Agreement and the unique circumstances of Northern Ireland demand particular care and attention. The Government is clear that the legislation is not intended to interfere with the underlying principles and spirit of the Agreement. In particular, we would welcome input, as part of the consultation, on how the FIR scheme, or wider legislative proposals can be developed in accordance with that intention.

Consultation principles

The principles that government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the consultation principles.

https://www.gov.uk/government/publications/consultation-principles-guidance

Annex A – Legislative context

State Threats legislation

Schedule 3 to the Counter Terrorism and Border Security Act 2019 – This legislation, which was introduced following the attack in Salisbury, provides a power to stop, question, search and detain individuals at a UK port or the Northern Ireland Border area to determine whether they are, or have been, involved in activity that threatens the UK's national security.

Other relevant legislation

Investigatory Powers Act 2016 – This provides a range of tools and powers to obtain communications and data about communications. The investigative tools in this legislation play a key role in the investigation of hostile activity by states.

Regulation of Investigatory Powers Act 2000 and the Covert Human Intelligence Sources (Criminal Conduct) Act – RIPA contains further powers that can be used to investigate and disrupt hostile activity by states including the use of Covert Human Intelligence Sources. The CHIS(CC) Act amends RIPA to provide a statutory power for the security and intelligence agencies, law enforcement agencies and a limited number of other public authorities to continue to authorise Covert Human Intelligence Sources (CHIS) to participate in criminal conduct where it is necessary and proportionate to do so.

Computer Misuse Act 1990 – This creates offences for unauthorised access to data stored on a computer; accessing a computer with intent to commit further illegal activity, such as stealing data for use in fraud or blackmail; or carrying out unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer or data held on it (including installing a virus or other malware). These offences are likely to be relevant to a range of hostile activity by states.

Counter Terrorism and Sentencing Bill[24] – Among other things this Bill will enable the Courts to consider if any serious offence is terror-related, rather than constraining the Courts to a defined list. Where the Courts identify a terrorism connection at the point of sentencing, for example in an offence involving firearms, then this can result in tougher sentences. This new approach is similar to that proposed in this consultation for a new aggravating factor in sentencing.

National Security & Investments Act 2021 – This Act, which was introduced to Parliament on 11 November, will establish a new statutory regime for Government scrutiny of, and intervention in, investments for the purposes of protecting national security. As an open economy, we welcome foreign trade and investment where it supports UK growth and jobs. The Government will not accept investments which compromise our national security and the Act provides predictability and transparency for businesses by setting out clear timelines for each stage of the

[24]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893148/cts-further-changes-sentencing-factsheet.pdf

screening process for the Government to consider notifications and assess potential transactions of national security interest.

Electoral integrity legislation - The Government, in its Manifesto, committed to ‘protect the integrity of our democracy, by introducing identification to vote at polling stations, stopping postal vote harvesting and measures to prevent any foreign interference in elections’. This Government is determined to strengthen the integrity of our electoral system and give the public confidence that our elections are modern, fair and secure. We will bring forward legislation on electoral integrity measures when Parliamentary time allows.

Other relevant work

Defending Democracy –Defending Democracy is a cross-Government initiative to maintain the integrity of our democracy and electoral processes. Its strategic objectives are to:

- protect and secure UK democratic processes, systems and institutions from interference;
- strengthen the integrity of UK elections;
- encourage respect for open, fair and safe democratic participation; and
- promote fact-based and open discourse, including online.

The Government is taking forward a co-ordinated programme of work to safeguard the integrity and security of our democratic processes. We are strengthening our legislative framework, driving policy across Government, enhancing capabilities and engaging with partners, including the Devolved Administrations in respect of their responsibilities for devolved legislature and local authority elections, to expand our efforts and ensure maximum impact of our work.

Disinformation - The Government’s view is that in order to reduce the potential impact of disinformation, we must take account not only of the actors involved, but of the environment that enables them to spread and amplify falsehoods, and the audience that they reach. Work is ongoing across Government to tackle the issue of disinformation.

In response to the wide-spread circulation of dis- and misinformation related to Covid-19, the DCMS-led Counter-Disinformation Unit stood up on 5 March 2020. The Unit brings together cross-Government monitoring and analysis capabilities to provide a comprehensive picture of the extent, scope and the reach of disinformation and misinformation linked to Covid-19, and to work with partners to address it. The Unit was previously stood up for both the European Parliament Election and General Election in 2019.

In December 2020 the Government published the Full Government Response to the Online Harms White Paper Consultation which sets out the new expectations on companies to keep their users safe online, and confirmed Ofcom as the regulator for Online Harms. The new laws will have robust and proportionate measures to deal with online disinformation that could cause significant physical or psychological harm to an individual, such as COVID-19 anti-vaccination content.

The forthcoming legislation will grant Ofcom a range of tools to tackle disinformation including: transparency reporting requirements; using media literacy to build audience resilience to disinformation; delivering supporting research on disinformation; and establishing an expert working group to build consensus and technical knowledge on how to tackle disinformation. The legislation will be ready later this year.

The Academic Technology Approval Scheme (ATAS) – ATAS applies to all international students (apart from exempt nationalities) who are subject to UK immigration control and are intending to study at postgraduate level in certain sensitive subjects. The subjects are those where students' knowledge could be used in programmes to develop Advanced Conventional Military Technology (ACMT), weapons of mass destruction (WMDs) or their means of delivery. These students must apply for an Academic Technology Approval Scheme (ATAS) certificate before they can study in the UK. ATAS will be expanded on 21 May to include individuals (apart from exempt nationalities) undertaking research into the same proliferation sensitive areas.

Export controls – The export of controlled goods and technology is regulated through a system of export licensing and includes military items, dual-use items (items with both civil and military uses), firearms, items that can be used for torture or capital punishment and goods subject to trade sanctions.

Annex B – The Government's Response to Law Commission recommendations

Official Secrets Acts 1911-39	
Law Commission Recommendation	**Government response**
Recommendation 1 – A new statute – containing modern language and updated provisions – should replace the Official Secrets Acts 1911 – 39.	The Government agrees that a new statute with modern language and reformed provisions is required to address current and future threats posed by espionage and hostile activity by states. The Government therefore intends to repeal the Official Secrets Acts 1911-39, with a view to reform and strengthen existing provisions.
Recommendation 2 – In any new statute to replace the Official Secrets Act 1911, the concept of "enemy" in section 1 should be replaced with that of "foreign power". The Canadian definition of "foreign power", including reference to terrorist groups and entities directed by a foreign government, should be used as a starting point for drafting that element of a new provision.	The Government welcomes the recommendation that the term "enemy" be updated. It is outdated, does not reflect the threat posed by non-state actors, and risks damage to bilateral relations in associating a country with the term "enemy", as part of a criminal prosecution. We consider it necessary to capture hostile activity by a broad range of actors, such as entities under the influence of, or acting on behalf of a foreign government, but not directed and controlled by that government. Further consideration will be needed to ensure a definition is chosen to explicitly capture such threats.
Recommendation 3 – In any new statute to replace the Official Secrets Act 1911, the term "safety and interests of the state" should be retained.	We welcome the recommendation that the term "safety or interests of the state" be retained. The experience of HMG and the governments of allied States is that espionage is frequently targeted at, and can do significant damage to, a wide range of national interests.
Recommendation 4 – An individual should be criminally liable for an espionage offence if he or she has a purpose	We welcome the recommendation that offences of espionage should be updated, to provide important safeguards, to prevent

which he or she knows or has reasonable grounds to believe is prejudicial to the safety and interests of the state.	the successful prosecution of those who may not have reason to believe that their conduct is prejudicial (for example, where they are misled regarding the nature of their actions or target), whilst allowing a sufficiently robust offence to deal with those who acted with intent or where, in all the circumstances, they should have reasonably known or suspected that their activities would be prejudicial.
Recommendation 5 – In any new statute to replace the Official Secrets Act 1911, the requirement that the defendant's conduct was capable of benefitting a foreign power should continue to be objectively determined. There should be no requirement to prove that the defendant personally knew or believed that his or her conduct had such capability.	The Government welcomes this recommendation and agrees that the fact that conduct was capable of benefitting a foreign power or entity should remain a point to be objectively decided by the jury. We view that this adequately reflects the spirit of the original offence whilst bringing the measure into line with modern criminal law.
Recommendation 6 – The list of prohibited places should be drafted to reflect the modern espionage threat. The Secretary of State should have the power, by statutory instrument subject to the affirmative resolution procedure, to amend the list of prohibited places where it is appropriate to do so in the interests of the safety or interests of the state. The Secretary of State is obliged to consider taking steps to inform the public of the effect of any designation order, including in particular, by displaying notices on or near the site to which the order relates, where appropriate.	We agree with the recommendation that the list of prohibited places should be drafted to reflect the modern espionage threat. The current list of sites is inadequate and leaves certain types of site, which hold sensitive information, vulnerable to hostile activity by states. We note the recommendation that the Secretary of State should have the power, via the affirmative resolution procedure, to amend the list of prohibited places where it is appropriate to do so in the interests of national security. We consider, however, that there is a requirement for a power that enables the Government to designate sites at pace, to protect sensitive sites which may suddenly face an increased threat and/or require temporary protection. This is an issue we intend to explore more when developing new legislation. We also note the recommendation that the Secretary of State be obliged to consider taking steps to inform the public of the effect

	of any designation order, including use of signage where appropriate. This will need to be balanced against the protection of sites where notification of the public may increase the threat.
Recommendation 7 – There should continue to be no restriction on who can commit the offences contained in the Official Secrets Act 1911 or in any replacement legislation. There should continue to be separate offences of espionage by trespass and espionage by collection or communication of information. The espionage by trespass offence should also continue to apply to those who approach, inspect, pass over, or enter any prohibited place within the meaning of the Act. The collection and communication offence should continue to be capable of being committed not only by someone who communicates information, but also by someone who obtains it. References in the Official Secrets Acts 1911 and 1920 to a sketch, plan, model, note and secret official pass word and code word are anachronistic and should be replaced with “document, information or other article”. Information should be defined to include any program or data held in electronic form.	We agree with the recommendations on reforming how espionage offences are constructed. We particularly welcome the retention of the elements of espionage offences which are committed by those who obtain information, and approach or inspect prohibited places. We note that the Law Commission consider that the espionage by trespass offence should continue to apply to those who approach, inspect, pass over, or enter any prohibited place within the meaning of the Act. As outlined above, we think this offence should be retained in a reformed, modernised prohibited places regime and will seek to capture the original essence of the offence, whilst bringing it up to date with the standards of modern criminal law. We agree with the recommendation to update terminology which refers to narrowly defined categories such as ‘sketches, plans and models.’ Ongoing work has found that the 1911-39 Acts are excessively narrowly drafted, with terminology which does not reflect the modern espionage threat. We will seek to ensure that the legislation adopts language which is both up to date and appropriately futureproofed.
Recommendation 8 – Sections 1(2) of the Official Secrets Act 1911 and section 2(2) of the Official Secrets Act 1920 should be repealed.	Given the difficulty reconciling these provisions with modern legal principles, the Government agrees with this recommendation. We do consider, however, that the formulation of the elements of future espionage offences will need to be defined with due regard to the practicalities of prosecution. For instance, the formulation must consider the challenges associated with obtaining evidence of people acting covertly, and the issues

	associated with the disclosure of intelligence in court, so that offences can be realistically proven.
Recommendation 9 – Section 7 of the Official Secrets Act 1911 and section 2(1) and section 6 of the Official Secrets Act 1920 should be repealed without replacement. The offence of doing an act preparatory to espionage should be retained. Save for that, section 7 of the Official Secrets Act 1920 should be repealed.	We welcome this recommendation. It is important that law enforcement can arrest those looking to conduct espionage at a preparatory stage, as this is the best means of ensuring that sensitive information remains secure. We are also considering the case for broadening the offence to apply to acts preparatory to other types of hostile activity by states, outside of espionage, such as sabotage or foreign interference. By maintaining and broadening an offence of this type, we would seek to criminalise relevant acts carried out in the lead up to hostile activity, which would enable the police to intervene at an early stage before these preparatory acts can culminate into serious harm.
Recommendation 10 – The territorial ambit of the offences contained in the Official Secrets Acts 1911-1939 should be expanded so that they can be committed irrespective of the individual's nationality. The test should be whether there is a "significant link" between the individual's behaviour and the interests of the United Kingdom. "Significant link" should be defined to include not only the case where the defendant is a Crown employee or contractor, but also the case where the conduct relates to a site or data owned or controlled by the UK government (irrespective of the identity of the defendant). To ensure that sensitive UK assets overseas receive maximum protection, any new definition of "prohibited place" (see recommendation 6) should explicitly provide that such places may be overseas.	We broadly welcome the recommendation that the territorial scope of offences under the 1911-39 Acts be updated and agree that the current legal position, which only applies to British citizens or subjects abroad, is insufficient to protect British assets at home and elsewhere. The nature of the threat and HMG's global footprint, as well as the movement of individuals around the world and developments in cyber technology, has changed the way espionage is carried out. Therefore, the Government agrees that the territorial application of espionage offences should be expanded, so they can be committed irrespective of the offending individual's nationality or location and applies when the UK's interests are damaged by espionage, or UK assets, sites or information are subject to espionage. The Government is considering whether the 'significant link' model (as seen in other UK legislation) is the correct model to

	cover espionage against assets in the UK from overseas, or upon a UK site or information based overseas.
Official Secrets Act 1989	
Recommendations 11 & 12 – 11 - Those offences under the Official Secrets Act 1989 that relate to Crown servants or government contractors and that require proof or likelihood of damage (section 1(3); section 2(1); section 3(1); section 4(1) should no longer require such proof or likelihood. Instead, there should be an explicit subjective fault element. Further work will be required to determine the most appropriate fault element (i.e. that the defendant (i) knew, (ii) believed; or (iii) was reckless as to whether the disclosure (a) would cause damage; (b) was likely to cause damage; (c) risked causing damage; or (d) was capable of causing damage). Sections 5 and 6 should continue to be based on proof or likelihood of damage. 12 - The offence contrary to section 1(1) of the Official Secrets Act 1989 should not be amended to require proof that the disclosure was damaging. The “defence” currently contained in section 1(5) of the Official Secrets Act 1989, of not knowing and having no reasonable grounds to believe that the material disclosed related to security or intelligence, should continue to apply.	The Government welcomes the Commission’s recommendations that offences in sections 1 to 4 of the Act - relating to Crown servants, government contractors and those notified - should no longer require the prosecution to evidence proof or likelihood of damage, and that offences contrary to section 1(1) of the Official Secrets Act 1989 should not be amended to require proof of damage. We agree with the Commission that this requirement is wrong in principle and creates real practical issues, acting as a barrier to potential prosecutions. In practice, proving damage in an open judicial system would likely require the disclosure of additional confidential information, which in turn could cause further material damage, meaning there is often a reluctance to pursue prosecutions. We note, however, that whilst the removal of the damage requirement would, for this reason, remove one barrier to the prosecution of offences in sections 1 to 4 of the Act, existing challenges surrounding the requirement to disclose (often highly sensitive) information as evidence, through usual criminal disclosure in open court, would still remain. We will consider the merits of this recommendation further when developing legislation. We also accept the recommendation that the ‘defence’ of not knowing or having reasonable grounds to believe that material disclosed related to security or intelligence (and thus in scope of section 1(1)), should continue to apply. In addition, the Government notes the additional recommendations that for sections 1 to 4, there should be an explicit, subjective fault element and that the offences in sections

	5 and 6 should continue to include the requirement to evidence proof or likelihood of damage. We will explore both of these suggestions further, but we do consider that both primary and onward disclosures have the potential to cause equal amounts of harm.
Recommendation 13 – The definition of “member” of the security and intelligence services should be clarified to mean any individual employed or contracted by the security and intelligence services or seconded or attached to them. There should be a statutory requirement to publish guidance on the notification process. The guidance should state which categories of office are subject to notification and how an individual can challenge a decision to notify him or her.	We welcome the recommendation that the definition of “member” of the security and intelligence services should be more clearly defined in any new legislation. We note the recommendation that there should be a statutory requirement to publish guidance on the notification process. We intend to explore options for reviewing the notification process, as we develop proposals for Official Secrets Acts reform.
Recommendation 14 – A maximum sentence of two years’ imprisonment does not provide the court with adequate powers in really serious cases. Parliament should consider increased maximum sentences for some offences under the Official Secrets Act 1989. Consideration should also be given to whether a distinction ought to be drawn in terms of maximum sentence between the offences in sections 1 to 4 of the Official Secrets Act 1989 and the offences in sections 5 to 6.	The Government welcomes the recommendation that a maximum sentence of two years does not provide the court with adequate powers in the most serious cases of unauthorised disclosure. Since the passage of the Act in 1989, there have been unprecedented developments in communications technology (including data storage and rapid data transfer tools) which in our view, means that unauthorised disclosures are now capable of causing far more serious damage than would have been possible previously. As a result, we do not consider that there is necessarily a distinction in severity between espionage and the most serious unauthorised disclosures, in the same way that there was in 1989. Although there are differences in the mechanics of and motivations behind espionage and unauthorised disclosure offences, there are cases where an unauthorised disclosure may be as or more serious, in terms of intent and/or damage. For example, documents made available online can now be accessed and utilised by a wide

	range of hostile actors simultaneously, whereas espionage will often only be to the benefit of a single state or actor. In severe cases, the unauthorised disclosure of the identities of agents working for the UK intelligence community, for example, could directly lead to imminent and serious threat to life. In addition, the unauthorised disclosure of information could also provide multiple hostile actors with critical information relating to core UK defence capabilities, for example, which could ultimately render these capabilities ineffective as a result.
Recommendations 15 – 17 – 15 - The professional bodies responsible for the Codes of Conduct for practising lawyers – the Solicitors Regulation Authority and Bar Standards Board – consider including explicit guidance on the importance of maintaining confidentiality in cases involving the Official Secrets Acts, and the obligation not to receive disclosures unless they have the appropriate security clearance and premises assurance. 16 – Where a person not subject to section 1(1) of the Official Secrets Act 1989 who is not a subject of a relevant criminal investigation makes a disclosure to a qualified lawyer for the purpose of obtaining legal advice, that disclosure should constitute an authorised disclosure, subject to specific safeguards being met. The safeguards are as follows: (i) the legal adviser must be subject to professional obligations, either through the Bar Standards Boar or the Solicitors Regulation Authority; and (ii) the lawyer to whom the disclosure is made must have undergone security vetting to the appropriate level and systems/premises assurance.	The Government welcomes the Law Commission's package of recommendations in relation to security and vetting requirements upon lawyers. Access to legal representation is a core part of the UK legal system and we fully support all attempts to ensure access, when seeking advice in this complex and sensitive area. However, such access must be balanced with the requirement to safeguard sensitive official material, the release of which could cause a threat to life, and/or significant damage to national security. We will consider options when developing legislation, which balance these requirements with the importance of people being able to seek independent legal advice, and will draw on the views advanced in the Review accordingly.

17 – Where a Crown servant, government contractor or notified person is a suspect in a criminal investigation and makes a disclosure to a qualified legal adviser for the purposes of legal advice, that disclosure should be authorised for the purposes of sections 1 to 4 of the Official Secrets Act 1989 if the legal adviser has security clearance to the appropriate level, given the nature of the protected information, and has undergone systems/premises assurance.	
Recommendation 18 – It should be made explicit that prior publication is a factor that ought to be considered by prosecution agencies, courts, and juries when determining whether an unauthorised disclosure was damaging for the purposes of the sections 5 and 6 offences under the Official Secrets Act 1989. It should be made clear that it is not an offence for the purposes of sections 1(3) to 4 to communicate information that has been already communicated to the public or made available to the public with lawful authority.	The Government welcomes these recommendations, in principle, and as part of legislative work in this area, we will consider whether a more explicit test around information lawfully in the public domain/widely distributed needs to be created. This may, for example, be the case if we sought to pursue legislation which did not incorporate a damage requirement. We can see merit in the recommendation that it should be clarified that it is not an offence for a member of the security and intelligence agencies, or a notified person, to communicate information that is already in the public domain with lawful authority. We will consider this as part of legislative work in this area.
Recommendations 19 & 20 – 19 – The categories of information currently protected by the Official Secrets Act 1989 should not be narrowed at this time. For any reform of the Official Secrets Act 1989, however, the possibility of defining the categories of	As part of legislative reform, we will consider whether to amend the categories of information protected[25], to reflect technological and national security developments since the legislation was enacted, and to ensure new legislation is futureproofed.

[25] The categories of information protected by the Official Secrets Act 1989 include; Security and Intelligence; Defence; International Relations; Crime and Special Investigation Powers; and Security, Intelligence, Defence or International Relations information communicated in confidence to another State or international organisation.

information with greater precision ought to be explored as a priority. 20 – The categories of information protected by the Official Secrets Act 1989 should not be expanded to include economic information in so far as it relates to national security.	
Recommendation 21 – The territorial ambit of sections 1 to 4 of the Official Secrets Act 1989 should be amended so that a government contractor or notified person commits an offence when he or she makes an unauthorised disclosure abroad irrespective of whether he or she is a British citizen.	The Government agrees that there is a need to change the territorial extent of the offences in the 1989 Act and we will consider adopting a version of the formulation proposed by the Commission, as part of legislative reform. We will also consider whether the territorial scope for the offences under sections 5 and 6 (onward disclosures by a third party) should be extended, to bring into scope British citizens and those with a right to remain in the UK, when overseas. The serious threat posed to UK interests by those who commit damaging unauthorised disclosures exists not solely in the case of British citizens, but also in the case of those who benefit from resident and settled status. We note that the Review is not explicit on whether this should also apply to formerly notified persons, government contractors and Crown servants, which is something we would also seek to consider, in more detail. In addition, the 1989 Act offences exclude the prosecution of other individuals overseas, even in cases where the individual would have known (or indeed intended) for the disclosure to cause damage. There may be circumstances in which the Crown should be able to consider prosecution against non-British citizens for unauthorised disclosure, who have caused damage through their disclosure, which we will consider further.

Recommendations 22 – 24 – 22 - There should be a review of unauthorised disclosure offences with the aim, in particular, of creating greater coherence and consistency in terms of the defences available and penalties that apply. 23 – If widescale review of the miscellaneous disclosure offences is conducted, it ought to include section 170 of the Data Protection Act 2018 for the sake of completeness and in an effort to ensure maximum coherence. 24 – National security disclosure offences should form part of the review of miscellaneous disclosure offences recommended above.	The Government notes these recommendations and will explore options for review, if relevant, as part of legislative reform.
Recommendations 25 – 28 – 25 – The Protocol on Leak Investigations should be reviewed and updated, in consultation with Government Departments, the Crown Prosecution Service, the Metropolitan Police, the Attorney General, and any other interested parties. 26 – Consideration should be given, as part of the review of the Protocol, to an appropriate mechanism for providing oversight of its operation. 27 – The Crown Prosecution Service guidance "Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists" should be updated to reflect developments in case law and to make reference to the Protocol.	The Government notes the Commission's recommendations with regards to Protocol on a Leak Investigations and the Crown Prosecution Service's guidance on "Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists," and will consider them further.

28 – The Protocol should be published more accessibly online with information stating when it came into force and detailing any revisions.	
Recommendations 30 & 31 – 30 – The [Crown Prosecution Service's] guidance on authorised jury checks ought to be amended to state that if an authorised jury check has been undertaken, then this must be brought to the attention of the defence representatives and the judge. 31 – A separate review should be undertaken to evaluate the extent to which the current mechanisms in the criminal trial process strike the correct balance between the right to a fair trial and the need to safeguard sensitive material.	We note these recommendations for authorised jury checks guidance to be amended and for there to be a separate review of the current mechanisms in the criminal trial process. The Government will consider these further.
Recommendations 32 & 33 – 32 – An independent, Statutory Commissioner should be established with the purpose of receiving and investigating allegations of wrongdoing or criminality, where otherwise, the disclosure of those concerns would constitute an offence under the Official Secrets Act 1989. That Commissioner would have to constitute an effective investigative mechanism: it would therefore have not only to be independent, but also be able to act expeditiously and have the legal authority to compel cooperation with its investigations. There should be a right of appeal by the complainant against decisions of the Statutory Commissioner. The jurisdiction of the Investigatory Powers Tribunal should be expanded such that it can hear appeals against decisions of the Statutory Commissioner.	We note these recommendations and will consider in further detail proposals relating to a Statutory Commissioner and a Public Interest Defence. As part of these considerations, we will also reflect on the Commission's comments regarding the compatibility of the Act with Article 10 of the European Convention on Human Rights – the right to freedom of expression. From our initial considerations, the Government believes that existing offences are compatible with Article 10 and that these proposals could in fact undermine our efforts to prevent damaging unauthorised disclosures, which would not be in the public interest. Safeguards already exist (including existing processes for Government whistleblowers) which allow them to raise concerns without needing to undertake an unauthorised disclosure. These processes include; the possibility of raising a concern inside their own organisation, with the Cabinet Office, the Civil Service Commission, and even the chair of the Intelligence and Security Committee of Parliament. For former and current members of the

33 – A person should not be guilty of an offence under the Official Secrets Act 1989 if that person proves, on the balance of probabilities, that: (a) it was in the public interest for the information disclosed to be known by the recipient; and (b) the manner of the disclosure was in the public interest. The Law Commission make no further recommendation beyond this in respect of the form of the defence.	security and intelligence agencies, there are additional offices to which disclosures can be made, creating a further set of safeguards for that group. Any decision to prosecute will be subject to the public interest test by the Crown Prosecution Service, and in most cases, requires the consent of the Attorney General to prosecute. The efficacy of existing mechanisms and safeguards across Government is key to the operation of these offences, and the Government will review their operation, in order to assess the Commission's recommendations for a Statutory Commissioner, when exploring options for Official Secrets Act 1989 reform. Press freedom is an integral part of the UK's democratic processes, as is the ability for individuals to whistleblow and hold organisations to account, when there are serious allegations of wrongdoing. However, a balance must be struck with safeguarding official information (including national security information), where its compromise could harm the UK, its citizens or interests, given the unlawful disclosure and/or subsequent publishing of sensitive documents can lead to serious harm in many cases. We are not convinced that the Law Commission's recommendations strike the right balance in this area. Our fundamental concern is that a person seeking to make an unauthorised disclosure, whether in Government or otherwise in possession of official material, will rarely (if ever) be able to accurately judge whether the public interest in disclosing the information outweighs the risks against disclosure. Even if the case is subsequently made that the disclosure was not in the public interest, and the person who published the information has committed a criminal offence, this does not undo the potential damage caused by the disclosure.