# INQUIRY INTO THE DEATH OF DAWN STURGESS

## HER MAJESTY'S GOVERNMENT'S RESPONSE TO THE NOTE FROM COUNSEL TO THE INQUIRY DATED 10 JUNE 2022

1. This Note responds to specific queries raised by Counsel to the Inquiry ["CTI"] arising from HMG's application for a restriction order in respect of the names of HMG staff.

**Definition of HMG staff**

2. HMG's application is intended to apply to all staff and former staff, with the specified exceptions set out in paragraph 2 of the OPEN application of HMG. The definition of "HMG staff" includes military personnel and reservists; and staff employed by any agency linked to a central government department (or departments). The definition excludes local government staff and emergency services personnel. The key distinction is that HMG staff are or were employed by a national government body of some sort; those excluded from the definition are or were employed by local or regional bodies.

3. The definition of "HMG staff" also includes contractors and experts engaged by HMG. Again, the contractors and experts covered by the definition are those who were engaged by a central government department or agency. For the purposes of this Restriction Order application, the only contractors and experts likely to be relevant are those who undertook some work for HMG on matters relating to the events of 2018 that are being investigated by the Inquiry. Individuals in this category include those who were not employed by HMG but acted in an official capacity as advisers, for example as a SAGE participant or adviser to a specific policy team in HMG. These individuals are included because they will be subject to similar risks to those faced by HMG employees, as set out in the HMG damage assessment. If named they could be targeted for the information they have or for their contacts within HMG. Many external experts engaged by HMG have extensive contacts in HMG and can work on very sensitive HMG material.

4. HMG does not seek a restriction on publication of the names of Senior Civil Servants "officially publicly linked" to the events of 2018. HMG regards a public link as "official" if there has been public confirmation by a central government department of the individual's role in these events, or when the individual in question has been authorised by a central government department to avow that individual's role in relation to the events.

5. HMG's application is for a Restriction Order in respect of the names of all those below the rank of SCS or one star in military rank equivalent, regardless of whether there has been any official public link between any such individuals and the relevant events of 2018. HMG submits that the appropriate course is for all such names to be redacted at this early stage of the Inquiry when disclosure is incomplete and the relevance of specific individuals and their roles is not yet established.

6. HMG has not attempted to create a list of those above (or below) SCS who have been publicly linked, whether officially or unofficially, with the events of 2018. Such a task would be immensely time-consuming. HMG respectfully submits that this would be a disproportionate use of finite resources, and that it would be preferable to revisit the question of whether individuals are publicly linked with relevant events once (a) disclosure is complete, or at least substantially so; and (b) the Inquiry has identified the documents it regards as relevant and the witnesses from whom it wishes to obtain evidence.

**The use of Relativity**

7. HMG recognises the need for the Inquiry to have a platform for document sharing, and agrees that Relativity can be used for documents in OPEN. HMG assesses that while Relativity has some security controls in place, these are insufficient to protect the system from cyber attack or hacking by a sophisticated cyber actor like the Russian Federation (Russia). Relativity is a commercial off the shelf product, and is therefore not designed to be – nor marketed as – a system that can provide protections against a determined hostile state actor.

8. Whilst HMG readily acknowledges that Relativity, or similar systems, have been used to hold documents in recent inquiries or inquests into mass casualty or otherwise high

profile killings, this Inquiry is wholly different because of the capabilities and motivations of Russia when compared to, for example, terrorist groups. HMG assesses that the security of Relativity is not sufficiently robust for the system to be used to store any information that would be detrimental to national security if accessed by Russia. This includes wider sensitive information such as names of those HMG staff involved in national security-related work.

**Vulnerability of others named in documents**

9. HMG has been asked to consider whether the risks that it has identified in respect of its own staff might apply similarly to others such as health or emergency workers, local government employees, police officers other than counter-terrorism officers, and lay witnesses. There might also be risks to others referred to in HMG's disclosure, for example international partners such as OPCW.

10. There are two aspects of risk to any individual: (i) the risk that the individual may be specifically targeted, for example by cyber means; and (ii) the risk that information relating to that individual (e.g. a name linked to an email address or job title) might be used by Russia to further other intelligence aims, for example: to aid phishing attempts to access data systems; to aid understanding of structures, teams and capabilities within HMG; and to identify other HMG staff to target.

11. HMG assesses that those individuals who could not reasonably be expected to have knowledge or access useful to Russia are less likely to be targeted than those that do. Therefore, for example, neighbours of Charlie Rowley or of the Skripals, interviewed as part of house-to-house inquiries and who had little of evidential value to say, or those officers that conducted the interviews, are less likely to be targeted. Whereas HMG staff or CTP officers that work with, or have worked with, UKIC on policy and/or investigations linked to Russian actors are more likely to be targeted.

**Requests for further information to be made OPEN**

**(i) Russian interest in the Inquiry**

12. As stated in the OPEN application, great care has been taken to include as much information in OPEN while not revealing anything that could create or increase the potential harm posed by Russia, which the application itself seeks to protect.

Disclosing such information in OPEN would therefore present a clear risk to UK national security. Examples of Russian espionage and interference against similar proceedings, which are available in open source, include the Dutch government's MH17 investigation and World Anti-Doping (WADA) Russian doping investigation.

**(ii) The provision to Core Participants of soft copy documents**

13. Making soft copy material containing unredacted names available to Core Participants would require them to comply with a set of extremely stringent restrictions that, in reality, would be unworkable. Whilst HMG has no doubt that Core Participants would in good faith give undertakings to comply with such restrictions, the risk of inadvertent breach of those restrictions, by at least one Core Participant or legal representative at some time over the life of the Inquiry, would be very high indeed.

14. Those known to be in possession of sensitive material (particularly, in this context, the legal representatives of Core Participants) would themselves be at increased risk of being targeted by Russia for cyber attack or even subjected to direct threats.

**(iii)The provision to Core Participants of hard copy documents**

15. The same concerns would arise if Core Participants were given hard copy documents. Again, Core Participants would be asked to comply with conditions that, in practice, some or all of them would inevitably fail to meet, however good their intentions. In addition, the storage of hard copies would create additional risks of those copies being stolen from solicitors' offices, accidentally being left lying around, or copied in breach (innocent or otherwise) of the order.

**(iv)Inspection by Core Participants of hard copy documents at Inquiry premises**

16. Again, exactly the same concerns arise. The Core Participants and their lawyers would find it in practice impossible to make or keep notes or hold discussions without there being a high risk of inadvertent disclosure of sensitive information.

17. In addition, while it is of course a matter for the Inquiry, HMG considers that the logistical burden of making large numbers of documents available for inspection by Core Participants, potentially on multiple occasions, would be immensely difficult.

18. HMG understands fully the need for these Inquiry proceedings to be as open and transparent as possible, and is committed to doing all it can to find practical means to make material available to Ms Sturgess' family, Mr Rowley and to other Core Participants. However, HMG respectfully submits that in this instance there is no safe way in which the names that it seeks to protect may be provided to Core Participants.

CATHRYN McGAHEY QC
RICHARD BOYLE

21 June 2022