Counter-Terrorism and Security Bill

Privacy Impact Assessment

November 2014

1. Executive summary

This document is the Privacy Impact Assessment (PIA) for the implementation of new measures included in the Counter-Terrorism and Security Bill. The purpose of this PIA is to consider the privacy impact of the proposed legislation; and address any issues raised in the regulatory impact assessments covering each policy area.

This Privacy Impact Assessment (PIA) follows the approach and guidelines recommended by the Information Commissioner's Office (ICO). It considers the impact on privacy of the proposed legislation.

This PIA identifies the risks to privacy arising from the capabilities that will be available under the new legislation, and sets out the safeguards, existing and new, intended to address these risks (section 4). The PIA concludes with a Privacy Impact Statement (see section 5).

This document should be read in conjunction with the overarching Counter-Terrorism and Security Bill Impact Assessment; and the standalone Impact Assessments covering each of the measures in the Bill. These documents can be found on the dedicated Counter-Terrorism and Security Bill page on the Gov.uk website.

2. The case for legislation

2.1 Rationale

Aim

The purpose of the new powers is to address the concerns of the security services and police about our ability to prevent individuals from travelling overseas for terrorism or terrorist related purposes and disrupt their return to the UK.

Background

On 29 August the Independent Joint Terrorism Analysis Centre raised the UK national terrorist threat level from SUBSTANTIAL to SEVERE meaning that a terrorist attack is 'highly likely'. Approximately 500 individuals of interest to the police and security services have travelled from the UK to Syria and Iraq since the start of the conflicts; a number of these individuals have joined terrorist organisations including the Islamic State of Iraq and the Levant (ISIL). On 1 September the Prime Minister announced that legislation would be brought forward in a number of areas to stop people travelling overseas to fight for terrorist organisations, or conduct terrorist related activity, and subsequently returning the UK, and to deal with individuals already in the UK who pose a risk to the public.

There is a need to legislate to deal with the increased terrorist threat. The provisions the Counter-Terrorism and Security Bill will strengthen the capabilities of operational partners (including the police, Security Service and Border Force) to disrupt the ability of people to travel abroad to fight, or engage in other terrorist related activity abroad, and control their return to the UK; enhance the ability of the law enforcement

and intelligence agencies to monitor and control the actions of those in the UK who pose a threat; and combat the underlying ideology that feeds, supports and sanctions terrorism.

2.2 Strategy

This legislation will help deliver a key part of CONTEST, the UK's Counter-Terrorism strategy, by enhancing the capabilities of law enforcement and the intelligence services for the protection of the public and to ensure public safety.

The legislation is informed by close engagement with: the police, law enforcement and intelligence agencies; Government partners; the insurance and re-insurance industry; aviation and maritime carriers and the wider transport sector; local authorities; communications service providers; the private sector; and international partners including overseas Governments and organisations who will be either directly responsible for enforcing the new measures and/or have a wider responsibility or interest in its success.

2.3 Overview of the proposed legislation

The objective of this legislation is to enhance the capabilities of law enforcement and the intelligence agencies to disrupt terrorism and prevent individuals from being radicalised in the first instance.

An overview of each of the measures included in the Counter-Terrorism and Security Bill is set out below:

Temporary Passport Seizure

The key elements of this power are that:

- It would be a new power for police officers (and designated Border Force officers under their direction) to exercise at ports where a person intends to leave Great Britain or the UK for the purpose of engaging in terrorism-related activity outside the UK;
- It will also include individuals who are returning inbound where there are reasonable grounds to suspect they will soon travel again for the purpose of engaging in terrorism-related activity outside the UK;
- The standard of proof would be 'reasonable suspicion' of intention to leave the UK in connection with terrorism-related activity;
- British or foreign passports (and any other travel documents) may be seized for up to 14 days, to conduct further investigations, to disrupt the immediate travel of a person while further disruptive actions are considered (for example, criminal prosecution, the exercise of the Royal Prerogative to cancel passports, Terrorism Prevention and Investigation Measures (TPIMs), deprivation of citizenship or deportation);
- The individual would not be detained and would remain in the UK during the period which their travel documents are being held;
- The passport (and/or other travel documents) would have to be returned when the test was no longer met or when no further disruptive action was considered appropriate and no later than the expiry of a 14 day period (unless the police had successfully applied to a court to extend the period, up to a maximum of 30 days);

- The police would need to apply successfully to a court to continue to hold the travel documents beyond 14 days, up to a maximum retention period of 30 days;
- The temporary passport seizure period could not be extended, but an individual could be subject to repeated exercise of the power if the threshold were met on future travel attempts; and
- The passport holder would be prevented from obtaining a replacement British passport during periods of seizure.

Temporary Exclusion

The main areas of this power are to:

- Create a statutory order that temporarily disrupts the return to the UK of a British citizen suspected of involvement in terrorism abroad;
- Place a prohibition on the individual returning to the UK without engagement with the UK authorities, supported by cancellation of their travel documents, inclusion of their details on watch lists (including the 'no fly' list); and
- Place requirements on the individual to comply in undertaking certain activities once back in the UK.

Terrorism Prevention and Investigation Measures

The proposal is to amend the TPIM Act to:

- Amend the definition of terrorism to remove conduct which gives support or assistance to individuals who are known or believed by the individuals concerned to be involved in the encouragement or facilitation of terrorism;
- Raise the threshold for imposing a TPIM notice so the Secretary of State must be satisfied to a balance of probabilities that the individual has been engaged in terrorism-related activity;
- Allow the Secretary of State to require a subject to reside in a particular location up to 200 miles from their current locality;
- To provide for additional measures to restrict a subject's travel outside the area in which their residence is situated;
- Include a power to require TPIM subjects to meet with statutory bodies or other persons specified by the Secretary of State;
- Prohibit TPIMs subjects from obtaining firearms and offensive weapons; and
- Increase the sentence for breaching the travel measure from a maximum of five years to a maximum of ten years, where the person leaves the UK or breaches the new power to impose a boundary around where they reside.

IP Resolution

This measure will:

- Amend the Data Retention and Investigatory Powers Act 2014 (DRIPA) to enable the Secretary of State to require Communications Service Providers (CSPs) who provide an internet access service to retain the data that will allow relevant authorities to link the unique attributes of a public IP address to the person (or at least the device) who was using it at any given time;
- Allow CSPs to be required to retain sufficient information regarding the use of their email, internet telephony and other internet communication services to enable law enforcement agencies to identify the users of such services; and

- Apply the additional safeguards relating to the retention and access of communications data, imposed under DRIPA, to the retention of any additional data under this measure.

Border Security

These proposals fall under four headings:

- Passenger data – to require carriers to use data systems capable of receiving no fly alerts and passenger screening requirements directly;
- Authority to Carry ('No Fly') – to extend the scope of the Authority to Carry ('No Fly') arrangements to include more individuals both British and foreign nationals, who pose a terrorist or terrorism-related threat to the UK and to put outbound Authority to Carry arrangements on a statutory footing;
- Specified Security Measures – to require carriers operating to the UK to undertake specified security measures, including screening of passengers.
- Schedule 7 to the Terrorism Act 2000 – to clarify the legal position in relation to the examination of goods in remote storage outside the immediate boundary of a port and the examination of goods comprising items of post.

Prevent

The legislation will create:

- A new statutory duty on specified authorities (including local government, the police, prisons, providers of probation services, schools colleges and universities – including in the private sector) to have due regard to the need to prevent people from being drawn into terrorism;
- A duty to have regard to guidance issued by the Secretary of State in fulfilling the duty above; and
- A power to direct a body to take certain action, which would be used to enforce compliance where the Secretary of State is satisfied that the body has failed to discharge the duty. These directions would be enforceable by court order.

Support for people vulnerable to being drawn into terrorism

The legislation will:

- Require local authorities to ensure that a multi-agency panel exists (and for local authorities to chair the panel) to assess the extent to which the individuals referred to it are vulnerable to being drawn into terrorism, and (in the event that the individuals are judged to be sufficiently vulnerable) to put together a support plan, and monitor and review that plan as necessary. Local authorities do not need to establish a new panel to do this if there is already one which carries out these functions;
- Set out the basics of what a support plan should include, and stipulate that, should support not be offered under Channel in England and Wales, and Prevent Professional in Scotland, other forms of support should be considered;
- Require the panel to seek the consent of the person before support is provided (and for local authorities to chair the panel);
- Require partners to pay due regard to guidance issued by the Secretary of State; and

- Allow the Secretary of State to indemnify support providers against costs arising from support they provide – this is to remove the need for intervention providers to take out bespoke insurance, which can be prohibitively expensive.

Kidnap and Ransom
This measure will:

- Ensure that the UK's reputation for not funding terrorism is maintained by preventing UK insurance companies from reimbursing ransom payments to terrorists;
- Make it more difficult for terrorists to obtain ransom payments through kidnapping by preventing reimbursement from UK insurance companies; and
- Amend the Terrorism Act 2000 to remove uncertainty around insurance (and reinsurance) payments and put this issue beyond doubt in law.

Advisory Board
The main areas of this proposal are to:

- Create an order making for the Secretary of State to set-up an advisory board to the independent reviewer of counter-terrorism legislation; and
- Provide a mechanism to assist the independent reviewer when discharging his statutory duties.

Special Immigration Appeals Commission
This measure will:

- Amend the SIAC Act 1997 to include a provision for the Home Secretary to certify a decision to refuse to grant British Overseas Territories Citizenship; and
- Ensure that any challenge to that decision may only be heard before SIAC if sensitive material has been used in reaching the decision.

Further background information on the measures can be found in the overarching and standalone impact assessments on Gov.uk.

2.4 Existing measures
This new legislation will sit alongside the existing suite of powers that are already used to combat the terrorist threat including:

- Cancelling the British passports of those who want to travel abroad to engage in terrorism under the Royal Prerogative.
- Barring foreign nationals from re-entering the United Kingdom, where they are suspected of terrorism-related activity, and can also strip British citizenship from those who have dual nationality.
- Working in partnership with the internet industry to remove terrorist material hosted in the UK or overseas; and
- Enacting emergency legislation to safeguard the retention of communications data, crucial in the investigation of those involved in terrorist activity, in this country and overseas.

3. Overview of planned safeguards

The UK already has in place a stringent framework of safeguards to protect against privacy and ensure the proportionate use of counter-terrorism powers. These safeguards include amending existing or introducing new Codes of Practice to ensure consistency of application across the UK; independent oversight; and administrative protections.

The Counter-Terrorism and Security Bill will strengthen the existing framework by introducing additional safeguards alongside existing protections.

Planned Safeguards

In addition to the current safeguards already outlined the new legislation will go further in protecting privacy. The new safeguards include:

- Consulting the public to inform the creation of a Code of Practice for the Temporary Passport Seizure power;
- Raising the standard of proof for imposing a TPIM notice and amending the definition of terrorism for purposes of TPIMs;
- Extend the existing oversight framework for communications data to include the new provisions on IP resolution.
- Consulting on statutory guidance for specified authorities affected by proposal to create a duty to have due regard to the need to prevent people from being drawn into terrorism; and
- Strengthening the oversight role of the Independent Reviewer of Terrorism Legislation by allowing for the creation of a Privacy and Civil Liberties Board to support the role of the Independent Reviewer of Terrorism Legislation.

We consider that these new safeguards provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy. These safeguards, along with the protections already in place, are examined in greater detail in section 4 below.

4. Privacy Risks and Mitigation

4.1 The risk of infringing on an individual's privacy if the Temporary Passport Seizure Power is misused

At present, operational partners do not have a power to search for and seize travel documents if they reasonably suspect an individual is travelling for the purpose of involvement in terrorism-related activity. There is a risk that an individual's right to lead a private life could be affected if their passport and travel documents were seized.

New Safeguards

To guard against the risk of misuse and concern about how the power will operate, the Government will provide clear guidance to police and Border Force officers in a statutory Code of Practice with which officers will be required to comply and which will be subject to a public consultation. Privacy and civil liberties groups will be invited to provide feedback on the Code of Practice during the consultation.

The Government will make the power to retain the travel documents subject to senior police officer review at two stages. The first review will be after the initial seizure at port, by an officer of Superintendent Rank or above, to authorise the continued retention of the documents. In addition at 72 hours there will be a review by a senior police officer outside the chain of command who will be required to write to the Chief Constable of the force retaining the document with his findings. The Chief Constable must have regard to this in taking any further action in relation to the matter.

If the police wish to retain the documents for longer than14 days, there will also be a court review of the continuing need by the police to retain the passport for up to 30 days.

No extension beyond thirty days retention is provided for, but it is possible that a determined individual might repeatedly attempt to travel, necessitating a fresh seizure of the document. To safeguard against repeated use of the power being used inappropriately against the same individual, if the power were exercised three times in a six month period in relation to the same person, the police would need to go in front of a District Judge within five days on the third occasion to justify the need to retain the passport.

A complaints procedure to provide information and a route to redress for individuals who believe they have been unfairly stopped and had their travel documents removed will be introduced. This will provide an avenue of complaint to the Independent Police Complaints Commission and acts as a further safeguard should an individual have any privacy concerns.

4.2 The risk of infringing on an individual's privacy by misusing the power to impose Temporary Exclusion Orders.

Temporary Exclusion Orders (TEOs) are a new power that will enable the Secretary of State to prohibit an individual from returning to the UK without engaging with the UK authorities. It will also allow for the imposition of certain requirements on the individual once they return to the UK.

Continuing Safeguards

The components of a TEO which might impact on a subject's privacy are already governed by strict safeguards in their respective areas. These components include entering the individual's details on the 'no fly' list and other watch lists; intelligence gathering and sharing with partners; handling data from any application for a permit to return; handling data obtained as part of any police interview; requiring reporting to the police and notification of a change of address.

Furthermore, as with other operational security matters, we would not intend to publish the names of individuals subject to TEOs or to comment on their cases.

New Safeguards

In addition to the above, a number of new safeguards are attached to the TEO power itself, which are designed to ensure the power is not misused and the rights of the individual, including privacy, are protected:

- The threshold for imposing a TEO would be that the Secretary of State 'reasonably suspects that the subject is or has been involved in terrorism-related activity while outside the UK';
- An order would be imposed for a maximum of two years, with the possibility of a new one being imposed only following fresh consideration;
- An individual would be able to challenge the imposition of a TEO through judicial review. We would rely on Section 6 of the Justice and Security Act to invoke closed material proceedings in the administrative courts; and
- If an individual subject to a TEO applied for a permit to return, the Secretary of State would be obliged to grant the person a permit to return within a reasonable period of time.

4.3 The risk that the strengthened Terrorism Prevention Investigation Measures (TPIMs) regime may infringe disproportionately on the privacy of individuals.

The Counter-Terrorism and Security Bill will include provisions to enhance the existing TPIMs regime to deal with the significant threat of British nationals returning from overseas conflict zones such as Syria and Iraq, with the intention of engaging in terrorist activities, and those individuals already in the UK who pose a security risk to the general public.

Continuing Safeguards

The existing framework of safeguards which govern the introduction of a TPIM are stringent and, as with the other safeguards described elsewhere in this document, will be retained as part of the Counter-Terrorism and Security Bill.

The Independent Reviewer of Terrorism Legislation has a statutory duty to review the Terrorism Prevention and Investigation Measures (TPIMs) Act 2011 and

publishes an annual public report setting out an assessment of the power to date and any recommendations to improve its use. The Secretary of State is also required to provide a quarterly report to Parliament on the use of the Act.
The Act sets out the conditions in Schedule 1 (Conditions A-E) that need to be satisfied to introduce a TPIM:

- Condition A is that the Secretary of State is satisfied to a balance of probabilities that the individual is, or has been, involved in terrorism-related activity;

- Condition B is that some or all of the relevant activity is new terrorism-related activity.

- Condition C is that the Secretary of State reasonably considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, for a TPIM to be imposed on the individual.

- Condition D is that the Secretary of State reasonably considers that it is necessary, for purposes connected with preventing or restricting the individual's involvement in terrorism-related activity, for a TPIM to be imposed on the individual.

- Condition E is that the court gives the Secretary of State permission under section 6 of the Act, or the Secretary of State reasonably considers that the urgency of the case requires terrorism prevention and investigation measures to be imposed without obtaining such permission.

All individuals upon which a TPIM is imposed are automatically entitled to a review hearing at the High Court for the decision to impose the notice and the individual measures in the notice. They may also appeal any decisions made subsequent to the imposition of the notice, i.e. a refusal of a request to vary a measure, a variation of a measure without their consent, and the revival or extension of their TPIM notice.

The Secretary of State must also keep under review the necessity of the TPIM notice and specified measures during the period that a TPIM notice is in force.

A TPIM notice lasts for one year and can be extended by a further year. No new TPIM may be imposed on the individual after that time unless the Secretary of State reasonably believes that the individual has engaged in further terrorism related activity since the imposition of the notice.

New Safeguards
Under the strengthened TPIMs regime the Secretary of State will have the power to require a subject to reside in a particular location up to 200 miles from their current locality and will be able to provide for additional measures to restrict a subject's travel outside the area in which their residence is situated. There is, in theory, a risk that these provisions interfere with an individual's privacy. To address this concern, the individual can not be re-located more than 200 miles from their residence prior to the imposition of the TPIM Notice without their agreement. The threshold for imposing a TPIM notice in Condition A is being raised so the Secretary of State must

be satisfied to a balance of probabilities that the individual is or has been involved in terrorism-related activity before imposing a TPIM.

4.4 The risk that data retrieved as part of the IP resolution measure will be handled inappropriately or insecurely stored.

The new legislation will provide for the retention of communications data by communications service providers which will allow those authorities who are designated under the Regulation of Investigatory Powers Act 2000 (RIPA) and lawfully allowed to access traffic data, to identify who in the real world was using an IP address at a given point in time. The Bill will ensure that UK service providers retain sufficient internet communications data to allow law enforcement to attribute communications to people or their devices.

There are, in theory, risks that data may be accessed without the necessary or appropriate approvals; that incorrect data may be returned to a public authority; and that data may be insecurely stored.

Continuing Safeguards

The Data Retention and Investigatory Powers Act 2014 (DRIPA) together with RIPA provide a robust framework which ensures that the retention of, and access to, communications data in the UK is a justifiable interference with the ECHR Article 8 right to a private life. DRIPA introduced additional protections surrounding the retention of communications data by communications service providers, including:

- Specifying that Ministers must consider the necessity and proportionality before issuing a notice to a communications service provider;
- Specifying further requirements around what information Ministers must consider before issuing a data retention notice;
- Amending the set period for which data is retained, from 12 months to a maximum of 12 months (allowing for shorter periods if there is lesser need);
- Limiting access to retained communications data to requests under RIPA and court orders;
- Ensuring that specific data security requirements must be specified in a notice to each CSP when it is issued; and
- Clarifying in the legislation the duties of the Information Commissioner, so that he can oversee all of the relevant aspects of the retention of data (including data integrity and destruction).

As part of these safeguards, Ministers must consider that retention of data is necessary for one of n the ECHR-compliant statutory purposes set out in RIPA in relation to data acquisition. DRIPA also sets out the requirements around what information Ministers must consider before issuing a data retention notice.

Section 1(6) of DRIPA provides that operators may only disclose data retained under a retention notice in accordance with the scheme under Chapter 2 of Part 1 of RIPA, which provides guarantees against abuse, or in accordance with a court order or warrant[1]. Under section 22 of RIPA access is only permitted by authorised public authorities. Public authorities are authorised to access different categories of data for

[1] Section 1(6) is not yet in force, but the Home Office intends to commence it this year.

different purposes. A notice or authorisation to access communications data must be necessary and proportionate for one of the authorised purposes, taking into account any collateral intrusion.

DRIPA places an obligation on CSPs to protect data from accidental destruction, loss, alteration or disclosure and sets out a maximum period of up to 12 months for retention of data by CSPs and a requirement to destroy it at the end of this period. The Interception of Communications Commissioner provides independent oversight of the acquisition of communications data by public authorities, including through inspections of public authorities. He provides a (published) annual report to the Prime Minister. Under provisions in DRIPA, the Commissioner will be required to report on a six monthly basis in the future, further enhancing transparency. The most recent annual report of the Commissioner covered 2013 and contained more detail than ever before on the use of communications data by public authorities, as outlined below.

The processing of personal information, including communications data, is regulated by the Data Protection Act 1998, which is overseen by the Information Commissioner. The Information Commissioner is also under a duty to audit compliance by communications service providers with the provisions of the Data Retention Regulations 2014 with respect to the security, integrity and deletion of retained data.

4.5 The risk that the number of people mistakenly identified as a person on the 'no fly' list could increase

As the scope of the authority to carry ('no fly') scheme is expanded and the number of individuals included increases, it is possible that more people could be mistakenly identified as someone included in the scheme.

Continuing Safeguards

There are two main safeguards:

i) Administrative arrangements provide for timely review of individuals' enquiries / complaints about inclusion on the No Fly list, to correct errors and ensure that the individual is not mistakenly identified in the future. These arrangements are administered by Border Force.

ii) An individual can seek judicial review action to challenge a decision to deny them boarding under the scheme.

4.6 The risk of infringing on an individual's privacy by misusing the power to examine goods under Schedule 7 to the Terrorism Act 2000.

The Counter-terrorism and Security Bill provides an opportunity to amend Schedule 7 to the Terrorism Act 2000 to clarify the legal position in relation to the examination of goods in remote storage outside the immediate boundary of a port.

Continuing Safeguards

The Independent Reviewer of Terrorism Legislation is responsible for reporting each year on the operation of the Terrorism Act 2000.

The existing Code of Practice for Schedule 7 powers provides detailed guidance to officers and ensures that powers are used consistently and in accordance with the law by all examining officers. The Home Office has a statutory duty to consult upon any revisions to the Code, and to subject the revised Code to the affirmative parliamentary procedure before it is brought into operation and it is issued to front line officers.

An individual can complain about a Schedule 7 examination by writing to the Chief Officer of the police force concerned. All Schedule 7 complaints are overseen by the Independent Police Complaints Commission (IPCC). Her Majesty's Inspectorate of Constabulary (HMIC) independently assesses police forces and policing activity from neighbourhood teams to serious crime and terrorism. This includes assessment of the use of Schedule 7 powers.

New Safeguards

In conjunction with the commencement of the provisions, a revised Schedule 7 Code of Practice would be brought into force, having been amended to include provisions governing the examination of goods. The Home Office will conduct a full public consultation on the Code of Practice shortly and will seek the views of privacy and civil liberties groups on the proposed amendments.

Schedule 7 examining officers will be required by 1 April 2015 to be trained to a national standard and, as part of the new safeguard regime, will be accredited to use Schedule 7 powers in relation to goods.

A notice will be placed on the outside of goods stating they have been examined. The notice will identify the police force that has examined the goods, and will give a unique reference number relating to the examination. This will allow the identification of the officer carrying out the goods examination in the event of a query or complaint.

4.7 The risk that the legislation lacks a sufficient oversight mechanism and future privacy issues arising will not be addressed sufficiently.

The Counter-Terrorism and Security Bill will improve the operation of existing legal powers and create new powers where they are needed. It is essential that the UK's counter-terrorism capabilities continue to evolve to ensure the police and security services have the powers they need to tackle emerging and existing threats.

Continuing Safeguards

The Independent Reviewer of Terrorism Legislation is appointed to review the operation of the provisions of the Terrorism Act 2000 and Part One of the Terrorism Act 2006. He has additional statutory functions to review the Terrorist Asset-Freezing etc. Act (TAFA) 2010 (under section 31 of TAFA 2010) and the Terrorism Prevention and Investigation Measures (TPIMS) Act 2011 (under section 20 of TPIMS Act 2011).The Independent Reviewer is required to report at least once in every 12 month period on each of the Acts which fall within his statutory responsibilities. Reports are provided to the relevant Secretary of State, and a copy of the report is laid before Parliament.

The Home Office also monitors the number of prosecutions under the new provisions and the range of sentences handed down. The Home Office publishes quarterly statistical releases on the arrests and outcomes of proceedings under terrorism powers. As with any extension of counter-terrorism powers, we are mindful of the need to ensure that the new powers remain necessary, proportionate and justified.

Intelligence activity more generally is overseen on multiple levels by the Government via Secretaries of State, independently by the Intelligence Services Commissioner and the Interception of Communications Commissioner, by Parliament via the cross-party Intelligence and Security Committee of Parliament, and judicially by the independent Investigatory Powers Tribunal.

New Safeguards

The legislation will provide the Home Secretary with a mechanism to establish a statutory Privacy and Civil Liberties Board, which will support the Independent Reviewer of Terrorism Legislation in discharging his statutory duties.

The remit of the Board will be explored during a full public consultation after the Bill has been introduced but it could fulfil the following functions:

- Assist the Independent Reviewer in reviewing the operation of those Acts which fall within his existing statutory responsibilities, with particular regard to whether these are sufficient too meet the threat and adequately take account of privacy and civil liberty concerns;
- Advise the Independent Reviewer on whether it considers government policy and its development, including new legislation, relating to the prevention of terrorism is sufficient to meet the threat and adequately takes account of privacy and civil liberty concerns;
- Carry out particular inquiries, on behalf of the Independent Reviewer, into the impact of particular issues or legislation relating to the prevention of terrorism, including at the direction of relevant Minister.

5. Privacy Impact Statement

This Privacy Impact Assessment has been carried out to assess the risks to privacy posed by the work carried out on the basis of the proposed legislation. It is assessed that implementation of the proposed legislation is capable of being fully compliant with relevant domestic and international law.