

RESTRICTED

The content of this letter is based on information available to CDF at the time, without reference to information provided by witnesses of the Inquiry.



Headquarters NZDF
Defence House,
Private Bag 39997,
Wellington 6011, New Zealand

T +64 (0)4 496 0999
F +64 (0)4 496 0869
E hqnzdf@nzdf.mil.nz
www.nzdf.mil.nz

08 November 2019

Sir Terence Arnold KNZM QC

Chairperson

Government Inquiry into Operation Burnham and related matters

Rt Hon Sir Geoffrey Palmer KCMG AC QC PC

Member

Government Inquiry into Operation Burnham and related matters

Dear Sir Terence and Sir Geoffrey

Re: Recent correspondence about NZDF email and information management systems

1. Thank you for your letters of 17, 21, and 22 October and 5 November 2019. The Director of the NZDF Special Inquiry Office (SIO) has replied already on the issues raised in your letter of 22 October regarding building access in 2014, and will respond to your letter of 5 November, as requested, by 8 November. This letter replies to the requests in your letter of 22 October related to email and information management systems, and in particular any emails and briefing documents from Colonel (Retired) Jim Blackwell's time as Director of Special Operations (DSO).

Colonel Blackwell's emails and briefing documents from his time as DSO

2. Unfortunately, at the time of the public hearing, the SIO understood, and had advised the Inquiry and all relevant witnesses, that emails exchanged on NZDF classified systems were generally not accessible unless the individual account holder either remained in the organisation (and thus their email accounts remained active), or had saved emails in a currently accessible location (which appears to have been the case with the emails between Peter Kelly and the SNOs deployed in 2010 referred to in your letter). As Secret Wide Area Network (SWAN) accounts such as HQJFNZ.DSO and HQNZDF.DSO no longer exist, it was understood that they could no longer be searched. Through further investigations, we are now aware that the situation is more nuanced and that, in some cases, data remains accessible or has been migrated to other accounts. However, despite considerable efforts, the NZDF has not been able to locate the email that Colonel Blackwell referred to in his evidence. The extensive and increasingly more targeted searching undertaken in an effort to locate the email in question has turned up only a relatively small number of additional potentially relevant emails, which will be provided under separate cover. This new data does not significantly alter the NZDF's understanding of events from the documentary evidence previously located and provided.

RESTRICTED

3. To explain the steps taken and challenges faced in locating classified emails from 2010-11 and 2014, I provide the following comments, which should be read in conjunction with my letter to you of 4 September 2019 on information management and record-keeping.

4. My letter of 4 September 2019 advised the number of items that the NZDF SIO had filtered, reviewed and provided to the Inquiry. Those numbers continue to rise: as of today's date, the SIO has filtered hundreds of thousands of discrete items, largely electronically, by reference to criteria such as date range, file type, keyword or name. Of these, tens of thousands have now been examined in detail by the SIO to locate material of potential relevance, and the material the NZDF is providing to the Inquiry as a result of the searches referred to in this letter is the 111th separate volume.

5. I provide these numbers as context for the explanations about classified email searches that follow, but also in light of the suggestion put to me in cross-examination by Ms McDonald QC that *"...that shows even now that NZDF through this Inquiry process have not been forthcoming in the provision of material to this Inquiry"*.¹ I strongly refute that suggestion, because, as I replied during cross-examination, in fact, my staff at the NZDF have *"worked incredibly hard to provide all documentation they could find"*. It is, of course, the NZDF's responsibility to provide potentially relevant material, and we would all have hoped that the disclosure process would have been completed at an earlier stage. However, in light of the Inquiry's iterative approach where terms of reference are being addressed sequentially through the public hearings and in response to your requests for information, the relevance of certain documents and individuals was not clear – including to the NZDF – at the outset when our focus was on the key allegations that led to the Inquiry's establishment.²

Emails

6. On multiple occasions, NZDF personnel have been directed to provide all potentially relevant data for the Inquiry. The SIO complemented this through active searching of sources considered likely to hold potentially relevant material, beginning with operational and tactical material. A large number of emails was discovered and provided – generally emails that had been saved into accessible shared folders or provided to the SIO by relevant personnel. Following the search of operational and tactical material prioritised as most likely to be relevant, more general searches to locate emails began.

7. Over the course of April and May of this year, my staff met on a number of occasions and exchanged correspondence with the Inquiry Secretariat and Counsel Assisting to discuss how the NZDF might best meet the Inquiry's request for material relating to terms of reference 7.5 - 7.7, and offered to provide briefings on the NZDF's communications systems. Noting the large volume of data, email searches had to be targeted. While it is for the NZDF to determine an effective method to meet its disclosure obligations towards the Inquiry, the keywords, timeframes and individuals' accounts searched were communicated to the Inquiry, and later modified in light of feedback received. The results of those searches were duly provided, and many have been made publicly available.

¹ Inquiry Public hearing 4 transcript, pages 1157 – 1158.

² In this context I wish to clarify some misunderstandings in the discussion with Ms McDonald QC, recorded at pages 1157-1158 of the Inquiry Public hearing 4 transcript, about the bundle containing the IAT report that was exhibited to Mr Hoey's 23 August 2019 affidavit. SIO staff had scanned that bundle from the hard copy into the SIO database in July 2018, but when the scanned bundle was reviewed during the initial disclosure process it was considered to be a collection of drafts, of which the final documents had been disclosed. As a result it was not provided to the Inquiry at that time. The significance of the bundle was not appreciated until the SIO and NZDF counsel began preparing for the Minute 19 hearing, but it is not accurate to say that that was the first time the bundle "came to light" (as Ms McDonald QC put it, at page 1157).

8. Your letter of 24 September 2019 asked the NZDF to search a number of email accounts (at all levels of classification) including accounts used by Colonel Blackwell. Following receipt of that letter, the relevant team from the NZDF Communications and Information Systems (CIS) Branch undertook email searches using specified time periods and keywords. Among other things, the NZDF's letter to you dated 4 October 2019 communicated the parameters of those searches and attached the results of the search for all of Colonel Blackwell's emails on the 'unclassified to restricted' network (DIXS). While the DIXS searches are relatively straightforward, searching emails on the NZDF's fifteen or so secure networks (or, in the case of deployments, subnetworks, some of which are stand-alone) such as SWAN, ~~PSR~~ or SIE (Secret Information Environment) is considerably more challenging. The NZDF's 4 October 2019 letter further advised that searches of classified networks were ongoing, and requested a meeting to discuss how the NZDF could most usefully search for and provide material to the Inquiry.

9. Your letter of 22 October noted Colonel Blackwell's evidence that he received the Incident Assessment Team (IAT) report by email on or shortly before 1 September 2011; sought access to his electronic databases; and, asked the NZDF to confirm that a full search of the DSO SWAN email inbox (or any remaining records of it) had been conducted.

10. SWAN accounts – such as that referred to by Colonel Blackwell in his evidence to the Inquiry – are role-based rather than linked to an individual's name. For CIS to search an individual's SWAN emails, it was necessary to determine, case by case, which SWAN accounts had been associated with particular people at relevant times. This was complicated by factors including:

- a. Over the long time period of interest to the Inquiry, large numbers of people have been associated with multiple different SWAN accounts as they have moved in and out of roles (for example);
- b. SWAN account names for the same job roles have changed over time; and
- c. When the NZDF transitioned from SWAN to SIE beginning in 2017, for various reasons there was not always consistency across the NZDF when data from SWAN accounts was migrated into new SIE accounts.

11. As SWAN account names were able to be associated with relevant personnel during the relevant periods, these accounts were searched using the parameters mentioned in paragraph 8. None of that work turned up accounts still in existence (and thus containing data) that would have been associated with Colonel Blackwell during his time as DSO.

12. Subsequently, the SIO made further enquiries with the Special Operations Component Command office (SOCC – the successor of the former Directorate of Special Operations office) to reconfirm that all potentially relevant locations had been searched. On 10 October 2019, the SIO was informed by the SOCC office of the address for a SOCC 'legacy SWAN' account and that it should also be checked for any DSO emails. This account was searched on 10 October 2019; CIS informed the SIO that nothing of potential relevance was found in that account that matched the key words and/or time periods.

13. On 22 October 2019, after the resumed Public Hearing 4, the SIO contacted the current SOCC (Colonel McKinstry) to reconfirm that he had no way of accessing Colonel Blackwell's emails. With

Colonel McKinstry's permission, a member of his staff was able to locate an archived DSO 'mailbox' in Colonel McKinstry's SIE account, which is identified by his name rather than role. The naming convention and location of this archived DSO account was different from what it had been believed to have been, and it is for this reason that it was not located during earlier searches. It appears that former DSOs, including Colonel Blackwell, used a SWAN role-based account. During Colonel Blackwell's tenure the DSO account name changed multiple times (such as when the role moved from HQNZDF to HQJFNZ). In 2015, Colonel Gillard replaced Colonel Blackwell and took over the SWAN DSO account the latter had been using, which in line with the change to that role, had become the SWAN SOCC account. In 2017, when the migration from SWAN to SIE commenced, material from the SWAN SOCC account was migrated to the SIE account in Colonel Gillard's name. When Colonel McKinstry later replaced Colonel Gillard as SOCC, material from Colonel Gillard's SIE account was moved to Colonel McKinstry's SIE account. Noting the multiple changeovers of people and systems in the intervening period, Colonel McKinstry was unaware of any ability to access former DSOs' emails through his current SIE account. Once this archived mailbox was discovered, CIS was able to retrieve the emails it contained. These have now been processed (again, refined using relevant keywords and time periods). The mailbox does not appear to include an email forwarding a copy of the IAT report such as that Colonel Blackwell referred to in his evidence and there is very little potentially relevant material that has not already been provided. Any potentially relevant material that has not already been provided to the Inquiry is being provided under separate cover.

14. While the accessible emails from the former DSO's account were located as outlined above, it remains the case that there was no formal archiving on SWAN: a deleted account or email is not readily retrievable after 30 days. The NZDF is aware of deficiencies in its IT architecture and there is currently work underway to address this and other issues, some of which was outlined in my letter to you of 4 September 2019.

15. Also as a result of further targeted searches in light of Public hearing 4, the SIO now has access to the content of two relevant ~~PSR~~ accounts (WAATEA.SNO³ and CO.FORWARD). The emails in these accounts have now also been processed (again, refined using relevant keywords and time periods); as with the SIE mailbox referenced at paragraph 13 above, any new potentially relevant material is being provided under separate cover. Again, neither of these two ~~PSR~~ accounts appears to include an email forwarding a copy of the IAT report such as that Colonel Blackwell referred to in his evidence and there is very little potentially relevant new material.

16. For completeness, I would note that there are potential ways for the IAT report to have been received which would not show up in the searches described above. The report may have been carried back to Wellington by a returning SNO (noting that there was a handover in August 2011) or obtained during a visit by the DSO to theatre in 2011 (although a traceable process should have been followed in either case). In terms of it having been received electronically, I recall that, contrary to his evidence under cross-examination that it could only have been from the SNO, Colonel Blackwell's brief of evidence stated that he had received the IAT from the SNO or the NZDF Liaison Officer within ISAF. That Liaison Officer, as well as some NZDF personnel in New Zealand, would have had access to accounts on a partner network, which is not controlled by the NZDF. It may be possible that an email

³ The data from this account appears to be accessible through an anomaly whereby a former SNO has manually copied a .pst backup file of the account to a desktop. This is not standard practice due to the size of such files.

was sent from the Liaison Officer within ISAF to someone in New Zealand who also had access to an account on that network, for on-passing to the DSO.

Colonel (Retired) Blackwell's briefings

17. Your letter notes that Colonel Blackwell said that his practice in briefing the Chief of Defence Force and Ministers was to prepare a dot point brief, which he would speak to and then shred following his meeting, after having saved an electronic version of the briefing in SWAN.⁴ I confirm that the SIO has rechecked all accessible dot point briefs, and the more formal Ministerial briefing documents (that were the subject of an Inquiry letter of 21 August 2019), and not located any brief that relates to Colonel Blackwell having briefed the Minister on the IAT on or around 1 September 2011, or any additional relevant material that has not already been provided. As has been noted previously, it may be the case that a document was created but stored on a desktop rather than an accessible, shared location.

18. Again, for completeness, I note that all of the accessible dot point briefings appear to relate to routine updates. This may suggest that the usual practice for routine briefings to the Minister was departed from in relation to urgent and ad hoc matters. For example, in the period leading to and shortly after 1 September 2011, according to information held by the SIO, the DSO briefed the Minister on 15 June 2011, 9 August 2011 and 12 September 2011. All three of those dot point briefings were provided to the Inquiry at the outset of this process. The dot point briefing of 12 September 2011 indicates that the previous such briefing took place on 9 August 2011, which, as above, corresponds with a dot point briefing held by the SIO and previously provided to the Inquiry; however, Dr Mapp's diary, as produced by the Inquiry at Public hearing 4, lists a DSO briefing on 22 August 2011. Similarly, the dot point brief for 9 August 2011 states that the previous briefing was on 15 June 2011; however, an email from Colonel Blackwell on 29 June 2011 – the day after the hostage rescue incident at the Hotel Intercontinental in which two NZSAS personnel were injured – refers to the DSO briefing the Minister on that date. Another email refers to the DSO having briefed the Ministers of Defence and Foreign Affairs on 27 June 2011. Both of these emails are provided under separate cover. Neither refers to the IAT or appears to have a connection to Operation Burnham, but they do show that the DSO was occasionally briefing the Minister of Defence outside the framework of routine briefings, and no dot point brief for those briefings was found in the DSO SWAN folder where the routine dot point briefings were located.

Concluding remarks

19. The searches of newly located relevant e-mail accounts that produced some 20,000 items and has taken multiple people more than two weeks to examine, has not revealed an e-mail enclosing the IAT report. The SIO is presently confirming whether any new potentially relevant material from other key SWAN accounts is accessible. The quantity of such material is not expected to be large, although the process required to search for it is time consuming. Especially at this late stage, the searches will be targeted on key accounts used at the time of Operation Wātea.

20. Your letter referred to the possibility of engaging a forensic email search capability to try and recover deleted documents. To date, the NZDF has not made use of any external forensic email search capability because it was considered that our in-house capability would be sufficient to locate all

⁴ Noting that, as SWAN is a network, saving something in SWAN could mean in an email account, on a desktop, on a hard drive connected to one computer, or on a shared drive on that network.

accessible, potentially relevant material for provision to the Inquiry. As noted, since the Inquiry began a very large pool of material has been reviewed, and a significant quantity of potentially relevant material (including emails) provided. Noting the significant resource that has been expended over the course of this year on searching for and reviewing emails of potential relevance to the Inquiry, the challenges encountered in that task, and taking into account developments over the Public hearing 4, I would say that email disclosure has been considerably more complicated than anticipated.

21. As always, the NZDF remains committed to assisting the Inquiry and to providing potentially relevant material. Accordingly, the NZDF would be happy to discuss whether there are other steps that might be useful to the Inquiry in connection with this issue, including any targeted search requests the Inquiry might have related to specific roles or individuals.

22. Finally, an option mentioned in the course of Public hearing 4, but which I understand may have been superseded by your letter, was for the NZDF to provide evidence explaining the searches that have been undertaken and the limitations and challenges involved in those searches. If the Inquiry remains of the view that that would assist, the NZDF would be happy to provide an appropriate person.

Yours sincerely



K.R. Short
Air Marshal
Chief of Defence Force