Royal Canadian Mounted Police
Commissioner

Gendarmerie royale du Canada
Commissaire

AUG 0 4 2022

Ms. Nancy Vohl
Clerk of the Committee
Standing Committee on Access to Information,
Privacy and Ethics
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Ms. Vohl:

In response to the motion adopted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics on July 26, 2022, concerning:

> *That the committee undertake a study of no more than 2 days, beginning no later than Monday, August 8th, 2022 to determine and identify which "device investigation tools" are being used by the RCMP, which have technological capabilities similar to Pegasus and provide the committee with the name(s) of such software and the terms and conditions of its use;*
>
> *That the committee request, by Thursday, August 4, 2022, that the RCMP provide a list of warrants obtained, if any, for each use of such software, as well as the scope of the warrants and the reasons for the monitoring;*
>
> *That the Committee also request, by Thursday, August 4, 2022, a list of warrants or any other information related to the wiretapping of Members of Parliament, Parliamentary Assistants or any other employee of the Parliament of Canada, for each use of such software;*

The RCMP welcomes the work of the committee and is committed to speak publicly, at the right level of detail, regarding this topic and to work with the Government and review bodies to ensure that the RCMP's use of the tools is

understood and consistent with the law. This is exemplified by the RCMP's recent demonstration of our "On Device Intercept Tools" (ODITs) to the National Security and Intelligence Review Agency (NSIRA), a similar upcoming presentation to the Office of the Privacy Commissioner scheduled for August 23, 2022, our support of the upcoming National Security and Intelligence Committee of Parliamentarians review related to these tools, and Sergeant Dave Cobey's recent publicly available RCMP Gazette magazine article on electronic surveillance challenges and opportunities at **www.rcmp-grc.gc.ca/en/gazette/qa-an-expert-electronic-surveillance-the-challenges-and-opportunities-collecting-evidence** that talks about ODITs.

In response to your request outlined above, the RCMP has provided the enclosed documents to aid the committee's study:

a) ODIT Technical Description: The purpose of this document is to inform about ODITs and describe how an ODIT will be used to carry out the activities for which judicial authorization will be sought. This document is attached to warrants submitted for judicial authorization.

b) Sample Warrant: This document was provided to NSIRA to demonstrate how warrants seeking the use of ODITs are drafted and the specific information that would be provided.

c) RCMP's Covert Access and Intercept Team (CAIT) draft policy on the management of ODITs and other sensitive assets.

d) RCMP's CAIT Assistance Request Form.

Regarding the specific device investigation tools used by the RCMP, including the names of the software and terms and conditions of its use, the above listed documents describe the capabilities of the various tools the RCMP uses, the purpose of their use, authorities required, and other related information. The RCMP can confirm that it has never procured or used Pegasus or any other NSO product. You will not find the specific names of the tools used by the RCMP as sharing those details publicly exposes sensitive information that could negatively impact the RCMP's, and our partners', ability to effectively use ODITs in the future due to the potential that criminal elements would use this sensitive information in order to render the tools ineffective. In addition to negatively impacting RCMP investigations, such exposure could jeopardize investigations of foreign partners and our relations with those countries.

In relation to the request for the list of warrants obtained, if any, for each use of such software, as well as the scope of the warrants and the reasons for the monitoring, there are limits to the information that the RCMP can provide in a public manner without impacting ongoing operations. Enclosed you will find a table that provides a description of the number and type of investigation in

.../3

which ODITs were used. Additionally, the RCMP is able to publicly provide the following information:

> *ODITs are used in extremely limited cases – only used for serious criminal offences and only if approved by a judge who explicitly authorizes the use of ODITs on a specific suspect's device. Their use is always targeted, time-limited, and never to conduct unwarranted or mass surveillance.*
>
> *Since 2017, ODITs have been used in support of 32 investigations in which a combined total of 49 devices were targeted. Of these 32 investigations, the associated Judicial Authorizations listed a total of 144 ODIT devices. However, only 49 devices were actually targeted for ODIT deployment.*

Regarding the request for a list of warrants or any other information related to the wiretapping of Members of Parliament, Parliamentary Assistants, or any other employee of the Parliament of Canada, for each use of such software, this information will not be provided by the RCMP. Any RCMP investigation involving elected officials or employees of the Parliament of Canada would follow the same process and procedures as any other subject of an investigation.

This package provides, to the best of my knowledge, as of August 4, 2022, the RCMP-held information that can be publicly disclosed in response to the above-noted request for production of papers and due diligence line of inquiry.

Kindest regards,

Brenda Lucki
Commissioner

Enclosures