Briefing note to the Minister for Justice and Equality
10 February 2014

This Commission was appointed on 12 December 2011. From an early stage, we talked about security and risks to our building. Even before this Commission, security checks were conducted by external specialist companies for the organisation.

In the course of our operations, the Commission has always been conscious of the need for appropriate confidentiality and proper levels of security. The Commission has brought to the attention of its staff the need to respect confidentiality of investigations and only to make appropriate contact with third parties.

On 23 to 27 September 2013, in accordance with standard operating procedures, a security sweep was conducted of GSOC's Head Office. This was conducted by a UK security firm as the Irish firm that had previously conducted such operations for GSOC had gone out of business. To ensure a significant degree of independence, the Commission decided to contract a UK security firm (Verrimus) that had been recommended to us as having previously done work for a credible agency with which we have a working relationship.

The overall cost of the security checks undertaken in late 2013 was just under €18,000. As well as the general check of our building, the Commission also sought expert advice on the sorts of capabilities that exist in relation to the interception of ICT communications (including telephones).

Two potential threats were identified during this security sweep of 23 to 27 September 2013.

Threat 1: a Wi-Fi device, located in the Boardroom (the Commission's conference room), was found to have connected to an external Wi-Fi network. Access to this Wi-Fi device was protected by a password; absent this password, the device should not have been able to connect to that external Wi-Fi network. As GSOC does not have a Wi-Fi network, this device had never been activated by GSOC and its password was unknown. Its connection to an external network was, therefore, a concern. This device, although Wi-Fi enabled, was unable to communicate with any of GSOC's databases or electronic systems.

Threat 2: as part of the security checks, the conference call telephone unit located in the Chairman's office was subjected to a number of tests. One of the tests involved sending an audio signal down the telephone line; this is known as an "alerting" test as it presents the possibility that a listener will hear this audio signal. Immediately after the transmission of this audio signal, the conference phone line rang. The Verrimus operator judged that the likelihood of a "wrong number" being called at that

time, to that exact unknown number, at the time of an alerting test, was so small as to be at virtually zero. GSOC conducted a number of telecoms checks to seek to establish the source of this telephone call but was unable to do so. Further checks revealed no additional anomalies or matters of concern.

On 7 October 2013, after confirmation paperwork was received from the specialist firm, the investigation team assessed these two threats. On 8 October 2013, a public interest investigation was launched pursuant to section 102(4) of the Garda Síochána Act, 2005. The investigation was launched on the basis that the Acting Director of Investigations was of the opinion that, to the extent that these threats could be proven, section 102(4) engaged – that is to say that such surveillance may have originated with AGS and, if so, a member of AGS may have committed an offence or behaved in a manner that justified disciplinary proceedings. The investigation was launched in the public interest to ensure that the objectives of GSOC, as set out in section 67(1) of the Act, were not compromised or impugned.

As part of that investigation, the specialist firm was re-engaged and a number of steps were undertaken, including accessing retained telecommunications. During the course of the investigation, the specialists advised regarding the risks of interception to mobile telephony. The Commission established that commercial products were available that could – for example - intercept mobile phones, take them over, send and delete texts from them, etc.

Threat 3: during a visit by the specialist firm on 19 and 20 October 2013, it detected a UK 3G network. UK networks do not operate within Ireland except in Border areas. They advised that such a network can only be simulated through a device called an "IMSI catcher". An IMSI catcher, in simulating a UK mobile phone network, will pick up UK phones registered to that network. Once a phone has been connected to the IMSI catcher, it can be forced to disable call encryption making the call data vulnerable to interception and recording. The specialist firm indicated that this level of technology is only available to Government agencies.

Preliminary Results:
Analysis of these threats was inconclusive. GSOC was operating at the limits of its technical knowledge and on information from security professionals. The Commission did not rule out that there could be reasonable explanations for any/all of these issues, e.g.:

- connection by the Wi-Fi device in the conference room with an external Wi-Fi network was occurring randomly and with no discernible pattern or agent apparent.
- the anomaly in the telephone unit in the Chairman's office could not be repeated – the Commission could not rule out the possibility that an innocent call was made to the office at 1am. Telecoms data could not identify a number from which the call originated or even that a call had been made.
- concerning the IMSI catcher, the Commission could not rule out that such a device was being lawfully used in the vicinity of Capel Street to, for example, counter subversion or organised crime.

Final Test:
Absent any further clarification, the Commission could not simply proceed on the basis that these issues were purely innocent or coincidental. Accordingly, the Commission conducted a specific operational test, on 19 November 2013; this was coordinated by the security firm and involved a GSOC investigation team and the three Commissioners to test these issues. This operational test yielded no results and added no clarity to the threats identified above.

Conclusion:
The investigation was completed on 17 December 2013 and concluded that no definitive evidence of unauthorised technical or electronic surveillance was found. It did, however, confirm the existence of the three technical and electronic anomalies set out above that could not – and still cannot - be explained. These raised concerns among the investigation team in terms of the integrity of GSOC's security.

A Designated Officer furnished the closing report on 17 December 2013.

On the basis of that report, it was decided that no further action was necessary or reasonably practicable. The investigation was discontinued.

GSOC suspects that this investigation report may be with the journalist who first reported the matter. If it is, there is an inaccuracy referenced in three places in the report as to the commencement of the investigation. The Commission is undertaking an inquiry into any possible leak that may have occurred.

Since the investigation concluded, GSOC has been working to review and enhance our security systems in the light what the investigation revealed. There are still some inconclusive issues in relation to the outcome of this investigation. The identified ongoing risks to our ICT security are being addressed.

The Commission has not reported this investigation more widely. We clearly want to maintain public confidence. We regret that decision; it was made with the very best of intentions.

Garda Síochána Ombudsman Commission