Home Office

LEGISLATION TO COUNTER STATE THREATS (HOSTILE STATE ACTIVITY) CONSULTATION

GOVERNMENT RESPONSE DOCUMENT

CONTENTS

INTRODUCTION

This is the Government's response to the Legislation to Counter State Threats (Hostile State Activity) public consultation. This should be read alongside the National Security Bill which was introduced in Parliament on the 11th of May.

This response details the following:

- Statistical reporting of the responses and summaries of the key themes; and
- An indication of how consultation responses have informed our recently introduced National Security Bill.

For an accessible format of this document, please visit:

Legislation to counter state threats - GOV.UK

(www.gov.uk)

MINISTERIAL FOREWORD

In May I introduced the National Security Bill in the House of Commons. The Bill will bring together a suite of new measures to further protect our national security, the safety of the British public, and our vital interests from those who would seek to do us harm.

In May 2021, the Home Office published a consultation on legislative proposals to counter state threats. In that document, I discussed the growing, diversifying, and evolving threat from hostile activity by states.

State threats are persistent and take many forms, including espionage, foreign interference in our political system, sabotage, disinformation, cyber operations, and even assassinations. These actions often take place in the shadows, but the harm is very real. The Security Service Interference Alert to Parliament in January, is a reminder of the very real and serious threat from those who seek to undermine and destabilise open and democratic societies, as well as the international rules-based system that underpins our stability, security and prosperity.

We need no reminder that 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. The Russian invasion of Ukraine is the most acute, but not the only, example of the lengths some foreign leaders go to in order to seek strategic advantage.

I want to thank all those who responded to the consultation. The responses informed many aspects of the Bill, as shown in this consultation response. I am confident that the measures included in this Bill will further protect us and keep our country safe, enhancing our ability to deter, detect, and disrupt those state actors who seek to do the UK harm.

The Bill will deliver the biggest overhaul of UK state threats legislation for a generation. It will keep our country safe by making the UK an even harder target for those states who seek to conduct hostile acts against the UK, steal our information for commercial advantage, or interfere in our society covertly. It will ensure our world class law enforcement and intelligence agencies have the modern tools, powers, and protections they need. With updated investigative powers and capabilities, those on the front line of our defence will be able to do even more to counter state threats and preserve the integrity of our society.

The Bill will reform existing espionage laws, providing effective legislation to tackle the current threat by creating a modern set of offences to protect the UK against espionage and related conduct, namely: obtaining and disclosing protected information and trade secrets; and assisting a foreign intelligence service. The Bill will also establish new offences to tackle state-linked sabotage and foreign interference. It will reduce the harm done by state threats actors as it will allow for disruptive action to be taken earlier through a preparatory conduct offence. The Bill also addresses the seriousness of state threats by enabling other offences where there is a state link (e.g. kidnap) to be aggravated (which may result in a sentence increase). The Bill will also improve existing powers which grant police officers the ability to stop individuals at ports to ascertain their involvement in hostile activity by foreign states. Additionally, it will introduce a new suite of State Threats ‘Prevention and Investigation Measures’ to use as a tool of last resort to manage those who pose a threat but whom it has not been possible to prosecute.

I also intend to introduce a Foreign Influence Registration Scheme. The scheme will require individuals to register certain arrangements with foreign governments to deter and disrupt state threats activity in the UK, bringing the UK into line with our allies. Further detail on the scheme will be set out.

Most recently on state threats, the Government introduced the Schedule 3 state threats examination power in the Counter-Terrorism and Border Security Act 2019, the linked National Security and Investment Act 2021, and the Economic Crime (Transparency and Enforcement) Act 2022, which was recently expedited in light of the Russian invasion of Ukraine. This legislation builds on those Acts and was designed in close consultation with security services to provide the tools and powers the UK needs to tackle state threats.

This Bill is part of the Government's priority to make our streets safer and should be viewed alongside the Online Safety and the Economic Crime and Corporate Transparency Bills which will be before the House in this session.

Together, these measures enhance support our world-class law enforcement and intelligence agencies by providing them with modern tools to protect us and our national security.

The Rt. Hon. Priti Patel MP
HOME SECRETARY

EXECUTIVE SUMMARY

The Legislation to Counter State Threats (Hostile State Activity) consultation ran from 13 May 2021 to 22 July 2021.

208 individuals or organisations responded to the consultation via an online survey or e-mail. A breakdown of submitted responses can be found below:

Response Method	Organisation response	Individual response	Campaign Responses	Total
Online portal	15	143*	0	158
E-mail	32	18	0	50
Total	47	161	0	**208**

*6 online respondees did not declare if responding as an individual or organisation.

Most responses sent directly were from organisations representing particular sectors (such as the media or academia), some of which followed attendance at a virtual roundtable. 90% of responses on the online portal were from members of the public.

Respondees had the opportunity to answer 39 questions spread across four sections. The sections were broken down as follows:

- Section 1: Official Secrets Acts Reform
- Section 2: Foreign Influence Registration (FIR) Scheme
- Section 3: Civil Orders
- Section 4: Additional questions for consultees

We have structured Section 1-3 of this Government response to align with our current legislative priorities, with Sections 4-5 covering those areas we will be continuing to work on in the longer-term. The Government's response is structured as follows:

- **Section 1: Official Secrets Acts 1911-39 Reform**
- **Section 2: State Threats Prevention and Investigation measures**
- **Section 3: Foreign Influence Registration Scheme**
- **Section 4: Additional questions for consultees (treason reform)**
- **Section 5: Official Secrets Acts 1989 Reform**

CONSULTATION EVENTS

In May 2021, Home Office officials began an engagement programme with a wide range of organisations, industry representatives, and operational partners with an interest in the legislative proposals.

Initial engagement focused on promoting awareness of the consultation through a range of communications and engagements across Government and its partners. The Home Office then ran virtual workshops with specific interested groups and sectors, providing an opportunity to comment directly on the key issues within the legislative proposals, encouraging further comments through the official consultation channels.

In total, seven virtual engagement events were undertaken on proposals with representation from 23 groups/organisations. Through these sessions the Home Office engaged with sector representatives from higher education, research, business, media, civil liberty, and legal sectors, alongside others.

SECTION 1: Official Secrets Acts 1911-39 Reform

Introductory remarks

Section One of the consultation set out the background to the Official Secrets Acts and the case for reform, and in particular responded to the Law Commission's Review of the Protection of Official Data, highlighting where the Government agreed with those recommendations, as well as highlighting issues we intended to consider further and were seeking input on. Responses to these aspects of the consultation have helped inform Part 1 of the Bill which provides a suite of offences and supporting measures to address criminal activity for or on behalf of, or with the intention to benefit, a foreign state. Generally speaking, an offence will be made out where the harmful activity has taken place and the person is acting for, on behalf or, or with an intention to benefit, a foreign state. The measures covered by the consultation and included in the legislation are as follows.

Espionage
The Bill reforms existing espionage offences to reflect the evolving threat and the interconnected nature of the modern world. Espionage is tackled by three new offences in the Bill that are designed to capture modern methods of spying and related harmful conduct, and provide the ability to impose penalties reflecting the additional seriousness and harm that can arise:

- The offence of obtaining or disclosing protected information criminalises espionage activity in relation to the Government's sensitive information, including defence information or the work of the intelligence agencies.
- The offence of obtaining or disclosing trade secrets criminalises espionage in relation to information that has actual or potential commercial, economic, or industrial value, such as a new technology developed in the UK.
- The provisions on assisting a foreign intelligence service will explicitly criminalise materially assisting a foreign intelligence service in carrying out activities in the UK, or overseas where such conduct is prejudicial to UK safety and interests.

Entering and inspecting places used for defence
The Bill establishes a standalone regime for protecting sensitive sites from espionage and other state threats, modernising the list of protected sites, and creating new offences and accompanying police powers to capture harmful activity around sites that are critical to the safety or interests of the UK.

Sabotage
Establishes a new offence of sabotage designed to capture state-linked saboteurs who act in a way that is prejudicial to the UK's safety or interests by causing damage, including through cyber-attacks, to assets such as the UK's critical infrastructure.

Foreign interference
Establish a new offence of foreign interference where conduct is intended to have a specified negative effect and certain conditions are satisfied. We are also increasing the maximum custodial penalties for certain election-related offences that are carried out for or on behalf of, or with the intention to benefit, a foreign power.

Preparatory conduct
Reforms the existing acts preparatory offence under the Official Secrets Act 1920, to ensure that it is can effectively target harmful preparatory state threats activity before serious and potentially irreversible harm occurs.

State threats aggravating factor
Create a new state threats aggravating factor to ensure that where individuals commit offences other than those in this Bill (e.g. kidnap) with a proven link to a foreign power, the state threat link is appropriately recognised in the sentencing.

Search and seizure powers
Modernise the existing search warrant power to enable the police to obtain evidence of state threats activities.

In Section One we sought further input in relation to a number of the Law Commission's recommendations, to inform final policy development. The Government also sought views on 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 was a case for new standalone offences to cover hostile activity including sabotage, economic espionage, and foreign interference.

We were grateful to receive a wide range of views, which we have broken down into key themes and responded to below as follows:

Issues raised and Government responses

The link to the state

Issues raised

The Government outlined its intention in the consultation to make a connection to hostile activity by states an aggravating factor in sentencing. Whilst no consultation questions were asked in this section, a view was put forward querying whether it would be unjust to aggravate a sentence where a defendant did not know the offence was connected to state threats.

Government response

The Government considers this an important point which has wider application to potential offences beyond the context of the aggravating factor. The Government agrees it is important that offences and supporting measures in the Bill apply in the right circumstances. It is also right to safeguard a defendant from having their sentence aggravated where they could not have known of the connection between the offence committed and state threats activity. To ensure the measures are applied appropriately, the Bill creates a 'foreign power condition' and associated definition of a 'foreign power'. Under these provisions a person will only commit a relevant offence, or have their sentence aggravated, where they know, or ought reasonably to know, that they are carrying out conduct for or on behalf of a foreign power or acts with the intention to benefit a foreign power.

In their consultation, the Law Commission specifically considered the need to replace the term '*useful to an enemy'* in the current espionage offence, instead considering a more modern concept of '*foreign power'*. Respondees to that consultation observed that without wider changes to the way the offences were constructed, this change could unreasonably broaden the scope of the legislation. Our approach recognises this.

Impact on media freedom & legal privilege

Issues raised

A large number of responses to the consultation conflated the potential reform of espionage provisions in OSAs 1911-1939 with the potential reform of offences in the OSA 1989 which relates to disclosing official information (covered in more detail in Section 5). There was concern that through these reforms the Government was intending to treat journalists like spies and that the legislation could undermine press freedoms.

The Official Secrets Act 1911 currently provides the police with the power to issue search warrants for investigations under the OSA. This power enables action to be taken where there are reasonable grounds for suspecting that an offence is being, or is about to be, committed. These provisions allow for searches of excluded and special procedure material and for warrants to be issued by a superintendent in urgent cases. In the context of proposals for reform of this power, a number of representations were made about the need to ensure that any such reform did not erode media freedoms or allow access to legally privileged material. Respondees helpfully drew the Government's attention to relevant caselaw in this area, and in particular the need for judicial authorisation based on clear criteria in cases seeking access to confidential journalistic material.

Government response

In developing new and modernised offences to address the threat of espionage, the Government has given careful regard as to how these could impact on press freedoms. When developing the foreign power condition, the Government carefully considered whether the legislation should capture activity that was 'capable of benefitting a foreign power' as an additional alternative to activity carried out for or on behalf of, or with the intention to benefit a foreign power.

The Government concluded that a formulation that simply required the Crown to demonstrate that the person was acting for a purpose prejudicial to the safety or interests of the UK and that the conduct was capable of benefitting a foreign power set too low a bar and could criminalise legitimate journalism.

In defining a foreign power, the Government also considered whether it would be appropriate to include companies that are under significant control of the foreign power within that definition. While the Government recognises the importance of capturing activity conducted by states through the use of proxies, it would not be appropriate to achieve this by defining state-owned companies, which could include foreign-owned media groups, as part of a foreign power given that this could include cases where a person is acting purely in the interests of the company. Instead, the provisions in the Bill capture those working indirectly through a state-owned company in cases where the person knows, or reasonably ought to know, that the activity in question is being conducted for or on behalf a foreign power.

Overall, the Government considers that the creation of two complementary offences of obtaining or disclosing information where a person is acting for a foreign power, allied with the offences of providing assistance to a foreign intelligence service, ensure that the requisite harmful conduct is covered without capturing legitimate activity.

In relation to the concerns about the impact of the search power on media freedoms, this power of search is a key tool in Official Secrets Acts investigations which is not replicated in other general search powers. Thus, other powers, such as those provided in the Police and Criminal Evidence Act 1984 will not suffice in state threats investigations which often involve

highly sophisticated state actors who are skilled in tradecraft. It is vital, in creating a suite of new offences, that the police and other agencies have the powers to effectively investigate the harms this Bill is seeking to address. The existing power provides a highly valuable investigative tool in countering state threats investigations which are complex with those working for states often skilled in how to keep their activities hidden.

In reforming the existing power, the Government has ensured it contains the same strong safeguards which apply to other modern search powers and has taken into account relevant caselaw on Article 10 of the ECHR. Safeguards include:

- The need for warrants authorising search and seizure to be made by the courts in all but the most urgent cases with the Secretary of State notified of any use of the urgent process;
- Any warrant for the search and seizure of confidential material needing to be preceded by a production order seeking disclosure of that information except in clearly specified circumstances;
- Any production order, warrant or authorisation seeking access to confidential material needing to be based on clear conditions, including the need for the order, warrant, or authorisation to be in the public interest having regard to the importance of the information;
- A strict prohibition on any order or warrant authorising the disclosure or seizure of legally privileged material; and
- A requirement that a warrant is sought for the ongoing retention of any journalistic material which is seized during a search that has been authorised under the urgent procedure.

Extraterritorial Jurisdiction and significant link to the UK

Issues raised

In the consultation the Government sought views on whether the jurisdiction of the espionage offence should be expanded to cover activities taking place overseas regardless of a person's nationality. It also sought further input on the Law Commission's recommendation that there should be a "significant link" between the individual's behaviour and the interests of the UK.

Many of the responses on this area related to concern that an approach to extraterritorial jurisdiction modelled on there being a significant link would impact journalists and whistle-blowers – this is covered in further detail above. Concern was also raised about the enforceability of extraterritorial jurisdiction.

Government response

Technological developments have enabled espionage to be conducted from a foreign state with greater ease, with the UK's assets and interests often targeted. For the legislation to be as effective as possible it is important that the legislation deters and allows us to address overseas activity.

The existing provisions do not capture activity conducted by non-British nationals operating in a foreign state. Expanding the existing extraterritorial jurisdiction means that we would be able to capture activity conducted against the UK from abroad, regardless of that person's nationality.

The recent case of an individual working in the British Embassy in Berlin being extradited and charged under the existing legislation shows the importance of extraterritorial jurisdiction. These reforms will enable us to act should a non-British employee of the Government abroad

carry out similar activity, as well as take action against those who act against the UK from overseas through modern vectors such as cyber.

The Government considers that expanding extraterritorial jurisdiction is necessary to defend the UK against the modern espionage threat, the global nature of which is not reflected in the current provisions. Although there may be practical challenges investigating and enforcing offences committed abroad, there will be cases where this is possible. Furthermore, in instances where it is not possible, an extant arrest warrant can severely limit an individual's ability to travel either to the UK or countries where the UK has extradition treaties in place: this would be an effective form of disruption against hostile actors.

For the majority of offences in the Bill where extraterritoriality applies, the activity must be conducted with a purpose or in a way that is prejudicial to the UK's safety or interests. That requirement creates the requisite link back to the UK. In cases where the activity being prejudicial to the safety or interests of the UK is not a core part of the relevant offence the legislation makes clear the link to the UK that needs to be made out in that case. For example, in the case of the obtaining and disclosing of trade secrets an offence will only take place abroad if some of the conduct takes place in the UK or the trade secret is in the possession of or control of a UK national or company.

Need for new offences

Issues raised

The consultation also considered 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 was a case for new standalone offences to cover other hostile activity including: sabotage, economic espionage and foreign interference.

Few responses were received with respect to new offences, and most responses were insufficiently detailed to draw firm conclusions about whether new offences were considered to be required. Moreover, while the balance of responses was against creating new offences, we have balanced this against the clear case for reform presented by our police and intelligence agencies.

Government response

As set out above, the Government has sought to create a suite of offences to replace the existing espionage laws.

In addition to reforming the Official Secrets Acts 1911-1939, the Government's legislative proposals include new measures to tackle the modern threat from hostile actors connected to foreign powers. These modern tools and powers will protect the UK's world-leading innovation and research across a wide range of sectors and industries, as well as our democratic system, strategic interests, and way of life.

The UK is a leader in innovation in a number of important industries such as defence, research and development, academia and technology. Promoting this innovation allows new ideas to be formed which meet the needs of consumers and tackle societal challenges. Recognising that state actors are increasingly seeking to undermine the UK's competitive and strategic advantage, and gain valuable information by targeting trade secrets, we are creating a new Protection of Trade Secrets offence to deter and disrupt those who steal sensitive intellectual property or attempt to undermine UK innovation. The offence will specifically target the illicit acquisition or disclosure of sensitive trade, commercial or economic information, the value of

which is directly linked to its secrecy. The offence will be committed if the conduct in question is linked to a foreign power.

We know that, in extreme situations, some state actors will not stop short of attacking critical UK infrastructure, information, or property. We will therefore create a new offence of sabotage designed to capture state-linked saboteurs who act in a way that is prejudicial to the UK's safety or interests by causing damage, including through cyber-attacks, to assets (including critical infrastructure, electronic systems, and information).

Foreign Interference 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. It 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. The Government has proposed a new foreign interference offence where the foreign power condition is met, the purpose of the activity is to interfere with protected rights, public functions, or services, political or legal processes, or prejudice UK safety or interests, and the activity is carried out in an illegitimate way, for example in a coercive or deceptive way.

As part of our efforts to deter foreign interference, the Government is also increasing the maximum penalties available for certain election-related offences that are carried out for, or on behalf of, a foreign power.

Preparatory conduct and legitimate activity

Issues raised

Some responses to the consultation raised concern about the potential breadth of a preparatory conduct offence in the context of state threats and its usefulness in practice. One of the challenges posed in the responses was around how there was no clear justification for expanding the remit of the offence to cover other harmful state threats activity and that, despite technological advances, the current law is broad enough. One respondee also highlighted the need for safeguards for an offence of this nature.

Government response

The need to capture preparatory activities is a concept which is recognised, both in the existing espionage legislation and in terrorism legislation, where there is an 'acts preparatory' offence which links to a definition of terrorism. The offence is a valuable tool in terrorism legislation and there have previously been prosecutions under the offences in existing state threats legislation. As with terrorism, the Government considered there is a need to have an offence which allows activity to be disrupted before damage is done.

The Bill therefore includes a preparatory conduct offence which provides an important tool which will prevent threats to our national security by criminalising preparatory conduct carried out in preparation for four specified offences in the Bill or other extremely harmful activity carried out for, on behalf of, or with the intention to benefit a foreign power. It is essential that we have the ability to disrupt state actors who are preparing to carry out the relevant acts before they cause significant and potentially irreversible harm to the safety and interests of the UK.

For the offence to be made out, there must be evidence to demonstrate, beyond reasonable doubt, that there was an intent to carry out an act which could constitute a relevant offence under the Bill (or other specified harmful activity on behalf of a state). In all cases this includes

a condition either that the activity is carried out for, on behalf of, or with the intention to benefit a foreign power, or with a purpose prejudicial to the safety or interests of the UK (or both).

Scope of prohibited places regime

Issues raised

A suggestion was provided in a consultation response that all sensitive sites in the UK, including military bases, sites belonging to the intelligence services and all other sensitive areas should be designated as such and photography of, and trespass on these sites should be criminalised, with safeguards should be put in place to prevent an overreach of powers regarding photography.

Government response

The prohibited places provisions in the Official Secrets Act 1911 play an important role in our existing arsenal to counter state threat activity by protecting the UK's most sensitive assets. The reforms included in the Bill will ensure that they continue to play this role by further enhancing their utility in order to better meet the modern-day threat. Simply put, if these sites are not afforded sufficient protection against those seeking to conduct harmful activity, this will have an impact on the safety of the UK.

By creating new offences and police powers to capture harmful activity in and around the UK's most sensitive sites, we make it more difficult for hostile actors to achieve their objectives and provide additional disruptive tools to be employed. The prohibited places regime supports the other provisions in the Bill and provides disruptive measures to prevent harmful activity being conducted before it takes place.

In designing the prohibited places regime, we have focussed on modernising the list of sites that will be prohibited places and ensuring that we have a designation power that enables us to designate sites most likely to be vulnerable to state threats. The reforms will also capture the range of modern methods to access, enter or inspect prohibited places, including through the use of unmanned devices (such as drones capable of physically entering or inspecting a site) and through cyber means (such as someone hacking into the CCTV feed of a prohibited place).

In developing the modernised regime, we have ensured that the legislation is targeted at the right activity. Two separate offences have been created. The first is offence focussed on the broad range of harmful activities that can be carried out in relation to a prohibited place including access onto the site, being in the vicinity of the site and inspecting the site – including through taking photographs. For this offence to be made out the person would need to be acting with a purpose that they know, or reasonably ought to know, is prejudicial to the safety or interests of the UK. This high bar ensures that it does not cover individuals innocently being in the vicinity of the site.

The second offence addresses those who are on or inspecting a prohibited place without authorisation. It is more limited in its scope as it does not apply to being in the vicinity of a site, for example, and it requires the person to know, or ought to have known, that their conduct was unauthorised. Accordingly, a person would not commit this offence if they, without a purpose prejudicial to the safety or interests of the UK, entered, or took a photograph of, a site and there was no reason for them to know this was not permitted.

In addition to these offences the legislation provides powers to the police to order a person not to engage in certain conduct where they believe doing so is necessary to protect the safety or

interests of the UK, for example, requiring a person to move away from a prohibited place. These can be used by the police to intervene in a proportionate way to manage the risks on or around sensitive sites.

Sentencing and investigation

Issues raised

While there was little comment provided in relation to sentencing and investigation, a point was raised that enhancing law enforcement and intelligence agencies' ability to investigate the threats was more important than increasing sentencing.

Government response

The Government considers that increasing the maximum penalties available to the courts is an important part of ensuring that the legislation provides an appropriate and robust response to the threat. The Bill contains a range of offences with the maximum penalty dependent on the nature of the conduct and the harm that could flow from it. For example, in the most extreme cases, serious harm, including loss of life, can arise from the obtaining and disclosing of protected information. These harms can be equal to or, in the most extreme circumstances, greater than offences in wider legislation which carry a maximum penalty of life imprisonment. We have reformed the penalties provided in this offence to bring these provisions in line with modern standards set by wider provisions.

The Government agrees, however, that it is vital that the offences in the Bill are accompanied by the tools required by the intelligence and law enforcement agencies to effectively investigate harmful activity. Many of those who conduct state threats activity in the UK are highly capable individuals and are often backed by foreign powers who are intent on causing significant harm in the UK.

Accordingly, The National Security Bill introduces a range of provisions which provide police with the investigative tools they need to successfully counter state threats activity.

The new powers emulate many existing tools already available to the police for terrorism investigations. The new powers therefore create parity in the national security system by ensuring that the police have the equivalent tools for state threats cases, which have shown to be effective in detecting and preventing terrorism.

The police powers are available for investigations into people who are suspected to be involved in foreign power threat activity. This is defined in the legislation and includes state threats offences such as espionage, sabotage and assisting a foreign intelligence service. The powers are also available for investigations into other acts where the foreign power condition is met which involve serious violence against another person, endanger the life of another person, or create a serious risk to the health or safety of the public.

SECTION 2: State Threats Prevention and Investigation Measures

Introductory remarks

In recognition of the fact that there may be cases where prosecution is not possible and it is not feasible to otherwise disrupt individuals considered to be involved in highly damaging threat activity on the behalf of states, the consultation also sought views on the case for inclusion of a power of last resort that would enable it to impose a range of restrictions on particular individuals. These will be civil measures called State Threats Prevention and Investigation Measures (ST-PIMs)

We have broken down respondees' views on ST-PIMs into three themes, which are summarised and responded to below.

The scope and benefits of civil measures

Issues raised

There were several comments on the need for more detail and clarity on the proposed framework's scope, legal tests and the available restrictions before further comments could be made. However, a number of respondees questioned the likely utility of civil measures and the principle of imposing intrusive restrictions on an individual outside the criminal justice process.

Other questions submitted in response to the consultation covered how long the measures could be imposed for, the checks and balances included and how the measures would be enforced. There was also a query received around whether these measures would replicate powers under sanctions and anti-money laundering legislation.

Government response

We understand why respondees were seeking more detail and clarity on these proposals. We expect ST-PIMs, as is the case with Terrorism Prevention and Investigation Measures (TPIMs), to be used sparingly and as a measure of last resort, providing operational partners with a tool to mitigate the threat posed by those engaged in high threat foreign power threat activity where there are no other options available. These measures will not replicate powers under sanctions and anti-money laundering.

Restrictive civil measures are used, and found to be effective, in a range of contexts (e.g. counter-terrorism, serious crime prevention, sexual offence prevention, anti-social behaviour prevention etc) to reduce the risk posed by an individual in a situation where they may be engaged in activity that could result in an offence or harmful activity or following conviction of an offence to prevent a further related offence being committed. Given such tools are available, accepted and found to be effective in other contexts, the Government assesses that there is a strong justification for considering their application for state threats. in a foreign power threats context.

As with TPIMs, the proposal is that the authority to impose a ST-PIM and the measures under it, will rest with the executive. The measures sit outside the criminal justice system because they are preventative rather than punitive and require a quick response to deal with the threat. ST-PIMs will be used to deal with live operational cases which could present imminent threat to the UK and so the Government must be able to act quickly. Notwithstanding this, robust safeguards exist to guard against any abuse, and these are outlined in the next section.

The decision-making process and safeguards in place to govern the use of the measures

Issues raised

Some respondees questioned the appropriateness of the executive being given the power to impose civil measures, rather than the judiciary, as imposing a civil measure would grant significant powers to the Government.

Other comments queried the individual's right to appeal and whether sufficient evidential justifications would be provided to ensure individuals who are subject to a civil measure would be fully aware of the reasons as to why it has been imposed and have an opportunity to challenge the imposition of these measures. A few respondees queried the rationale for imposing measures on individuals if they are unable to be prosecuted. There was also concern about the potential for arbitrary or politically motivated use of the powers and questions around whether they are proportionate and compatible with human rights legislation. Respondees also highlighted the importance of legal checks and balances to govern the use of civil measures as well as an oversight mechanism. One respondee emphasised the importance of focusing on the prevention of foreign power threat activity, rather than punitive measures.

Government response

We have set out further detail below about the ST-PIMs framework and the range of safeguards in place to guard against abuse.

The proposed framework would largely mirror that of TPIMs, which have been in place for a decade and have proved an important measure for preventing and restricting engagement in terrorism-related activity. The courts have upheld the compatibility of the TPIM regime with human rights legislation and have never determined that a TPIM in its entirety should not have been imposed by the Secretary of State. This precedent gives us confidence in taking a similar approach to the framework for ST-PIMs. Individuals who are subject to a civil measure will have the opportunity to apply for legal aid should they so wish.

Although the executive will be responsible for making the decision to impose a ST-PIM, the High Court will also have a role to play in terms of granting permission to the executive. Without this permission, the executive will not be able to impose the measure. This will ensure that the power is not open to abuse.

Before making an application for permission to impose a ST-PIM on an individual, the Secretary of State would be required to consult the chief officer of the appropriate police force about whether there is evidence available that could realistically be used for the purposes of prosecuting the individual for an offence. It may not be possible to prosecute an individual for the following reasons:

- either the investigation is at an early stage and disruptive action is needed to prevent serious harm; or
- disclosure of relevant evidence as required in a criminal trial would be damaging to national security.

It is in these circumstances that ST-PIMs will be helpful to mitigate the threat posed from those engaged in foreign power threat activity where there are no other options to mitigate the threat.

Under the proposed legislative framework, the Secretary of State will only be able to impose a ST-PIM if five conditions are met:

i. The Secretary of State must reasonably believe that an individual is, or has been, involved in foreign power threat activity (Condition A). This would include (the commission, preparation or instigation, or facilitation, support or assistance of) activity that could amount to an offence of obtaining or disclosing protected information or trade secrets, accessing a prohibited place for a purpose prejudicial to the safety or interest of the UK, sabotage, foreign interference or assisting a foreign intelligence service; or the following acts or threats of acts where the foreign power condition is also met : a) involve serious violence against another person, b) endanger the life of another person, or c) create a serious risk to the health and safety of the public or a section of the public.
ii. Some, or all, of the activity is new (Condition B).
iii. The Secretary of State will also be required to reasonably consider that imposition of the ST-PIM is necessary to protect the UK from threats from foreign powers (Condition C).
iv. That the individual measures applied are necessary to prevent or restrict the individual's involvement in foreign power threat activity (Condition D).
v. In all but the most urgent cases, before the ST-PIM can be imposed, the court must review the decision of the Secretary of State to determine whether it is obviously flawed and grant permission to impose (Condition E).

There will be a number of safeguards in place to govern the operation of ST-PIMs to ensure that they are not used arbitrarily and are compliant with the European Convention on Human Rights:

i. As part of the conditions for imposing a ST-PIM Measure, the Secretary of State must have obtained the permission of the court;
ii. The Secretary of State must consult with the police over whether a prosecution for an offence is possible in the first instance;
iii. The imposition of a ST-PIM would automatically trigger a review, to be heard on judicial review principles, which would require the court to review the decisions of the Secretary of State to ensure the relevant conditions were met and continue to be met;
iv. The individual concerned would have the right to appeal to the court against an extension or revival of their civil measure; or against a Secretary of State decision on the individual's application for a variation or revocation of the measures; or against a Secretary of State decision on the individual's application for permission in relation to the measures imposed;
v. A requirement for the Secretary of State to review the ongoing necessity of the measures;
vi. ST-PIMs can only be imposed for a period of one year. There would be the possibility of seeking a one-year extension if the conditions of necessity and proportionality continue to be met. Such an extension could be made up to four times, which would mean the maximum duration an individual could be subject to a ST-PIM is five years; and
vii. A requirement for the Secretary of State to report on the exercise of the powers every three months, as well as a requirement for an independent reviewer to report on the operation of the powers which would be laid before Parliament each year.

Protecting journalists and whistle-blowers

Issues raised

Some respondees raised concerns that civil measures could have a negative impact on

journalistic freedoms if the restrictions were used to prevent a journalist communicating with their sources. There were also concerns that the proposals may intimidate journalists from reporting on items of public interest for fear of facing repercussions. Some respondees believed that the measures could be used to restrict free speech or prevent legitimate whistleblowing. Others were concerned about the potential for a "chilling effect" on rights enjoyed by citizens.

Government response

Journalists will, rightly, always remain free to hold the Government to account. We are clear press freedom is an integral part of the UK's democratic processes. We are committed to the continued protection of privacy, press freedoms and freedom of expression and ensuring that protection of national security is balanced with the protection of the important individual rights and values we all enjoy in the UK.

Multiple safeguards already exist for Government whistle-blowers, including members of the security and intelligence agencies, where concerns can be raised and investigated without requiring an unauthorised disclosure to be made.

SECTION 3: Foreign Influence Registration Scheme

Introductory remarks

In our consultation paper, we indicated that the Government saw the creation of a Foreign Influence Registration Scheme as an important part of the package of measures to combat state threats. We sought views to help develop the design of a government-managed register of declared activities that are undertaken for, or on behalf of, a foreign state. In particular, the consultation sought views to ensure the scheme would deliver the most value for the individuals, organisations, and sectors most likely to be in scope, by being practical, accessible, and protecting their interests.

The responses reflected in the following paragraphs were received from a range of stakeholders including those representing media, legal, academia and research sectors. They have been broken down into the following three key themes.

Overall reflections on the proposal and experience of existing schemes

Issues raised

Several respondees reflected on their experience of the U.S. Foreign Agent Registration Act (FARA) 1938 and the Australian Foreign Influence Transparency Scheme (FITS) Act 2018. These are existing registration schemes designed to increase transparency around activities seeking to influence political and public affairs for, or on behalf of, a foreign principal. Those respondees highlighted the importance of ensuring any new registration obligations are a proportionate means of addressing the specific harms identified. Respondents said that a key part of this would be to make sure that the obligations themselves do not impose an undue burden on prospective registrants. Some respondees cited the U.S. FARA as an example of a scheme that requires extensive registration paperwork and supporting documentation.

A number of respondees acknowledged the importance of making the UK a harder operating environment for undercover foreign intelligence officers and their agents, to protect their sectors against malign activity. Some respondees cautioned, however, that such a scheme would require a strong public communications strategy and clear guidance to avoid the risk of individuals or organisations being unfairly stigmatised for complying with the scheme's requirements and appearing on a publicly accessible register.

Several responses sought further clarity on what value a UK scheme would add over and above existing legislation and regulation, including the Lobbying Act 2014 and the National Security and Investment Act 2021. They sought reassurance that the scheme would not create duplication for sectors that already comply with wider government policies. Some responses suggested amending existing legislation to deliver the policy intent.

While the majority of respondees were supportive of the principle of tackling state threats, there was clear recognition that a UK scheme would need to strike the right balance between delivering the policy intent and the need to protect those engaged in legitimate activity from disproportionate compliance and reputational costs. Some respondees wanted more information about how a scheme would deliver the policy objective of providing an alternative and earlier means of disruption and highlighted possible evidential challenges in proving an offence of failing to comply with any scheme's requirements.

Scope of the requirements

Issues raised

A number of respondees sought further detail on how an arrangement between a foreign state and an individual would be defined for the purposes of registration. This was identified as a critical term that would likely determine the volume of individuals and activities which are found to be within scope of the scheme. These responses cautioned that if defined too widely, the volume of potential registrants could become difficult to manage from an administration perspective but would also risk a 'chilling' impact on key UK sectors including research, media, and academia.

Several responses focused on how the scope of the scheme could be refined to ensure the requirements are more targeted and proportionate. Firstly, a number of respondees suggested that the scope of the scheme could be reduced by making the requirement to register applicable to activity undertaken for countries that are of most concern to the UK from a state threats perspective. This would deviate from the state-agnostic approach taken internationally and reduce the potential impact on those that are engaged in legitimate activity and are less likely to pose a threat to the UK. Secondly, some respondees suggested that it may be more practical to permit organisations and entities to register, rather than requiring every individual to register their activity. This may significantly reduce the compliance burden, particularly where arrangements and activity involve large numbers of people working together for a single organisation. Finally, there were several suggested exemptions across multiple sectors, including for legal professionals and journalists, with respondees citing parallels under FARA and FITS.

The process of registration and public register

Issues raised

Several respondees asked about how new registration obligations would work and the associated practicalities of supplying required information. They advised that a burdensome, ambiguous, and duplicative scheme could slow the free exchanges of information and to disincentivise international collaboration.

A number of respondees sought further clarity on the policy intention behind a suggested publicly accessible register. Firstly, some respondees sought assurance that the register would comply with data protection legislation and the extent to which an individual's personal information would be made public. Secondly, one respondee queried whether a public register could be used to benefit our adversaries and those engaged in state threats activity. A related concern was raised that individuals could be vulnerable, not only to foreign states, but to criticism or attacks by the media, opposition groups or online communities as a result of publicising their engagement in activities for foreign states.

A further suggestion was made that an individual or organisation should be notified that they are required to register, as opposed to immediately being liable to prosecution for not registering. A related suggestion was that there should be a mechanism for an individual to challenge a direction or obligation to register.

Government response and next steps

We have noted all views put forward and they have been taken into account in considering the development of a UK scheme.

We continue to assess that such a scheme would add strength to the UK's response to state threats and we will bring forward proposals requiring the registration of certain arrangements

with foreign governments to deter and disrupt state threats activity in the UK. This will bring the UK into line with similar schemes of our allies. The scheme will be brought forward by government amendment to the National Security Bill as soon as possible.

Russia's actions to undermine European stability have brought the need for such a scheme into sharp focus and we are taking the time to review its requirements to ensure their effectiveness and proportionality. It is important to ensure the scheme's requirements will provide an effective tool in deterring and disrupting state threats activity.

A consistent message from respondees to this consultation was that a UK scheme must strike the right balance between highlighting foreign influence in the UK and protecting those involved in legitimate activity from disproportionate compliance and regulatory costs.

The Government recognises the importance of international collaboration across UK sectors and the scheme will not halt or obstruct such collaboration. We do not intend the scheme to create unnecessary barriers or to deter those engaged in legitimate activities with foreign states in the UK.

We will bring the scheme forward by government amendment to the National Security Bill as soon as possible.

SECTION 4: Additional questions for consultees (treason reform)

Introductory remarks

In the consultation, we also sought input on any other additional tools and measures which could be introduced or whether there is any existing legislation which could be amended or updated to address the threat.

Some respondees said they did not think there are any other additional or reformed tools or powers that could be utilised to address the threats. We have balanced this view against the clear requirements presented to us by our police and intelligence agencies.

One additional measure which some respondees provided views on was treason reform.

We have reflected on the issue of treason reform and have determined that its complexity, coupled with the wide range of views on the subject, warrant further study. We are working to consider the next steps for review of this area of law.

Treason Reform

Issues raised

A small number of responses were in favour of treason reform. One respondee said treason reform is overdue. Another said treason should be reformed to capture non-TACT offences which cause significant harm to the UK or its interests. Another referenced the Policy Exchange's 2018 paper entitled 'Aiding the Enemy' saying that it stated a very strong case for treason reform. In other references to treason, a small number said that treason reform did not need reforming, with one commenting that treason laws already meet the UKs security requirements.

Government response

As reflected in the diversity of respondees' views, reform of treason legislation is a complex and technical undertaking, and a vast amount of resource would be required to undertake wholesale treason reform, as all of the UK's archaic treason legislation tracing back to 1351 would need to be examined and potentially modified, repealed, or replaced. Significant historical analysis would need to occur to enable reform of treason and that would have significantly delayed this Bill, had we proceeded with reform as part of the legislative proposals to counter state threats.

The Government's view is that many of the harms that treason legislation was intended to address are now covered by modern legislation and this Bill will further strengthen the UK against harmful threats to our security.

However, we also consider that work should continue to consider the future role of treason law. To inform our longer-term approach, the Government have engaging with the Law Commission regarding the possibility of them undertaking a review in this area to inform next steps.

SECTION 5: Official Secrets Act 1989 reform

Introductory remarks

This section focuses on responses to the Law Commission's recommendations relating to provisions which criminalise individuals for disclosing official information without authorisation, under the Official Secrets Act 1989.

While it is undeniable that the world has changed since the OSA 1989 was first passed, it is clear to us that reform is complex and engages a wide range of interests. With that in mind the Government has decided not to legislate on OSA 1989 reform at this time. It is only right that proper, due consideration should be given to the concerns (as detailed below) raised in the consultation.

It is important that our work runs in lockstep with other crucial work the Government is doing to strengthen whistle-blowing practices and transparency. This includes consideration around reforming Misconduct in Public Office offences, the operation of which has also been reviewed by the Law Commission, and the recommendations of the Boardman Review on how the Government can improve the processes for individuals to raise a concern.

Issues raised

The dominant theme across all questions from respondees was concern over journalistic freedom, whistle-blowing processes, proposals to provide proof or likelihood of damage as the result of an unauthorised disclosure and safeguarding the ability for information, which was judged to be in the public interest, to be disclosed.

Many respondees indicated they were against 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 OSA 1989, instead of a damage requirement. There were also several comments on the prospect of higher sentences targeted at journalists and investigative journalists. Many respondees indicated they were opposed to longer sentencing for OSA reforms. Respondees were in favour of a distinction in sentencing between those making unauthorised disclosures and those making onward disclosures of that material.

Many of the responses to the consultation support the Law Commission's recommendation for a Public Interest Defence (PID) to be inserted into the OSA 1989, as part of a package of reforms which would strengthen that legislation, to act as a safeguard against the Act being misused by the Government to cover up wrongdoing and embarrassing mistakes.

Another view provided to the consultation was that it would be preferable to not amend OSA 1989 at all.

Government response

We have listened to the views raised in response to our public consultation and our response to the Law Commission's recommendations on reforms to the OSA 1989. The OSA 1989 is an essential part of our ability to protect national security and information, which, if improperly handled by those entrusted with it, could cause real harm to our national security. This legislation also has relevance for the values that we hold dear, such as freedom of expression and therefore it is important that we carefully consider any reform in context and consider the strong views and concerns raised. It is important to make clear that the Government will always remain committed to ensuring the right balance is struck between the freedom to

publish information that is in the public interest and the need to protect against serious harm to the UK and its citizens if information is disclosed in a damaging way.

We similarly have heard the strong views regarding the efficacy of the existing safeguards in the OSA 1989 to prevent its misuse, most notably the requirement for the Government to prove damage of an unauthorised disclosure when prosecuting an individual for the vast majority of OSA 1989 offences. the Government recognises the importance of maintaining this existing safeguard.

To enable wrongdoing to be exposed safely while ensuring that the Act remains workable to protect UK national security, the focus should be on making sure that individuals can make disclosures in a safe way, for instance through proper, protected routes for making an authorised disclosure. The Government is committed to ensuring that these routes are clear and accessible to individuals across government. Therefore, the Government is updating guidance for government departments and bodies to ensure that there are safe and effective whistle-blowing routes available to all current and former staff and contractors who may wish to raise a concern.