Northern Ireland Office

Secretary of State's Guidance to the Independent Reporting Commission under section 2(5) of the Northern Ireland (Stormont Agreement and Implementation Plan) Act 2016

Contents

Secretary of State's Statutory Guidance to the Independent Reporting Commission – disclosures connected with national security or risk to life or safety

Introduction and statutory framework

1) Section 1 of the Northern Ireland (Stormont Agreement and Implementation Plan) Act 2016 ("the Act"), and paragraph 5.1 of the Fresh Start Agreement, make provision for an Independent Reporting Commission ("the Commission") to be established by agreement between the Government of Ireland and the Government of the United Kingdom. The agreement, hereafter referred to as "the Treaty", was signed by the UK Government and the Government of Ireland on 13 September 2016.

2) The Commission's objective is to carry out its functions with a view to promoting progress towards ending paramilitary activity connected with Northern Ireland, and supporting long term peace and stability in society and stable and inclusive devolved Government in Northern Ireland. The Commission's functions, which are set out in paragraph 5.1 of the Fresh Start Agreement, and in Articles 4 and 5 of the Treaty, are to:

   - report annually on progress towards ending continuing paramilitary activity connected with Northern Ireland (or on such further occasions as jointly requested by the Government of the United Kingdom and the Government of Ireland);
   - report on the implementation of the relevant measures of the three administrations; and
   - consult the UK Government and relevant law enforcement agencies, the Irish Government and relevant law enforcement agencies and, in Northern Ireland, the Northern Ireland Executive, PSNI, statutory agencies, local councils, communities and civic society organisations.

3) The Secretary of State for Northern Ireland remains responsible for national security matters following devolution of policing and justice in 2010, by virtue of Section 4 of, and Schedule 2 to, the Northern Ireland Act 1998 and is required, by virtue of Section 2(5) of the Act, to issue this guidance about the exercise of the Commission's functions in relation to information the disclosure of which might (a) prejudice the national security interests of the United Kingdom, or (b)put at risk the life or safety of any person. The Commission is required, by virtue of Section 2(6) of the Act, to have regard to this guidance in exercising its functions.

4) In carrying out its work the Commission must act consistently with the statutory duty conferred upon it by Section 2(3) of the Act and by the Northern Ireland (Stormont Agreement and Implementation Plan) Act 2016 (Independent Reporting Commission) Regulations 2016, and accordingly must not do anything which might:

- prejudice the national security interests of the United Kingdom or Ireland;
- put at risk the life or safety of any person;
- have a prejudicial effect on the prevention, investigation, detection or prosecution of crime; or
- have a prejudicial effect on any actual or prospective legal proceedings.

5) In order to fulfil its objective, and in light of the functions and the range of bodies the Commission will consult in the course of its work, it is likely that the Commission will receive information which could, if disclosed, be prejudicial to the national security interests of the United Kingdom. This guidance therefore draws together the principles and arrangements for managing national security sensitive information so as to ensure that the Commission can carry out its responsibilities effectively and that the national security interests are also properly protected.

6) Some of the national security sensitive information provided to the Commission will also be information the disclosure of which might put at risk the life or safety of a person. This guidance therefore also provides guidance to the Commission in complying with its duty not to put at risk the life or safety of any person, by ensuring the proper protection of such information.

7) Any reference in this guidance to the Commission's "staff" includes reference to persons employed by, or providing assistance to, the Commission.

Sensitive information

8) In this Guidance "sensitive information" means information which if disclosed generally might prejudice the national security interests of the United Kingdom or put at risk the life or safety of any person.

9) Such information may be provided by any individual or organisation (whether to the Commission or to some other person) and could include the following organisations: the Security Service; the Secret Intelligence Service; GCHQ (which has the same meaning as in the Intelligence Services Act 1994); any part of Her Majesty's forces, of the Ministry of Defence, or of the Police Service which engages in intelligence activities.

10) Where sensitive information, from any source, is disclosed to the Commission, the Commission should adhere to the principles for handling and storing sensitive information, for the return or destruction of sensitive information, and for disclosing sensitive information outlined below.

11) The Commission will be notified by the information provider when information being shared constitutes sensitive information and should therefore be treated in accordance with this Guidance.

12) Requests by the Commission for information should be made to the relevant point of contact within the organisation which holds the information in accordance with the procedure agreed between that organisation and the Commission. The Commission will need to comply with the requirements set out by the relevant organisation for the disclosure and, where relevant, review of information held by that organisation.

Handling and storage of sensitive information

13) The Commission should ensure there are arrangements in place for securing at all times access to, and handling and storing of , sensitive information in accordance with the following (collectively referred to in this guidance as "the national standards")[1]:

(i) HMG Security Policy Framework (Cabinet Office);

(ii) HMG Personnel Security Controls (Cabinet Office);

(iii) Government Security Classifications (Cabinet Office);

(iv) Physical Security (Cabinet Office);

(v) Working with SECRET and TOP SECRET information (Her Majesty's Government).

14) In order to assist the Commission in ensuring the arrangements mentioned in paragraph 13 are fully and adequately in place, the Commission should consult with appropriately qualified individuals appointed by the Secretary of State ("qualified officials") to provide advice and assistance on meeting the national standards.

15) As part of that consultation, the qualified officials may wish to inspect, report and advise on the facilities, systems and processes for secure handling and storage of sensitive information maintained by the Commission ("the Commission's security arrangements"). Whilst the Commission has inviolability of premises, it should, in line with national standards, arrange to provide the qualified officials access to its security arrangements to enable them to conduct such an exercise.

[1] These documents may be updated from time to time. The latest versions of these documents will be provided to the Commission and any revisions will be notified to the Commission.

16) In the event that the Commission's security arrangements are found not to accord with the national standards, the qualified officials will provide feedback on the reasons for this and advice on how the deficiencies can be remedied.

17) If at any time the qualified officials are not content that the Commission can fully comply with the national standards, the Commission should return all sensitive information in its possession which cannot be held and stored in accordance with the national standards, and instead make arrangements to review the sensitive information at the information owner's offices.

18) The national standards set out the detailed guidance for accessing, handling and storing sensitive information. Within the national standards, here are a number of key principles which the Commission should note in particular, including that:

(i) access to sensitive information must only be given to authorised individuals who hold the level of security vetting appropriate to the security classification of that information and any special handling instructions;

(ii) access to sensitive information must only be given to individuals on the basis that the information is directly relevant to the Commission's work and to it fulfilling its functions;

(iii) individuals who access sensitive information have a duty of confidentiality and a responsibility to safeguard that information, and must be provided with appropriate training, including notification that an unauthorised disclosure of such information may be an offence under the Official Secrets Act 1989;

(iv) where the sensitive information is in electronic form, it must be accessed, handled and stored only in accordance with national standards (see para 13);

(v) appropriate physical security controls are required for protecting sensitive information;

(vi) sensitive information should never be taken off-site without prior authorisation by the information owner;

(vii) lost or stolen sensitive information must be reported immediately to the owner and to the NIO.

Return or Destruction of sensitive information

19) The Commission should ensure there are arrangements for securing that at all times Commissioners, persons employed by, or providing assistance to, the Commission destroy sensitive information in accordance with national standards on secure destruction of sensitive material.

20) Alternatively, once the Commission ceases to require the sensitive information disclosed to it for the discharge of its functions, the Commission should securely return the sensitive information (including any copies or notes) to the information owner together with written confirmation that the sensitive information and any reference to it has been deleted from all of the Commission's computerised or other electronic records, to include removal from the hard-drive, i.e. to destroy that information in accordance with the national standards on the secure destruction of sensitive material.

Disclosure of sensitive information

21) Sensitive information may contribute to the reports to be published by the Commission in accordance with its statutory functions or to other statements or disclosure to the public that the Commission may wish to make. The disclosure of sensitive information may, by its nature, be prejudicial to the national security interests of the United Kingdom, or put at risk the life or safety of a person. Disclosure of such information should therefore be approached carefully to ensure that national security interests are not prejudiced, and that the life or safety of a person is not put at risk and the Commission should seek advice from the Secretary of State or relevant agency accordingly.

22) Where a draft report or other proposed publication by the Commission ("draft publication") contains or makes reference to the existence of sensitive information, the Commission should refer that draft publication to the Secretary of State prior to its publication or dissemination outside the Commission's office. The Commission should allow the Secretary of State 30 working days (or such other period as agreed between them) to consider the draft report or other publication and notify the Commission of any concerns he may have about the effect its disclosure would have on national security or on the life or safety of any person.

23) The Commission should have regard to any notification by the Secretary of State that the proposed disclosure would prejudice national security interests or would put at risk the life or safety of any person. Where the Secretary of State identifies such a risk the Commission should liaise with the Secretary of State, or the relevant agency nominated on the Secretary of State's behalf, to agree an acceptable way forward. It may not always be feasible to "gist", summarise or refer to the sensitive information in a way which does not pose a risk to national security or to the life or safety of

another person. In some instances it may involve redacting the sensitive information entirely. The Commission should ensure that the Secretary of State or relevant agency is content that there is no risk of prejudice to national security or to the life or safety of any person before the report or other proposed publication is published or information disseminated outside the Commission's office.

Useful information - NCND principle

24) It is a longstanding principle of Her Majesty's Government that it will neither confirm nor deny allegations or assertions relating to intelligence matters and, in particular, claims that individuals have or have not assisted public authorities by providing information or other assistance in confidence ("the NCND principle"). The NCND principle also extends to the existence or otherwise of sensitive intelligence operations or information in the possession of the Security Intelligence Agencies and /or other agencies.

25) In order to be effective, the NCND response must be applied consistently, including when no activity has taken place and a denial could properly be made. If the Government denied a particular activity in one instance, the inference might well be drawn that the absence of a denial in another amounted to confirmation of the alleged activity. In Re Scappaticci [2003] NIQB56 Carswell LCJ explained the basis of the maintenance of NCND as follows: "*to state that a person is an agent would be likely to place him in immediate danger from terrorist organisations. To deny that he is an agent may in some cases endanger another person who may be under suspicion from terrorists. Most significant, once the Government confirms in the case of one person that he is not an agent, a refusal to comment in the case of another person would then give rise to an immediate suspicion that the latter was in fact an agent, so possibly placing his life in grave danger... There is in my judgment substantial force in these propositions and they form powerful reasons for maintaining the strict NCND policy*".

26) It is accepted that the NCND policy may be departed from in a particular case if there is an overriding and exceptional reason to do so. However the effectiveness of the policy in protecting national security and protecting individuals' Article 2 (right to life) and 3 (prohibition on torture and inhuman or degrading treatment) ECHR rights is undermined if it is not applied consistently.

27) In exercising its functions, the Commission and its staff should have regard to the NCND policy and should consult the Secretary of State with any queries regarding that policy in order to ensure that national security interests or an individual's Article 2 and 3 ECHR rights are not prejudiced. Where the Commission wishes to depart from the NCND principle they should refer the matter to the Secretary of State in advance to consider the matter and the Secretary of State should notify the Commission of

any concerns. A departure from the NCND principle may exceptionally be made in cases concerning the Security Service only when the Security Service and the Commission, having consulted with the PSNI as appropriate, agree in writing that it is justified in the particular case in accordance with the policy of HMG.