REVISED EXPLANATORY MEMORANDUM TO

THE INVESTIGATORY POWERS (CODES OF PRACTICE) REGULATIONS 2018

[2018] No. [XXXX]

1. Introduction

1.1 This explanatory memorandum has been prepared by the Home Office and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 The instrument brings into force five codes of practice regarding functions carried out under the Investigatory Powers Act 2016 ("the Act"). Those five codes of practice relate to: the interception of communications; equipment interference; the bulk acquisition of communications data; national security notices; and the intelligence services' retention and use of bulk personal datasets.

3. Matters of special interest to Parliament

Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None

Other matters of interest to the House of Commons

3.2 Disregarding minor or consequential changes, the territorial application of this instrument includes Scotland and Northern Ireland.

4. Legislative Context

4.1 Paragraph 1 of Schedule 7 to the Act requires the Secretary of State to issue codes of practice about the exercise of functions conferred by virtue of the Act.

4.2 Paragraph 6 of Schedule 7 to the Act sets out the effect of the codes of practice. A person must have regard to the codes when exercising any functions to which the codes relate. The codes are admissible as evidence and a court or tribunal may take into account a failure to have regard to them.

5. Extent and Territorial Application

5.1 The extent of this instrument is the whole of the United Kingdom.

5.2 The territorial application of this instrument is the whole of the United Kingdom.

6. European Convention on Human Rights

6.1 The Minister of State for Security, Rt Hon Ben Wallace MP, has made the following statement regarding Human Rights:

"In my view the provisions of The Investigatory Powers (Codes of Practice) Regulations 2018 are compatible with the Convention rights."

7. Policy background

What is being done and why

7.1 Schedule 7 to the Act requires codes of practice about the exercise of the functions conferred by the Act to be issued. The Government intends to issue six codes of practice.

7.2 The five codes brought into force by these Regulations and a summary of the provisions they cover are set out below.

7.3 **Interception of Communications:** this code relates to the exercise of functions conferred by Part 2 and Chapter 1 of Part 6 of the Act, covering powers of targeted interception (which also include targeted examination warrants) and bulk interception respectively. These powers enable the interception of a communication in the course of its transmission such that the content of the communication is made available to someone other than the sender or intended recipient. The Act makes it a criminal offence to intercept the communications of a person in the UK without lawful authority and stipulates what constitutes lawful authority to do so. On way in which a public authority may have lawful authority to intercept communications where they have a warrant issued by the Secretary of State. Such a warrant may only be issued where it is necessary and proportionate on one or more of three statutory grounds (in the interests of national security, for the prevention and detection of serious crime and in the interests of the economic well-being of the UK, so far as those interests also relate to national security). The decision to issue interception warrants are also subject to approval by a Judicial Commissioner. Targeted interception warrants are primarily an investigative tool that enable the interception of communications in relation to a specified subject matter such as an individual person or a group of persons carrying out a particular activity or sharing a common purpose, for example an organised crime group. Targeted interception warrants may only be sought by a small number of public authorities, limited to the intelligence services, certain law enforcement bodies (The Metropolitan Police Service, the National Crime Agency, Police Scotland, the Police Service of Northern Ireland and HMRC) and the Ministry of Defence. The primary purpose of bulk interception warrants is to authorise the interception of overseas-related communications and the subsequent selection for examination of the intercepted material. Bulk interception is primarily an intelligence gathering tool that is used, for example, to identify previously unknown threats to the national security of the UK. Such a warrant may result in the acquisition of large volumes of data that may only be selected for examination for an operational purpose specified on the warrant. Bulk interception warrants may only be sought by the intelligence services and must always be necessary in the interests of national security.

7.4 **Equipment Interference:** this code relates to the exercise of functions conferred by Part 5 and Chapter 3 of Part 6 of the Act, covering powers of targeted equipment interference (which also include targeted examination warrants) and bulk equipment interference respectively. Equipment interference describes a range of techniques used by the equipment interference authorities that may be used to obtain communications, equipment data or other information. Equipment interference can be carried out either remotely or by physically interacting with the equipment. Equipment interference operations vary in complexity. At the lower end of the complexity scale, an equipment interference authority may covertly download data from a subject's mobile device when it is left unattended, or may use someone's login credentials to gain access to data held on a computer. More complex equipment

interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device. As with targeted interception, targeted equipment interference warrants are primarily an investigative tool and are used to interfere with the equipment of specified subject matter. For equipment interference operations such subject matters might include the equipment of an individual person or in a specified location. Targeted equipment interference warrants may only be sought by a limited number of public authorities such as the intelligence services, law enforcement agencies (including police forces, the National Crime Agency, HMRC and immigration and customs authorities) and certain oversight bodies such as the Independent Police Complaints Commission. Targeted equipment interference warrants may only be sought on one or more of the same three statutory grounds as targeted interception warrants. In addition, certain equipment interference authorities may only seek warrants for specified limited purposes. For example, an immigration officer may only seek an equipment interference warrant in relation to a serious crime that is an immigration or nationality offence. Bulk equipment interference warrants enable interference with equipment for the purpose of obtaining overseas-related communications, equipment data or other information and also authorise the selection for examination of the material obtained for operational purposes specified on the warrant. As with bulk interception, bulk equipment interference warrants are primarily used as an intelligence gathering tool, may only be sought by the intelligence services and must be necessary in the interests of national security.

7.5 **Bulk Acquisition of Communications Data:** this code relates to the exercise of functions conferred by Chapter 2 of Part 6 of the Act. Bulk acquisition warrants authorise both the obtaining of communications data (the context of a communication but not its content) in bulk from a telecommunications operator and the selection for examination of the data obtained under the warrant. This may result in the collection of large volumes of data, which is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation. Given that the acquisition of bulk communications data is an intelligence gathering capability, the Act does not impose a limit on the volume of communications that may be collected and, unlike targeted communications data authorisations under Part 3 of the Act, a bulk acquisition warrant need not be constrained to a specific investigation. Given the large volume of communications data that may be obtained, acquisition warrants may only be sought by the three intelligence services and must be issued by the Secretary of State only where necessary and proportionate and subject to approval by a Judicial Commissioner. A bulk acquisition warrant may only be issued where necessary in the interests of national security, for the prevention and detection of crime or in the interests of national security so far as those interests also relate to national security. As with bulk interception and bulk equipment interference warrants, national security must always be one of the grounds on which such a warrant is issued. Once acquired in bulk, selection of data for examination is only permitted for operational purposes specified on the warrant.

7.6 **National Security Notices:** this code relates to the exercise of functions regarding national security notices, which may be given under section 252 of the Act. The Secretary of State may give a national security notice to a telecommunications operator only where the Secretary of State considers that the notice is necessary in the interests of national security and proportionate. Such a notice must be approved by a

Judicial Commissioner. A national security notice may require the taking of such specified steps as the Secretary of State considers are necessary in the interests of national security. In particular, a national security notice may require an operator to: carry out any conduct for the purpose of facilitating anything done by an intelligence service; carry out any conduct for the purpose of dealing with an emergency; or provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively. However, a national security notice may not have as its main purpose something for which an authorisation under a relevant enactment would be required. For example, a national security notice could not be used as an alternative to an interception warrant where such a warrant is required to authorise the relevant activity.

7.7 **Intelligence Services' Retention and Use of Bulk Personal Datasets:** this code relates to the exercise of functions conferred by Part 7 of the Act. The intelligence services need to obtain a range of information from a variety of sources to meet the requirements of their statutory functions. They do this in accordance with the Security Service Act 1989 and the Intelligence Services Act 1994. Among the range of information obtain are bulk personal datasets: a dataset including personal data in relation to a number of individuals where the nature of that dataset is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the intelligence services in the exercise of their statutory functions. A bulk personal dataset is, or is to be, held electronically and will typically be very large. The Act does not create any new powers to obtain such datasets. Rather, it requires that the retention and use of these datasets by the intelligence services must be subject to an authorisation scheme and robust and transparent safeguards. The Act enables an intelligence service to obtain two kinds of warrant in relation to bulk personal datasets. First, a class warrant that authorises an intelligence service to retain, or retain and examine, datasets that fall within a class specified in the warrant (for example, a warrant authorising an intelligence service to retain and examine travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness). Second, a specific warrant that authorises an intelligence service to retain, or retain and examine, the particular dataset described in the warrant. Any bulk personal dataset warrant (of either type) must be issued by the Secretary of State and must be approved by a Judicial Commissioner. Such warrants may only be issued in the interests of national security, for the prevention and detection of serious crime or in the interests of the economic well-being of the UK, so far as those interests also relate to national security. Data contained within a bulk personal dataset may only be selected for examination where necessary and proportionate for an operational purpose specified on the warrant.

7.8 The intention is that a sixth code of practice, about communications data, will be brought into force at a later date.

7.9 Each of the five codes sets out the processes and safeguards governing the use of the relevant investigatory powers by public authorities. They give detail on how the relevant powers should be used, including examples of best practice. They are intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with this important legislation.

7.10 These codes are primarily intended to guide those public authorities which are able to exercise powers under the Act. They provide information on the processes associated with applying to use, and using, each of the powers, as well as the safeguards and

oversight arrangements that will ensure the powers are used in the intended manner. The codes will also be informative to staff of telecommunications and postal operators which may be served with warrants or given notices under the Act.

7.11 The codes contain guidance in relation to a number of matters, including those set out below. To the extent possible and appropriate the five codes of practice set out guidance in relation to these processes and safeguards in a consistent manner:

- definitions of key terminology used throughout the codes of practice;
- details of the information that public authorities must include in an application to use the relevant powers;
- the format of, and detail that must be included in, a warrant or notice;
- the matters which much be considered and processes that must be adhered to by the issuing authority as part of the authorisation process;
- details about the circumstances in which warrants may be renewed and the circumstances in which warrants must be cancelled or notices revoked;
- where giving effect to warrants may require the assistance of other persons, such as telecommunications operators, guidance in relation to: how warrants should be served on such persons, the documentation that may be provided, and information about steps that such persons are required to comply with;
- the safeguards that apply in relation to the retention, storage, copying, destruction and dissemination of material obtained using the relevant investigatory powers;
- where relevant, details of the safeguards that apply in relation to particularly sensitive forms of information, such as: items subject to legal professional privilege, confidential journalistic information, and information that might reveal the identity of a journalist's source;
- details of the records that must be kept by public authorities when utilising the relevant powers to facilitate oversight by the Investigatory Powers Commissioner.

Consolidation

7.12 Not applicable.

8. Consultation outcome

8.1 A public consultation on the Investigatory Powers Act Codes of Practice was carried out between 23 February 2017 and 6 April 2017. The response to the consultation was published at the same time that the draft codes were laid in Parliament and is available at www.gov.uk/government/consultations/investigatory-powers-act-2016-codes-of-practice.

8.2 In total, there were 1098 responses to the consultation. Of those responses, 32 were from members of the public, academics, and representatives from legal bodies, media organisations, an oversight body, privacy groups, and technology companies. The remaining 1066 responses were from other members of the public responding to a request made by the Open Rights Group, who encouraged members of the public to submit identical responses to the consultation based on a template they had provided.

8.3 Significant constructive feedback was received in response to the consultation and consequently a number of changes have been made to the codes of practice in relation to a number of issues, including (among other things): the legal status of the codes; definitions; judicial commissioner approval and oversight; record keeping regarding errors; processes for sharing material; and the safeguards that apply to sensitive or privileged information. Further detail is set out in the Government's response to the consultation.

9. Guidance

9.1 The Codes of Practice brought into effect by this instrument contain guidance, including guidance about the effect of the Codes as set out above.

10. Impact

10.1 There is no impact on business, charities or voluntary bodies.

10.2 There is no impact on the public sector.

10.3 An Impact Assessment has not been prepared for this instrument. However, the codes of practice are about the exercise of functions under the Act and a full impact assessment was prepared for that legislation. That impact assessment concluded that the cost of the primary legislation itself (as opposed to the codes of practice brought into force by these regulations) would be £247.5 million to the Government. That figure primarily related to the costs of establishing the Investigatory Powers Commissioner and his office and the ongoing running costs, compliance and reimbursement to business of costs associated with the new communications data provisions in the Act (which are not relevant to these codes of practice).

10.4 There is no impact on telecommunications operators or postal operators. Section 249 of the Act requires the Secretary of State to ensure arrangements are in force for securing that operators receive appropriate contribution in respect of their relevant costs. Government policy is that the appropriate contribution is calculated on a case by case basis to ensure that an operator makes neither a gain nor a loss from complying with the Act.

11. Regulating small business

11.1 There is no impact on small business. The regulations and codes of practice in and of themselves do not impose requirements on small businesses, rather they set out guidance and best practice, primarily for public authorities, in relation to the exercise of investigatory powers. However, the exercise of powers under the Act could apply to small businesses. To minimise the impact of the requirements on small businesses (employing up to 50 people), there are stringent safeguards regulating the use of powers in the Act, including tests of necessity and proportionality and, in certain circumstances, approval by a Judicial Commissioner.

11.2 The Act also makes clear, at section 249, that the Secretary of State must ensure that arrangements are in force for securing that relevant operators receive an appropriate contribution in respect of such of their costs incurred in complying with the Act as the Secretary of State deems appropriate.

12. Monitoring & review

12.1 Section 260 of the Investigatory Powers Act 2016 requires the Secretary of State to report on the operation of the Act, after a period of 5 years and 6 months from Royal Assent. The report must be published and laid before Parliament. In preparing the report the Secretary of State must take into account any report on the operation of the Act produced by a Select Committee of either House.

13. Contact

13.1 Home Office Public Enquiries; public.enquiries@homeoffice.gsi.gov.uk; 0207 035 4848.