

Title: Investigatory Powers Bill: Overarching Impact Assessment IA No: HO0234 Lead department or agency: Home Office Other departments or agencies: FCO, Cabinet Office, MOJ, CPS, MOD, HMRC, MI5, SIS, GCHQ, NCA, wider law enforcement, other public authorities	Impact Assessment (IA)		
	Date: 7 July 2016		
	Stage: Final		
	Source of intervention: Domestic		
	Type of measure: Primary legislation		
Contact for enquiries: investigatorypowers@homeoffice.gsi.gov.uk			

Summary: Intervention and Options

RPC Opinion: Green

Cost of Preferred (or more likely) Option			
Total Net Present Value	Business Net Present Value	Net cost to business per year (EANCB on 2009 prices)	In scope of One-In, Measure qualifies as Two-Out?
-£247.5	£0m	£0m	No
			NA

What is the problem under consideration? Why is government intervention necessary?

The legislation that governs the use of investigatory powers by the security and intelligence agencies, armed forces and law enforcement is spread out over a number of statutes and requires updating. New legislation is required to update and modernise the use of investigatory powers, apply greater safeguards and oversight and to prevent the degradation of the capabilities of law enforcement, armed forces and the security and intelligence agencies necessary to protect the public and to keep us safe. The Data Retention and Investigatory Powers Act 2014 is subject to a 31 December 2016 sunset clause and legislation is necessary to ensure a legislative basis for these powers and oversight arrangements

What are the policy objectives and the intended effects?

To provide a clear and transparent framework for the exercise of investigatory powers by the security and intelligence agencies, armed forces and law enforcement, with greater oversight and safeguards. To consolidate existing legislation into a concise and comprehensive Act that will improve public understanding of the need for, and the use of, these important and sensitive capabilities. To modernise and update the legal framework to ensure the security and intelligence agencies and law enforcement can continue to exercise the capabilities they need to maintain public safety and protect us from terrorism, and serious crime including cyber-crime, human trafficking and child sexual exploitation.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

Option one, do nothing: The capability gap for law enforcement in respect of communications data remains. Investigatory powers remain spread out over a number of statutes.

Option two, re-legislate for investigatory powers and clarify the existing legal framework for investigatory powers, including interception, communications data and equipment interference, the safeguards for security and intelligence agencies' use of bulk personal datasets, and the retention of communications data, including additional retention of internet connection records, increasing oversight and providing for judicial approval of warrants.

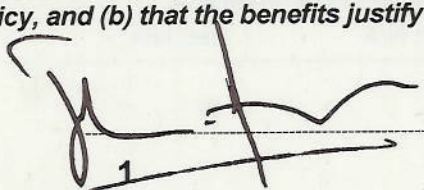
Option two is the preferred option as it meets the required policy objectives.

Will the policy be reviewed? It will be reviewed. If applicable, set review date: December 2022

Does implementation go beyond minimum EU requirements?			N/A		
Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base.	Micro	< 20	Small	Medium	Large
	No	Yes	Yes	Yes	Yes
What is the CO ₂ equivalent change in greenhouse gas emissions? (Million tonnes CO ₂ equivalent)			Traded:	Non-traded:	
			N/A	N/A	

I have read the Impact Assessment and I am satisfied that (a) it represents a fair and reasonable view of the expected costs, benefits and impact of the policy, and (b) that the benefits justify the costs.

Signed by the responsible Minister:

 Date: 7/7/16

Summary: Analysis & Evidence

Policy Option 1

Description: Do nothing

FULL ECONOMIC ASSESSMENT

Price Base Year 2016	PV Base Year 2016	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: 0	High: 0	Best Estimate: 0

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	0	0	0
High	0	0	0
Best Estimate	0	0	0

Description and scale of key monetised costs by 'main affected groups'

The 'do nothing' option is the baseline, and the agencies, armed forces and law enforcement would continue to exercise the existing powers proposed in the draft Bill under the current statutory basis. Therefore costs and benefits are zero.

Other key non-monetised costs by 'main affected groups'

The 'do nothing' option is the baseline and therefore costs and benefits are zero.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0	0	0
High	0	0	0
Best Estimate	0	0	0

Description and scale of key monetised benefits by 'main affected groups'

The 'do nothing' option is the baseline and therefore costs and benefits are zero.

Other key non-monetised benefits by 'main affected groups'

The 'do nothing' option is the baseline and therefore costs and benefits are zero.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5
-------------------------------------	-------------------	-----

That the data retention regime would not be allowed to lapse. No changes would be made to the oversight and authorisation regimes and legislation would remain spread over a number of Acts. The agencies, armed forces and law enforcement would continue to exercise their existing powers to conduct equipment interference (and bulk powers in respect of the agencies) under existing statutory bases. A gap would still remain in capabilities to gain access to electronic communications to progress investigations.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			In scope of OIOO?	Measure qualifies as
Costs: N/A	Benefits: N/A	Net: N/A		
			No	NA

Summary: Analysis & Evidence

Policy Option 2

Description: Legislate comprehensively for investigatory powers

FULL ECONOMIC ASSESSMENT

Price Base Year 2016	PV Base Year 2016	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: N/K	High: N/K	Best Estimate: -

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	169.1	13.7	242.6
High	171.1	14.3	249.7
Best Estimate	170.42	14	247.5

Description and scale of key monetised costs by 'main affected groups'

A small cost associated with increased compliance, reporting and safeguards to the agencies, law enforcement and other public authorities. A minimal cost to the justice system for offences and changes to the Investigatory Powers Tribunal. A large cost to Government Departments associated with the establishment of the Investigatory Powers Commission and authorisation of warrantry. A large cost associated with the ongoing running costs, compliance and reimbursement to business of costs associated with new communications data provisions.

Other key non-monetised costs by 'main affected groups'

Greater transparency of the investigatory powers available to the state to tackle crime and conduct investigations may result in greater use of obfuscation techniques by criminals, making it more difficult for the agencies and law enforcement to protect the public.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	N/K	N/K	N/K
High	N/K	N/K	N/K
Best Estimate	N/K	N/K	N/K

Description and scale of key monetised benefits by 'main affected groups'

Benefits have not been quantified.

Other key non-monetised benefits by 'main affected groups'

Increased detection and prevention of crime, safeguarding of the general public and a likely reduction in threat to individuals from terrorism. Greater transparency, and public understanding of the use of investigatory powers, including public confidence in the oversight of investigatory powers and the accountability of those who may use them.

Key assumptions/sensitivities/risks	Discount rate (%)
Technical complexity can increase projected costs. There is also a risk that technical solutions will be outpaced by technical change and/or changes in consumer behaviour. Continued use of powers available currently to the agencies and law enforcement under existing statutory bases provided for under the Investigatory Powers Bill.	3.5

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:	In scope of OIOO?	Measure qualifies as
Costs: 0 Benefits: 0 Net: 0	No	NA

Evidence Base

A. Strategic Overview

A.1 Background

The Data Retention and Investigatory Powers Act 2014 (DRIPA) was a fast-tracked piece of legislation responding to a ruling by the Court of Justice of the EU (CJEU) that the EU Data Retention Directive was invalid. DRIPA forms the basis for the UK's data retention regime, but is subject to a December 31 2016 sunset clause. DRIPA also clarified the application of the UK's legislation (the Regulation of Investigatory Powers Act 2000) to communication service providers. During the passage of that legislation, the Government committed to a review of investigatory powers by the Independent Reviewer of Terrorism Legislation, David Anderson QC. Two other reviews were carried out in parallel. The Intelligence and Security Committee of Parliament (ISC) looked into the activities of the security and intelligence agencies and published a report in March 2015, and the Royal United Services Institute (RUSI) established a panel to review the impact on civil liberties of Government surveillance which concluded in July 2015. David Anderson's report was published in June 2015.

All of the reviews concluded that the legislative framework for investigatory powers needed to be updated and modernised, to make clearer the statutory basis for their use. Existing legislation governing the use of investigatory powers is spread over a number of Acts, including but not limited to, the Regulation of Investigatory Powers Act 2000 (RIPA), the Telecommunications Act 1984, the Wireless Telegraphy Act 2006 (WTA), the Police Act 1997, the Intelligence Services Act 1994 (ISA), the Anti-Terrorism, Crime and Security Act 2001 (ATCSA), the Security Services Act 1989 (SSA), and the Counter-Terrorism and Security Act 2015 (CTSA) as well as the Data Retention and Investigatory Powers Act 2014 (DRIPA).

The principal recommendation made by David Anderson was:

'1. RIPA Part I, DRIPA 2014 and Part 3 of the CTSA 2015 should be replaced by a comprehensive new law, drafted from scratch, which:

- (a) Affirms the privacy of communications;*
- (b) Prohibits interference with them by public authorities, save on terms specified;*
- (c) Provides judicial, regulatory and parliamentary mechanisms for authorisation, audit and oversight of such interferences' (A Question of Trust, pg. 285)*

The speed of technological change has increased rapidly over the last sixteen years since the enactment of RIPA. The use of cloud computing has made it easier to enter the market and provide new services, while the increase in encryption has made it more difficult for law enforcement, armed forces and security and intelligence agencies to access, where necessary and proportionate, the content of communications and communications data. The use of electronic communications has grown: the Office of National Statistics reported 74% of adults in 2015 had used the internet 'on the go' using a mobile device. Investigatory powers are a vital tool in the detection and prevention of terrorism and crime, such as cyber-crime, human trafficking and online child sexual exploitation. Without legislating to modernise the legal framework for the use of investigatory powers by law enforcement and the security and intelligence agencies, capabilities will continue to degrade.

David Anderson went further to recommend:

- '3. The new law should be written so far as possible in non-technical language*
- 4. The new law should be structured and expressed so as to enable its essentials to be understood by intelligent readers across the world' (A Question of Trust, pg. 285)*

The report of the Intelligence and Security Committee of Parliament concluded that the security and intelligence agencies do not seek to circumvent the law, but seek rigorously to comply with it. However, the legislation could be made clearer and more transparent to increase public understanding of what the agencies and law enforcement can and cannot do.

Without introducing new legislation, law enforcement and the security and intelligence agencies will continue to operate within the bounds of the law, but will see further erosion of the capabilities they rely upon to keep the public safe.

The draft Investigatory Powers Bill was published on 4 November 2015, and scrutinised by a specially convened Joint Committee of both Houses of Parliament. They published their findings on 11 February 2016. Two other Parliamentary Committees conducted parallel scrutiny: the Commons Science and Technology Committee and the Intelligence and Security Committee. They published their findings on 1 and 9 February respectively.

The Government considered all of the recommendations made in the three independent reviews and three reports on pre-legislative scrutiny before bringing forward revised proposals for legislation. A revised Investigatory Powers Bill was introduced in the House of Commons on 1 March 2016 and received its Third Reading on 7 June 2016. A number of amendments were made during the course of its passage through the House of Commons; these are captured below in Section D.

A.2 Groups Affected

- Government Departments (Home Office, FCO, MOD, MOJ, NIO, Cabinet Office, DCMS, BIS)
- SIAs (Security Service, Secret Intelligence Service, GCHQ)
- LEAs (National Crime Agency, the Police, HM Revenue and Customs, wider law enforcement)
- HM Courts and Tribunal Service
- Crown Prosecution Service
- HM Prison Service
- The Scottish Government
- The public
- The communications industry – telecommunication service providers.

A.3 Consultation

Within Government

All Government departments affected by the legislation were consulted in the policy-development process and the pre-legislative process. This included (but was not limited to) the Foreign and Commonwealth Office, Business Innovation and Skills, Department of Culture, Media and Sport, Ministry of Defence, the Attorney-General's Office, the Northern Ireland Office, the Cabinet Office and the Scotland Office

Public Consultation

All operational stakeholders affected by the legislation were consulted during the policy-development process and throughout pre-legislative scrutiny. This included the National Police Chiefs' Council, the NCA, MPS, Police Scotland, PSNI, the three security and intelligence agencies and others. Extensive engagement with communication service providers and industry groups, civil liberties, charities and victims' groups, legal experts and others took place throughout the development of the Bill and pre-legislative scrutiny. The Joint Committee, Science and Technology Committee and the Joint Committee on Human Rights issued calls for evidence. The Government considered carefully all the responses to those calls for evidence and the resultant reports where available as part of drawing up revised legislation.

B. Rationale

The Government must ensure that law enforcement, armed forces and the security and intelligence agencies have the powers they need to prevent terrorism and tackle serious and organised crime. Equally, the Government must ensure that the use of these powers is scrupulously overseen and subject to effective safeguards. It has a responsibility to ensure that the agencies that can exercise

these powers can be held to account for their activities, that they are transparent (while protecting sensitive techniques), and that there is public understanding as to what types of activity may be undertaken and in what circumstances.

The use of investigatory powers is vital to preventing and detecting all forms of crime and for the purpose of safeguarding national security. Such powers might be necessary for the location of a missing and vulnerable person, to exonerate a suspect of a crime, or to avert a terrorist attack

However, investigatory powers are by their nature intrusive, and their use must be subject to effective oversight and safeguards. Existing safeguards and oversight arrangements must be strengthened and made clearer. A clear expectation was set by the reviews undertaken by RUSI, the ISC and David Anderson that the Government should bring forward a comprehensive and comprehensible Bill that will provide a clear basis for the future use of investigatory powers. Furthermore, the Joint Committee convened to scrutinise the Bill said:

'Resolving the tension between privacy and effective law enforcement in this area is no easy task. The Home Office has now come forward with a draft Bill which seeks to consolidate in a clear and transparent way the law enabling all intrusive capabilities. The Committee together with the many witnesses who gave evidence to us, was unanimous on the desirability of having a new Bill' (page 5, Draft Investigatory Powers Bill Report)

C. Objectives

The objective of any legislative change is to update and modernise the legal framework for the use of investigatory powers, including the acquisition of communications data (targeted, and in bulk), the retention of communications data, the interception of communications (targeted, and in bulk), equipment interference (targeted, and in bulk) and the agencies' use of bulk personal datasets, as well as improvements to the oversight and safeguards that apply to these powers. The intended effect is to mitigate the erosion that technical change is having on the capabilities used by law enforcement, armed forces and the security and intelligence agencies. The intention is to make sure those capabilities can be used to protect the public but in a transparent way, with greater safeguards and controls on their use, and only where necessary and proportionate. Our objective is to improve public understanding and the ability of the agencies to lawfully detect, prevent and tackle terrorism and crime, including child sexual exploitation, fraud, human trafficking, cyber-crime, drug-trafficking and other harms. A key objective is to make clear where and how those powers can be exercised, with a new regime for the authorisation and oversight of them. It is also an objective to respond to the recommendations of the three independent reviews of investigatory powers, and the pre-legislative scrutiny reports of three Parliamentary committees.

D. Options

Option 1 is to make no changes (do nothing).

There is a general assumption that the data retention regime would not be permitted to lapse. No changes would be made to the authorisation and oversight regime and the legislation would remain spread over a number of Acts. All of the powers within the Bill in respect of interception, equipment interference and communications data – both targeted and bulk powers – would continue to be exercised under the existing statutory bases with existing safeguards applying. A gap would still remain in the ability of the agencies to gain access to the communications data required to progress investigations in an increasingly internet-based communications environment, and the capabilities of law enforcement would be further eroded over time.

Option 2 re-legislate for the use of investigatory powers by operational partners

This option would re-legislate for all the investigatory powers that are used by law enforcement, armed forces and the security and intelligence agencies in respect of the acquisition, retention and examination of communications. It would consolidate relevant provisions under RIPA Part I and sections of IV, DRIPA, CTSA, ATCSA, parts of the Police Act, WTA, and the Telecommunications

Act 1984 into a single, transparent and clear piece of legislation, and make apparent the safeguards and oversight that apply.

A powerful new Investigatory Powers Commissioner would be established, replacing the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner. The Commissioner would lead a new oversight body, which would review and approve warrants authorised by the Secretary of State before they are issued and audit the activities of the security and intelligence agencies, law enforcement and armed forces in respect of the powers in the Bill. It would be supplied with technical expertise.

The powers in the legislation would be more transparent and subject to greater safeguards, with codes of practice to illustrate the retention, handling, destruction and audit arrangements for material acquired under the power, for each of the powers within the Bill. The legislation would be clearer and have greater foreseeability so that the public better understands when and how these powers can be used, and so that public confidence in the accountability to the public and to Parliament of the exercise of the powers is increased.

An overview of the measures in the Bill is as below:

- **General protections**

The Bill will re-affirm the protection of privacy and the limited circumstances in which it is lawful to interfere with privacy. A new overarching privacy clause was included into the Bill as part of the Bill's passage through the Commons.

- **The acquisition of communications data**

The ability of law enforcement, armed forces and security and intelligence agencies to access and require the retention of communications data is eroding as communications change, including the ability to resolve IP addresses. The UK's data retention regime rests upon the Data Retention and Investigatory Powers Act 2014, which falls away on 31 December 2016. Government intervention is necessary to ensure the continued availability of, and access to communications data, primarily for law enforcement.

Our proposal is to legislate to maintain the capability of relevant public authorities designated by Parliament to access and retain communications data, both on a targeted basis and in bulk. This will require replacing the provisions under Chapter 2 of Part I of RIPA and other statutes, and legislating for the retention of internet connection records (local authorities will be prohibited from acquiring internet connection records.) and for the creation of a safeguard in the form of a request filter. It will also provide for an offence for the knowing acquisition of communications data without authority, and a disclosure provision backed by a criminal offence.

As a result of the passage of the Bill in the Commons, the legislation will provide for additional protections, in the requirement that the Judicial Commissioner may only approve an authorisation to acquire communications data to identify a journalist's source where he considers that there is an 'overriding requirement in the public interest'.

- **The interception of communications**

Legislation is required to make clearer and more transparent the legislative basis for the interception of communications by law enforcement, the armed forces and the security and intelligence agencies on a targeted basis, and the interception of communications in bulk by the security and intelligence agencies.

Our proposal is to re-legislate to consolidate and maintain current interception capabilities provided for under RIPA (as clarified by DRIPA) and sections of the Wireless Telegraphy Act 2006 into the new Investigatory Powers Bill, subject to additional safeguards and oversight as recommended by David Anderson, the ISC and RUSI; and to ensure that these capabilities can be maintained after DRIPA sunsets in December 2016. New legislation will include additional protections for the communications of Members of Parliament and

members of other legislatures. The Bill was amended to make clear that the Prime Minister must personally authorise any case where it is necessary to intercept a Parliamentarian's communications. The Bill makes clear that legally privileged material is subject to additional safeguards and oversight and makes clear the requirement for companies to remove electronic protection where they have themselves applied it, and where it is reasonably practicable for them to do so.

- **Equipment interference**

Legislation is required to make clearer and more transparent the use of targeted equipment interference for the acquisition of electronic communications and other data by security and intelligence agencies, armed forces and law enforcement agencies, and the use of bulk equipment interference reserved for use by security and intelligence agencies, and to increase the safeguards and oversight of these powers.

Our proposal is to replace existing statutory bases for equipment interference for the acquisition of electronic communications and other data into a single legislative provision that will provide for equipment interference by law enforcement, the armed forces and the security and intelligence agencies on a targeted basis; to make clear that assistance can be requested under a technical capability notice; and to apply additional protections for the communications of Members of Parliament and other legislatures. The Bill was amended to make clear that the requirement for Prime Minister authorisation of warrants seeking to acquire a Parliamentarian's communications applied to warrants authorised by law enforcement chiefs as well as those of the security and intelligence agencies.

- **Bulk Personal Datasets**

Legislation is required to make explicit and transparent the protections that apply to the security and intelligence agencies' retention and use of bulk personal data and the robust safeguards that are engaged.

Our proposal is to provide reinforced statutory safeguards, including the requirement for use of specific or class-based authorisations, issued by the Secretary of State, subject to review by a Judicial Commissioner for the retention of BPD. This would also require the security and intelligence agencies to seek specific authorisation to retain and use the most sensitive datasets, as well as making explicit the safeguards surrounding the retention and use of bulk personal data by the security and intelligence agencies in a statutory Code of Practice.

The Bill was amended to make clear that where the purpose, or one of the purposes, of a specific BPD warrant would be to authorise the retention, or the retention and examination, of health records, the Secretary of State may issue the warrant only if he or she considers that there are exceptional and compelling circumstances that make it necessary to do so.

- **Oversight of powers**

The use of investigatory powers by public authorities and oversight of the work of the security and intelligence agencies more generally is currently split between three bodies: the Office of Surveillance Commissioners; the Intelligence Services Commissioner; and the Interception of Communications Commissioner.

Our proposal is to legislate to consolidate the existing oversight structures into the Investigatory Powers Commission, headed in statute by the Investigatory Powers Commissioner, who will approve warrants as part of a double-lock authorisation process and will have oversight of all the investigatory powers within the Bill.

The Bill will also make clear that a company subject to a technical capability notice may request an appeal of that notice, and make clear the role of the Technical Advisory Board in statute.

- **Right of domestic appeal from the Investigatory Powers Tribunal**

Individuals who believe themselves to have been unlawfully surveilled can bring a case before the Investigatory Powers Tribunal (IPT) and currently those wishing to challenge a judgment from the IPT must bring it before the European Court of Human Rights. Legislation is necessary to provide the public with reassurance that the processes for holding the agencies to account are robust and effective.

Our proposal is to legislate to allow appeals to be brought in the domestic courts following permission to appeal from the IPT on either a decision or a determination. This is intended to increase public confidence that those who use investigatory powers are fully held to account by the law, and that Articles 8 and 10 of the European Convention on Human Rights are respected.

E. Appraisal (Costs and Benefits)

GENERAL ASSUMPTIONS & DATA

- That the UK requirement for a data retention regime is such that it would not be permitted to lapse.
- We have assumed that the powers currently available to law enforcement, the armed forces and the security and intelligence agencies would remain in the long run were this Bill not brought forward.
- While efforts have been made to understand the costs and benefits to all affected groups, it is necessary to make some assumptions. The Home Office has consulted Government departments; communication service providers; and operational partners including law enforcement and the security and intelligence agencies.
- The only new costs arising from any of the options considered relate to communications data obligations. The Home Office maintains a policy of reimbursing 100% of the reasonable costs incurred by business in complying with communications data retention requirements under current legislation and will continue to do so for existing and new capabilities under the Bill. The net cost of the new provisions to business will therefore be zero.

OPTION 2 – Re-legislate for the use of investigatory powers by operational partners

COSTS

There would be minimal increases above existing baseline costs for interception, equipment interference and bulk personal data. The costs of the Bill are primarily in relation to increased cost of establishing a new oversight body (led by the Investigatory Powers Commissioner), including accommodation, overheads, running costs and the administration of a new warrant process. The provisions in the Bill in relation to internet connection records and the request filter for communications data also have associated costs to business, which are reimbursed by Government.

BENEFITS

The monetary benefits derived from this option would stem from the cost-effectiveness of investigatory techniques that would obviate the need for greater use of covert surveillance. These have not been quantified. The non-monetary benefits of this policy would include: greater public confidence in the transparency and clarity of the investigatory powers regime, greater safeguards and accountability of the investigatory powers regime to independent oversight, Parliament and the public, crimes detected, investigated and averted.

The specific costs and benefits relating to all of the measures within the Bill are set out in the table below. A discount rate of 3.5% has been applied to these costs, in accordance with HMT Green Book guidance.

F. Risks

OPTION 2 – Re-legislate for the use of investigatory powers by operational partners.

There is an ongoing risk with all options outlined above that technology will continue to evolve and develop rapidly, outpacing legislation.

G. Enforcement

This legislation does not intend to introduce any new requirements for communications companies, or place any unnecessary burden on them. The government will work with communications companies to ensure that any requests for assistance can be carried out with the least amount of impact on their business.

Section 13 of RIPA established the Technical Advisory Board (TAB), which provides an important safeguard for communications companies and the Government, and ensures that any disputes that arise from the obligations imposed on communications companies can be resolved satisfactorily. The Bill includes clear provisions for telecommunications or postal operators to request a review of the requirements placed on them in a technical capability notice. However, under new legislation a person may refer the whole or any part of a technical capability notice back to the Secretary of State for review under section 220 of the Bill. Before deciding the review, the Secretary of State must consult and take account of the views of the TAB and the Investigatory Powers Commissioner (IPC). The Board must consider the technical requirements and the financial consequences of the notice on the person who has made the referral. The Commissioner will consider whether the notice is proportionate. After considering reports from the TAB and the IPC, the Secretary of State may vary, withdraw or confirm the effect of the notice. Until this decision is made, there is no requirement for the CSP to comply with the notice.

H. Summary and Recommendations

The table below outlines the costs and benefits of the proposed changes.

Policy provision	Net Present Cost over 10 years, £m (discounted)	Net Present Benefit over 10 years £m	Non-monetised cost	Non-monetised benefit
Oversight	£61.51M	N/K	There are additional non-monetised costs as staff in the new bodies take time to familiarise with new structures and reporting arrangements.	Increased public understanding of the oversight and accountability of investigatory powers. Public and Parliamentary trust and confidence in the rigour of Commissioner oversight and the way in which the use of investigatory powers is authorised. There are also likely to be efficiency savings from the merger of the existing oversight bodies, as shared resources and knowledge reduce duplication of effort.
Domestic right of appeal from the IPT	The Home Office and Ministry of Justice have agreed that the impact to the justice system is likely to be minimal.	N/K	There will likely be a necessary cost of time in order to train the IPT and its secretariat in the new rules and procedures.	Allowing a domestic right of appeal from the IPT will have a positive impact on those who are able to appeal. It will: <ul style="list-style-type: none">- be easier to understand and less stressful to those involved- Fewer cases referred to the ECtHR, having been dealt with in the domestic courts – thus saving those bringing challenges both time and cost.
Interception	N/K	N/K	N/K	Greater public confidence and transparency in the interception regime. Legislation will allow UK intercepting agencies to continue to investigate threats to ensure they can

				keep the public safe.
Communications Data	£187.1M	N/K	There will be minimal business change costs associated with each of these capabilities, such as training for operational personnel.	Greater public confidence and transparency in the communications data regime. Law enforcement and public authorities able to access the data they need as part of investigations.
Bulk Personal Data	N/K	N/K	There will be additional training and familiarisation costs for the reporting arrangements, applicable to the Commissioners, SIAs, the Home Office and the Foreign and Commonwealth Office, policy officials and legal advisers as they spend time understanding the new authorisation and reporting arrangements.	Will improve public confidence in the safeguards that apply to the SIA use of bulk personal datasets, providing the public with greater understanding and transparency.
Equipment Interference	N/K	N/K	N/K	Greater public confidence in the exercise of equipment interference by law enforcement agencies, the armed forces and the security and intelligence agencies, to acquire communications, equipment data and other information as a result of the clearer, robust safeguards and oversight applied to the use of equipment interference, with accountability to Parliament.

I. Implementation

The data retention provisions in the Bill will commence immediately on Royal Assent, in order that the data retention regime does not lapse. The Government will commence the provisions in the Investigatory Powers Act once full implementation plans have been considered and the associated public cost has been approved by Parliament. A full consultation process with affected Government departments, agencies, telecommunications operators and stakeholders will form part of implementation. Codes of Practice, which will be approved by Parliament, will set out the practical effects of the legislation.

J. Monitoring and Evaluation

The application of the legislation will be scrutinised on an ongoing and statutory basis by the Investigatory Powers Commissioner. The Intelligence and Security Committee of Parliament will continue to oversee the activities of the security and intelligence agencies, including their exercise of investigatory powers. And the Investigatory Powers Tribunal will provide a right of redress to any individual who believes they have been affected by the misuse of any of the powers in the Bill. The legislation will be subject to post-legislative scrutiny five years after Royal Assent.

K. Feedback

The Government has considered all of the recommendations of the three Parliamentary Committees and the public submissions made as part of the consultation process in responding with revised legislation.

Impact Assessment Checklist

Economic Impact Tests

Does your policy option/proposal consider...?	Yes/No (page)
Business Impact Target The Small Business, Enterprise and Employment Act 2015 (s. 21-23) creates a requirement to assess the economic impacts of qualifying regulatory provisions on the activities of business and civil society organisations. [Better Regulation Framework Manual] or [Check with the Home Office Better Regulation Unit]	N/A
Review clauses The Small Business, Enterprise and Employment Act 2015 (s. 28) creates a duty to include a review clause in secondary legislation containing regulations that impact business or civil society organisations. [Check with the Home Office Better Regulation Unit]	Yes
Small and Micro-business Assessment (SaMBA) The SaMBA is a Better Regulation requirement intended to ensure that all new regulatory proposals are designed and implemented so as to mitigate disproportionate burdens. The SaMBA must be applied to all domestic measures that regulate business and civil society organisations, unless they qualify for the fast track. [Better Regulation Framework Manual] or [Check with the Home Office Better Regulation Unit]	N/A
Clarity of legislation Introducing new legislation provides an opportunity to improve the clarity of existing legislation. Legislation with multiple amendments should be consolidated, and redundant legislation removed, where it is proportionate to do so.	Yes.
Primary Authority Any new Government legislation which is to be enforced by local authorities will need to demonstrate consideration for the inclusion of Primary Authority, and give a rationale for any exclusion, in order to obtain Cabinet Committee clearance. [Primary Authority: A Guide for Officials]	N/A
New Burdens Doctrine The new burdens doctrine is part of a suite of measures to ensure Council Tax payers do not face excessive increases. It requires all Whitehall departments to justify why new duties, powers, targets and other bureaucratic burdens should be placed on local authorities, as well as how much these policies and initiatives will cost and where the money will come from to pay for them. [New burdens doctrine: guidance for government departments]	N/A
Competition The Competition guidance provides an overview of when and how policymakers can consider the competition implications of their proposals, including understanding whether a detailed competition assessment is necessary. [Government In Markets Guidance]	N/A

Social Impact Tests

New Criminal Offence Proposals Proposed new criminal offences will need to be agreed with the Ministry of Justice (MOJ) at an early stage. The Justice Impact Test (see below) should be completed for all such proposals and agreement reached with MOJ before writing to Home Affairs Committee (HAC) for clearance. Please allow 3-4 weeks for your proposals to be considered.	Yes
--	-----

Justice Impact Test The justice impact test is a mandatory specific impact test, as part of the impact assessment process that considers the impact of government policy and legislative proposals on the justice system. [Justice Impact Test Guidance]	Yes
Statutory Equalities Duties The public sector equality duty requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity, and foster good relations in the course of developing policies and delivering services. [Equality Duty Toolkit]	N/A
Privacy Impacts A Privacy Impact Assessment supports an assessment of the privacy risks to individuals in the collection, use and disclosure of information. [Privacy Impact Assessment Guidance] or [Contact the Corporate Security Information Assurance Team Helpline on 020 7035 4969]	Yes
Family Test The objective of the test is to introduce a family perspective to the policy making process. It will ensure that policy makers recognise and make explicit the potential impacts on family relationships in the process of developing and agreeing new policy. [Family Test Guidance]	N/A
Powers of Entry A Home Office-led gateway has been set up to consider proposals for new powers of entry, to prevent the creation of needless powers, reduce unnecessary intrusion into people's homes and to minimise disruption to businesses. [Powers of Entry Guidance]	Yes
Health Impact Assessment of Government Policy The Health Impact Assessment is a means of developing better, evidenced-based policy by careful consideration of the impact on the health of the population. [Health Impact Assessment Guidance]	N/A
Environmental Impact Tests	
Environmental Impacts The purpose of the environmental impact guidance is to provide guidance and supporting material to enable departments to understand and quantify, where possible in monetary terms, the wider environmental consequences of their proposals. [Environmental Impact Assessment Guidance]	N/A
Sustainable Development Impacts Guidance for policy officials to enable government departments to identify key sustainable development impacts of their policy options. <i>This test includes the Environmental Impact test cited above.</i> [Sustainable Development Impact Test]	N/A
Rural Proofing Guidance for policy officials to ensure that the needs of rural people, communities and businesses are properly considered. [Rural Proofing Guidance]	N/A