Home Office

NATIONAL SECURITY NOTICES

DRAFT Code of Practice

December 2017

Home Office

NATIONAL SECURITY NOTICES

DRAFT Code of Practice

Presented to Parliament pursuant to paragraph 4(5) of Schedule 7 to the Investigatory Powers Act 2016

December 2017

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk.

Contents

Introduction

1.1 This Code of Practice relates to the powers and duties conferred or imposed under sections 249, 252, and 254 to 258 of Part 9 of the Investigatory Powers Act 2016 ("the Act"). It provides guidance on the procedures to be followed when a national security notice is given. This Code of Practice sets out further detail on the circumstances in which a national security notice can be given; the process that must be followed before a notice can be given; the obligations that may be imposed by the giving of a notice and the ensuing right of review; and oversight of the use of national security notices.

1.2 The Act provides that all Codes of Practice issued under Schedule 7 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to the Investigatory Powers Commissioner responsible for overseeing the powers and capabilities conferred by the Act, it may be taken into account.

1.3. For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of an intercepting agency's internal advice or guidance.

Scope and definitions

What is a national security notice?

2.1 The Act provides that the Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of such specified steps as the Secretary of State considers necessary in the interests of national security. A notice can be given only if the Secretary of State is satisfied that the steps required are necessary in the interests of national security and proportionate. Detail on the definition of a telecommunications operator is provided later in this chapter.

2.2 The power to give a notice under section 252 replaces in part the power in section 94 of the Telecommunications Act 1984 which has been used for a range of purposes including for civil contingencies and to acquire communications data in bulk. Powers to acquire communications data in bulk are now contained in Chapter 2 of Part 6 of the Investigatory Powers Act 2016. Paragraph 99 of Schedule 10 to the Act repeals section 94 of the Telecommunications Act 1984.

2.3 Chapter 3 provides information on the type of support that may be required by a national security notice. It also explains where a warrant or authorisation under the Act, the Intelligence Services Act 1994 (ISA), the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) may be required in addition to the notice.

What is a telecommunications operator?

2.4 A telecommunications operator is a person who offers or provides a telecommunication service to persons in the UK or who controls or provides a telecommunication system which is (wholly or in part) in or controlled from the UK. The Act makes clear that the Secretary of State may give a national security notice only to operators in the UK.

2.5 Section 261(11) of the Act defines ‘telecommunications service’ to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service) (section 261(11)). The Act then defines ‘telecommunication system’ to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the UK or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy (section 261(13)). The definition of ‘telecommunications service’ in the Act is intentionally broad so that it will remain relevant in respect of new technologies.

2.6 The Act makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be

transmitted, by means of a telecommunication system is included within the meaning of ‘telecommunications service’. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

2.7 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunication service. For example, an online market place may be a telecommunications operator if it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

2.8 Telecommunications operators may also include persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises such as hotels, or public premises such as airport lounges, or on public transport.

.

National Security Notices – general rules

The activity authorised by a notice

3.1 Section 252 of the Act states that a Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of specified steps as the Secretary of State considers necessary in the interests of national security. A notice can only be given if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by the conduct. Subsection (8) makes clear that conduct required by a national security notice is lawful for all purposes.

3.2 The Act does not set out an exhaustive list of the type of conduct that might be required by a national security notice. Section 252(3) does however provide that a notice may, in particular, require an operator:

- to carry out any conduct for the purpose of facilitating anything done by an intelligence service;
- to carry out any conduct for the purpose of dealing with an emergency;
- to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively.

3.3 In practice, the steps that an operator may be required to take include the provision of services or facilities which would help an intelligence service in safeguarding the security of their personnel and operations, or in providing assistance with an emergency as defined in section 1 of the Civil Contingencies Act 2004. An emergency is described in that Act as:

a) an event or situation which threatens serious damage to human welfare in a place in the UK;

b) an event or situation which threatens serious damage to the environment of a place in the UK , or

c) war or terrorism, which threatens serious damage to the security of the UK.

3.4 It is not possible to list the full range of steps that telecommunications operators may be required to take in the interests of national security; not only would this affect the ability of the police and security and intelligence agencies to carry out their work, but as communications technology changes the Secretary of State will need to retain flexibility to respond. However, a notice may typically require a telecommunications operator to provide services to support secure communications by the intelligence services, for example by arranging for a communication to travel

via a particular route in order to improve security, or asking a telecommunications operator to refrain from doing something they might otherwise do. A national security notice might relate to the confidential provision of services to the intelligence services by a telecommunications operator, such as by requiring the operator to maintain a pool of trusted staff for the management and maintenance of sensitive communications services.

Limitations as to what can be authorised by a notice

3.5 Section 252(4) and (5) restrict when a national security notice can be given. These provisions provide a number of safeguards

3.6 **A notice <u>cannot</u> be given when the main purpose of the notice is something for which a warrant or authorisation under a relevant enactment is required.** Section 252(6) defines relevant enactments as: Act, ISA, RIPA, and RIP(S)A. For example, a national security notice cannot be used as an alternative to an interception warrant where such a warrant is required to authorise the activity. The notice may require the taking of a step that involves conduct that could be authorised under one of the relevant enactments, but that conduct cannot be the main purpose of the notice.

3.7 Secondly, where a notice requires the taking of a step that must be authorised under a relevant enactment, the Act mandates that a warrant or authorisation under one or more of the relevant enactments must be obtained.[1] For example, this might occur where the notice requires an operator to provide a service and one of the steps involved in the provision of that service involves the obtaining of communications data. The obtaining of such data (which cannot be the main purpose of the notice) would need to be authorised under the relevant provisions in the Act. When authorised, the acquisition and use of the communications data would be subject to the usual safeguards that apply to such authorisation regardless of the presence of the notice.

3.8 In addition to the limitations detailed above, the Secretary of State must have particular regard to circumstances where a notice requires the taking of any steps that involve an interference with privacy (such as the acquisition of private data) for which a warrant or authorisation under a relevant enactment is not required. In such circumstances, the Secretary of State must be satisfied that a warrant or authorisation is not required, and must, when deciding to give the notice, consider whether it is necessary and proportionate for the data to be acquired. For example, an operator may provide a service to an agency. The agency might require information about staff involved in providing the service for security purposes. This would be an interference with privacy, but it isn't something for which a warrant or authorisation is required.

[1] Section 252(4).

Necessity and proportionality

3.9 The Act provides that a national security notice can only be given if the notice is necessary in the interests of national security, and the conduct required is proportionate to what is sought to be achieved by that conduct.

3.10 Any assessment of proportionality involves balancing the reasonableness of the steps that must be taken, against the need for the activity in the interests of national security. The conduct authorised should offer a realistic prospect of bringing the expected benefit and should not be disproportionate or arbitrary.

3.11 Paragraph 2 of Schedule 7 of the Investigatory Powers Act provides that a code issued under the Act must contain particular provision designed to protect the public interest in the confidentiality of sources of journalistic information and any data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information. Where a notice requires the taking of a step that involves an interference with privacy, and a warrant or other authorisation has been obtained to authorise that conduct, the Code of Practice relevant to that authorisation will contain provisions required by Paragraph 2 of Schedule 7 of the Act. Where a warrant or authorisation is not required to authorise an interference with privacy, it will never be appropriate to obtain journalistic information or any data which relates to a member of a profession which routinely holds material of this nature via a national security notice. As such, it is not necessary to include more detailed safeguards in respect of such information in this code as they are not relevant.

Matters to be considered by the Secretary of State

3.12 Section 255(2) provides that before giving a notice to an operator, the Secretary of State must consult the operator. More detail on the consultation is set out in chapter 4 of this code. Following the conclusion of consultation with a telecommunications operator, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is justified and that proper processes have been followed.

3.13 As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 255(3):

- the likely benefits of the notice;
- the likely number of users of any telecommunications service to which the notice relates, if known;
- the technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator;

- the likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator as part of the notice, such as those relating to security, as well as the cost to Government. This will enable the Secretary of State to consider whether the imposition of a notice is affordable for the operator and is both affordable and represents value for money for Government;

- any other effect of the notice on the telecommunications operator – again taking into account any representations made by the company.

3.14 In addition to the points above, the Secretary of State should consider any other issue which is relevant to the decision. Section 2 of the Act sets out the general duties that apply to public authorities in relation to privacy.[2] The duties include a requirement on the Secretary of State to have regard to the following when giving, varying or revoking a notice so far as they are relevant:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means;

- the public interest in the integrity and security of telecommunication systems, and

- any other aspects of the public interest in the protection of privacy.

3.15 When considering the public interest in the integrity and security of telecommunication systems, the Secretary of State should consider specifically the integrity and security of telecommunication systems impacted by obligations set out in the notice.

3.16 Section 2(3) of the Act acknowledges the need to take other considerations into account, including but not limited to the considerations set out at section 2(4). In cases where a national security notice is to be given, the considerations set out at section 2(4) may not be relevant but where they are relevant, they must be taken into account.

3.17 In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision.

Format of national security notice applications

3.18 Responsibility for giving a national security notice rests with the Secretary of State. An application to the Secretary of State for a national security notice to be given to a telecommunications operator should contain the following information:

[2] See section 2(3)(a)

- the purpose of the notice and what it seeks to achieve;
- why it is not possible to achieve the required outcome by using one of the other powers contained in the Act or any other relevant enactment;
- why the notice is necessary in the interests of national security;
- why the activity required by the notice is necessary and how that activity is proportionate to what it seeks to achieve;
- whether the activity proposed is likely to interfere with privacy and if so, why it is not possible to achieve the required outcome by using less intrusive means;
- an assessment of the reasonableness of the steps the telecommunications operator is required to take, and details of the consultation that has taken place with the telecommunications operator to whom the notice will be given;
- an assessment of risk to the security and integrity of operator's systems and services.

3.19 Where another warrant or authorisation is required (by virtue of Section 252(4)), the application must provide details of the warrant or authorisation that has been or must be obtained. If a notice requires the taking of any steps that involve an interference with privacy for which a warrant or authorisation under a relevant enactment is not required, the application must:

- set out the known/expected interference or where there is a potential for interference to occur;
- explain why this specific interference is necessary and proportionate; and
- describe any mitigating action which will be taken to keep the interference to a minimum.

3.20 An example of what should be contained in an application for a national security notice is attached at Annex A.

Giving a national security notice

3.21 Paragraph 3.13 details the matters that must be taken into account before a notice can be given and makes clear that an operator must be consulted prior to a notice being given. Section 252 provides that the Secretary of State may only give a notice if the Secretary of State considers the following tests are met:

- **The notice is necessary in the interests of national security**;

- **The conduct authorised by the notice is proportionate to what it seeks to achieve**;

- **There are satisfactory safeguards in place** (as described in Chapters 3 and 5 of this Code).

- **Judicial Commissioner approval has been obtained**. The Secretary of State may not give a notice unless and until the decision to give the notice has been approved by a Judicial Commissioner. Section 254 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the notice is necessary, and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

3.22 The notice must specify the period within which the steps specified in the notice are to be taken. The period of time must be one the Secretary of State considers to be reasonable.

Duration and review of national security notices

3.23 A national security notice remains in force until it is revoked by the Secretary of State.

3.24 Section 256(2) of the Act imposes an obligation on the Secretary of State to keep a notice under review. This helps to ensure that the notice, and any of the steps specified in the notice, remain necessary and proportionate. This evaluation differs from the process provided for in section 257 of the Act, which permits a telecommunications operator to refer a national security notice to the Secretary of State for review (as set out in paragraph 4.16 to 4.20).

3.25 The exact timing of a review of a national security notice is at the Secretary of State's discretion. However, a review must take place at least once every two years. Reviews are likely to be more frequent where regular conduct is required by the notice, such as the provision of service to support the security of the communications of an intelligence service. Where a step to be taken is less frequently used, such as in relation to civil contingency planning, a less frequent review may be appropriate. The undertaking of periodic reviews should not prevent further ad hoc reviews being carried out where that is considered appropriate. Where a notice relies on another warrant or authorisation, the Secretary of State may wish to review the notice at the same time as considering whether the other warrant or authorisation should be renewed.

3.26 In reviewing the notice, the Secretary of State must consider whether the activity required by the notice remains necessary and proportionate. As part of the review, the Secretary of State must have particular regard to any interference with privacy

which is not authorised by a warrant or authorisation. In such cases, the Secretary of State must consider whether this specific conduct remains necessary and proportionate and should continue to be required by the notice, and must continue to be satisfied that a warrant or authorisation under a relevant enactment is not required.

3.27 A review must be instigated as soon as is practicable where any interference with privacy occurs that was not anticipated. The Secretary of State must be satisfied that any continued interference is justified, and should not be authorised by alternate means.

3.28 The Secretary of State must vary or revoke the notice, wholly or in part, if the conduct it requires is no longer necessary or proportionate.

Variation of a national security notice

3.29 Section 256 of the Act provides that national security notices may be varied by the Secretary of State if the Secretary of State considers that the variation is necessary in the interests of national security and the conduct required by the notice as varied is proportionate to what is sought to be achieved. Where the notice as varied imposes further obligations on the telecommunications operator, the decision to vary a notice must be approved by a Judicial Commissioner. Judicial Commissioner approval is not required where a variation removes or reduces obligations from the notice.

3.30 Where a telecommunications operator has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Secretary of State, in consultation with the telecommunications operator, will need to consider whether the existing notice should be varied or whether a new notice should be given.

3.31 Before varying a notice, the Secretary of State is required to consult the telecommunications operator to understand the impact of the change, including cost and technical implications. The consultation requirement is the same when varying a notice as it would be when giving a new notice. Once this consultation process is complete, the Secretary of State will consider whether it is necessary to vary the notice and whether the requirements imposed by the notice as varied are proportionate to what is sought to be achieved by that conduct.

3.32 Once a notice has been varied by the Secretary of State, and the decision to vary a notice has been approved by a Judicial Commissioner where that is required, arrangements will be made for the telecommunications operator to be notified of this variation in writing and to be provided with details of the timeframe in which the steps specified in the notice as varied are to be taken by the telecommunications operator. The time taken to take these steps will be taken into account and, accordingly, different elements of the variation may take effect at different times.

Revocation of national security notices

3.33 Section 256 provides for the revocation of a national security notice.

3.34 Circumstances where it may be necessary to revoke a notice include where the steps specified in the notice are no longer necessary or proportionate, where an operator no longer operates or provides the services to which the notice relates, or where operational requirements have changed.

3.35 The revocation of a national security notice does not prevent the Secretary of State giving a new notice, covering the same, or different services, to the same operator in the future should it be considered necessary and proportionate to do so.[3]

[3] See Section 256(8)

Telecommunications operator compliance

4.1 Where a national security notice is given to a telecommunications operator, that person is under a duty to take all the steps required by the notice. This applies to any company in the UK. Section 255 sets out the means by which that duty may be enforced.

4.2 An example of what a national security notice will look like is contained at Annex B. This is provided for illustrative purposes; it is not intended to dictate how national security notices must appear. It is necessarily blank so as not to reveal sensitive capabilities and undermine their effectiveness.

Consultation with operators

4.3 As set out at paragraph 3.12, before giving a notice, the Secretary of State must consult the operator.[4] In practice, consultation is likely to take place well in advance of a notice being given in order that the operator understands the aims of the notice, can consider the impact of the notice and can work with the Secretary of State to agree how to deliver the required service. The Secretary of State will also provide advice and guidance to the operator to prepare them for the possibility of receiving a notice. The time taken for the consultation will vary depending on the individual circumstances in each case, such as the complexity of the notice, the nature of the obligations to be imposed, and the resources available to the operator to consider the proposed obligations.

4.4 In the event that the Secretary of State considers it appropriate to give a notice, the Government will take steps to consult the telecommunications operator formally before the notice is given. Should the person to whom the notice is to be given have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision making process.

Receiving a notice

4.5 Once the Secretary of State has made a decision to give a notice, and the decision has been approved by a Judicial Commissioner, arrangements will be made for it to be given to the telecommunications operator. During consultation, it will be agreed who within the company should receive the notice and how it should be provided (i.e. electronically or in hard copy). If no recipient is agreed, then the notice will be given to a senior executive within the company.

[4] See section 255(2).

4.6 A person to whom a national security notice is given is under a duty to comply with the notice. The duty to comply with a national security notice is enforceable against a person in the UK by civil proceedings brought by the Secretary of State.[5] The duty to comply with a notice applies despite any other duty imposed by Part 1, or Chapter 1 of Part 2 of the Communications Act 2003.[6]

Disclosure

4.7 Any person to whom a national security notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person[7] unless given permission by the Secretary of State. The circumstances in which permission may be given by the Secretary of State may include disclosure:

- to a person (such as a system provider) who is working with the telecommunications operator to give effect to the notice;
- to relevant oversight bodies;
- to regulators where, in exceptional circumstances, information relating to an obligation imposed by a notice may be relevant for the purpose of carrying out their functions;
- to a legal advisor in contemplation of legal proceedings, or for the purpose of those proceedings;
- to other telecommunications operators who have been given a national security notice to facilitate consistent implementation of the obligations.

Contribution to the costs of taking the steps required by a national security notice

4.8 Operators may incur costs in complying with the Act, including in taking steps required by a national security notice. In recognition of this, the Act therefore requires the Secretary of State to have in place arrangements to ensure that operators receive an appropriate contribution to these costs.

[5] See section 255(10).

[6] See section 255(12)

[7] See section 255(8)

4.9 To ensure that operators can take the steps set out in a notice, public funding will be made available to contribute towards costs that the operator would not otherwise have incurred when conducting their normal business practices.

4.10 It is legitimate for an operator to seek contributions towards its costs which may include an element of providing funding of those general business overheads required in order to take the steps specified by a national security notice.

4.11 This is especially relevant for operators which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems.

4.12 Contributions may also be appropriate towards costs incurred by an operator which needs to update its systems to maintain, or make more efficient, the taking of steps required by a national security notice. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to take the steps specified in the notice.

4.13 The cost of complying with the requirements in a notice will be discussed during the consultation before a notice is given. Any operator seeking to recover appropriate contributions towards its costs should make available to the Secretary of State such information as the Secretary of State requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the operator.

4.14 Any operator that has claimed contributions towards costs may be required to undergo a Government audit before payments are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

4.15 The level of contribution which the Secretary of State determines should be made in respect of the costs incurred, or likely to be incurred, by the telecommunications operator in complying with the notice must be specified on the notice.[8]

Referral of national security notices

4.16 The recipient of a national security notice may refer the notice, or any part of the notice, back to the Secretary of State for review.

4.17 The circumstances and timeframe within which a telecommunications operator may request a review are set out in regulations made by the Secretary of State and approved by Parliament. Details of how to refer a notice back to the Secretary of State for review will be provided to the operator either before or at the time the notice is given.

[8] See section 249(7) of the Act.

4.18 Before deciding the review, the Secretary of State must consult the Technical Advisory Board (the TAB) and a Judicial Commissioner. The Board must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Judicial Commissioner must consider whether the notice is proportionate.

4.19 The TAB and the Judicial Commissioner must give the relevant telecommunications operator and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions.

4.20 After considering reports from the TAB and the Judicial Commissioner, the Secretary of State may decide to vary, withdraw or confirm the effect of the notice. Where the Secretary of State's decision is to confirm the effect of the notice, this decision must be approved by the Investigatory Powers Commissioner. Until this decision is made and approved by the Commissioner, there is no requirement for the telecommunications operator to comply with those part of the notice that have been referred.

Oversight

5.1 The Investigatory Powers Act provides for an Investigatory Powers Commissioner, whose remit is to provide comprehensive oversight of the use of the powers contained within the Act and adherence to the practices and processes described by this code. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts and legal experts, qualified to assist the Commissioner in his or her work. The Commissioner will also be advised by the Technical Advisory Panel.

5.2 The Investigatory Powers Commissioner, and those that work under the authority of the Investigatory Powers Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. Section 229(3)(b) sets out that the Investigatory Powers Commissioner must keep under review the giving and operation of national security notices. The Investigatory Powers Commissioner may undertake these inspections, as far as they relate to the Investigatory Powers Commissioners functions, entirely on his or her own initiative. Section 236 provides for the Intelligence and Security Committee of Parliament to refer a matter to the Investigatory Powers Commissioner with a view to carrying out an investigation, inspection or audit.

5.3 The Investigatory Powers Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Investigatory Powers Commissioner must not act in a way which is contrary to the public interest, or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (see section 229(6)). A Judicial Commissioner must in particular not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces (see section 229(7)).

5.4 All relevant persons using investigatory powers must provide all necessary assistance to the Investigatory Powers Commissioner and anyone who is acting on behalf of the Investigatory Powers Commissioner. Here, a relevant person includes, among others, any person who holds, or has held, an office, rank or position with a public authority (see section 235(7)).

5.5 Anyone, including anyone working for a public authority or telecommunications operator who has concerns about the way that investigatory powers are being used may report their concerns to the Investigatory Powers Commissioner. This may be

in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority.

5.6 The Investigatory Powers Commissioner must report annually on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the Investigatory Powers Commissioner's report. If the Investigatory Powers Commissioner disagrees with the proposed redactions to his or her report then the Investigatory Powers Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

5.7 The Investigatory Powers Commissioner may also report, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publically available subject to public interest considerations. Public authorities and telecommunications operators may seek general advice from the Investigatory Powers Commissioner on any issue which falls within the Investigatory Powers Commissioner's statutory remit. The Investigatory Powers Commissioner may also produce guidance for public authorities on how to apply and use investigatory powers. Wherever possible this guidance will be published in the interests of public transparency.

5.8 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [website for IPC once created]

Annex A: Detail which must be contained in a national security notice application

National security notice application

An application to the Secretary of State for a national security notice should set out:

- the purpose of the notice and what it seeks to achieve;
- why it is not possible to achieve the required outcome by using one of the other powers contained in the Investigatory Powers Act or any other relevant enactment;
- why the notice is necessary in the interests of national security;
- why the activity required by the notice is necessary and how that activity is proportionate to what it seeks to achieve;
- whether the activity proposed is likely to interfere with privacy and if so, why it is not possible to achieve the required outcome by using less intrusive means;
- an assessment of the reasonableness of the steps the telecommunications operator is required to take, and details of the consultation that has taken place with the telecommunications operator to whom the notice will be given;
- an assessment of risk to the security and integrity of operator's systems and services;
- any other relevant considerations including those set out in section 2 of the Investigatory Powers Act 2016.

An application should also address the following questions:

<u>Necessity</u>

- **What is the purpose of the notice*/* what are you seeking to achieve and why is it necessary?** *[Brief description of what the telecommunications operator will be asked to do and why it is necessary in the interest of national security]*
- **Why an NSN is required and the objective cannot be achieved using a warrant or authorisation under a relevant enactment?** *[if so, explain why a national security notice is necessary to achieve the objective]*

Proportionality

- **How is the conduct required by the notice proportionate to what you are seeking to achieve?** *[the application must set out how what the telecommunications operator is being asked to do is proportionate to the objective sought]*

- **Will the activity proposed interfere with an individual's privacy?** *[The application must set out: known/expected interference or where there is a potential for interference to occur; explain why the interference is necessary and describe any mitigating action which will be taken to keep the interference to a minimum.]*

- **Is another warrant or authorisation required?**
  [Where a national security notice requires the taking of a step for which a warrant or authorisation under the IPA, ISA, RIPA, or RIPSA is required, the application must explain that such an authorisation or warrant will be obtained and the conduct the authorisation or warrant is expected to authorise.]

- **Is it reasonable to require the operator to take the steps set out in the notice? Provide details of the consultation. Confirm that has taken place with the telecommunications operator to whom the notice will be given** *[The application should highlight any concerns which have been expressed by the intended recipient during the consultation period and describe what action has been/can be taken to mitigate their concerns. The application should also set out the period within which the steps specified in the notice are to be taken and an assessment of why that period is reasonable.]*

- **Is the telecommunications operator on whom the notice is to be given uniquely placed to undertake the activity required by the notice or are other operators subject to similar obligations?**

ANNEX B: Example of a National Security Notice

INVESTIGATORY POWERS ACT 2016
Section 252(1)

DRAFT NATIONAL SECURITY NOTICE

Notice Number:

To be completed after Judicial Commissioner approval:

Date Given:

To <*insert name of telecommunications operator*>

In exercise of the power conferred on me by section 252(1) of the Investigatory Powers Act 2016 ("the Act") I hereby require that <*insert name of telecommunications operator*> take the following steps in the interest of national security:

1. <*list steps*>
2.

The steps specified in this notice are to be taken by <*insert date*>.

This notice does not require the taking of any steps the taking of which would, in the absence of this notice, be lawful only if a warrant or authorisation under the Act, the Intelligence Services Act 1994, the Regulation of Investigatory Powers Act 2000, or the Regulation of Investigatory Powers (Scotland) Act 2000.

or

This notice requires the taking of steps which, in the absence of this notice, would be lawful only if authorised by a warrant or authorisation under a relevant enactment. The following warrants or authorisations <*insert details of warrant or authorisation*> are required to authorise <*specify the relevant step(s)*>.

I have determined that the level(s) of contribution that should be made in respect of costs incurred, or likely to be incurred, by <*insert name of telecommunications operator*> in complying with this notice is as follows: <*insert appropriate level(s) of contribution*>.

Revocation of notices or directions

In exercise of the power conferred on me by section 256(3)(b) of the Act, I hereby revoke the national security notice given to *<insert name of telecommunications operator>* on *<insert date>*.

or

The direction given under section 94 of the Telecommunications Act 1984 to *<insert name of telecommunications operator> on <insert date>* is hereby revoked.

Secretary of State decision to issue

I consider that the notice is necessary in the interests of national security and that the conduct required by the notice is proportionate to what is sought to be achieved.

_____ Date of Signature:

Secretary of State

Judicial Commissioner approval of decision to issue

Having reviewed the Secretary of State's conclusions as to whether this notice is necessary in the interests of national security and whether the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, I have approved the Secretary of State's decision to issue the warrant.

_____ Date of Signature:

Judicial Commissioner

Internal Reference: