National Security and Intelligence Review Agency

Office de surveillance des activités en matière de sécurité nationale et de renseignement

~~SECRET // CEO~~

REVIEW OF THE CANADIAN FORCES NATIONAL COUNTER-INTELLIGENCE UNIT - OPERATIONAL COLLECTION AND PRIVACY PRACTICES

(NSIRA REVIEW 2021-10)

Contents

EXECUTIVE SUMMARY

1. This review focused on the Canadian Forces National Counter-Intelligence Unit (CFNCIU) and how Information Technology (IT) searches were used to support counter-intelligence (CI) investigations. The review assessed whether IT searches and the collection of information in support of CI investigations interfered with individuals' reasonable expectation of privacy in the circumstance(s).

2. Through the course of the review NSIRA has identified three (3) areas of concern tied to the requests for, and conduct of, CI information technology network searches. These are arranged under the following categories: (1) CFNCIU's search of a Subject's email, Internet and removable device activity; (2) The CFNCIU checklist used to identify and restrict search parameters, and how applicable stakeholders define search parameters; and, (3) How the acquisition of information is used to expand supplementary searches.

3. DND employees and CAF members have a reasonable expectation of privacy when using work computers for personal use. [redacted] **contains information related to DND/CAF operational capabilities** [redacted] NSIRA found that CFNCIU may be inappropriately relying on DND/CAF policies as lawful authority to interfere with a Subject's reasonable expectation of privacy.

4. NSIRA observed that the checklist has the potential to capture intimate and personal information that touches upon a Subject's biographical core. NSIRA found that the checklist risks capturing information that is protected by s. 8 of the *Charter*. NSIRA also found that DND/CAF is applying a definition of metadata that captures information that could be subject to a reasonable expectation of privacy.

5. NSIRA also observed that CFNCIU IT inquiries utilized broad search parameters which may include information not relevant to the investigation. These parameters were applied as broad approvals with no specific internal controls or oversight at both the operational and working levels. Collection techniques, due in part to the limitations of IT audit tools and broad search parameters, resulted in a wide net being cast. NSIRA found that the investigative IT system practices it observed in the context CFNCIU's CI investigations **contains information protected by solicitor-client privilege** [redacted] have insufficient legal oversight to ensure that they are as minimally invasive as possible.

6. As a result of these findings, NSIRA recommends that DND/CAF suspend investigative IT system practices in the context of CFNCIU CI investigations until a reasonable legal authority has been established. Once a reasonable legal authority has been established DND/CAF should create a new policy framework that is reflective of the noted findings.

7. In keeping with NSIRA's *2020 Annual Report*[1] which emphasized the implementation of a "trust but verify" approach for assessing information provided over the course of a review, NSIRA worked with the DND/CAF to design an approach for "proxy access" *i.e.* an

[1] Refer to 2020 Annual Report, section 1.5 "Trust but Verify", p. 13.

approach involving a departmental intermediary an intermediary who accesses information repositories in the presence of NSIRA staff, and who can review relevant information on the system. DND/CAF agreed in principle to this form of access, however, given the disparate number of databases for which CI searches are conducted, this initiative could not be implemented in the course of this review. Notwithstanding, the information provided by DND/CAF has been independently verified by NSIRA through documentation analysis and meetings with DND/CAF subject matter experts. Further work is underway to continue mutually developing an access model for the independent verification of various kinds of information.

AUTHORITIES

8. This review is being conducted under the authority of paragraph 8(1)(b) of the *National Security Intelligence Review Agency Act (NSIRA Act).*

REVIEW BACKGROUND

9. In July 2019, the *NSIRA Act* came into force, establishing the National Security Intelligence Review Agency (NSIRA). NSIRA's mandate allows it to review the full range of national security or intelligence activities across the Government of Canada, including authority to review the Department of National Defence / Canadian Armed Forces (DND/CAF).

10. NSIRA completed its first review of DND/CAF in 2020, focusing on the Canadian Forces National Counter-Intelligence Unit (CFNCIU). During the course of the review, two (2) possible compliance issues were identified, with NSIRA Members approving further review in 2021.

11. The issues identified for further review were:

    - the practice by CFNCIU, Assistant Deputy Minister Information Management [ADM(IM)] and DND/CAF of requesting information from, and searching DND/CAF Information Technology (IT) systems in support of Counter-Intelligence (CI) investigations;[2] and,

    - 2014 CFNCIU Subject interview **contains information related to DND/CAF operations** [redacted].[3]

IT SYSTEM SEARCHES

12. This review assessed, both in legal and technical terms, how IT searches are used to support CI investigations and the accountability structures that guide the acquisition of information and data.

13. Through the course of this review NSIRA examined all available written and electronic records, case files, correspondence, computer databases, and other information holdings

[2] This review will assess a CFNCIU information holdings and DWAN collection activities conducted from January 2017 to September 2019.

[3] [redacted] - Refer to S.06-NSIRA2019-001, Written Submission, Oct. 16, 2020, p. 7.

and documentation related to the operations/investigations selected for review, as well as applicable policies, procedures, and legal advice to verify compliance with legal, ministerial and policy requirements. Presentations, interviews and meetings were conducted with managers/officers, as well as other pertinent DND/CAF personnel.

14. Through examination of selected case files, the review assessed whether IT searches and the collection of information in support of CI investigations interfered with individuals' reasonable expectation of privacy in the circumstance(s). More specifically, NSIRA closely examined whether the searches used to support counter-intelligence (CI) investigations had the potential to include information that is meaningful, intimate and touching on a user's "biographical core" of personal information. Everyone in Canada is constitutionally entitled to expect privacy in personal information of this kind, including when this information is contained on workplace computers.[4]

15. NSIRA selected a sample of CFNCIU's requested IT system searches, to assess whether CFNCIU, in the course of its activities, acted in compliance with the law, ministerial direction, and internal directives, policies and procedures, and had exercised its powers in a manner that is consistent, reasonable and necessary.

16. The review examined a cross-section of CFNCIU case files, and has focused on a contemporary, high level (Level III) case file [redacted] to illustrate CFNCIU and ADM(IM)'s practices when conducting searches on IT systems (Please refer to Appendix 1 for more on this case file). Through the lens of [redacted], NSIRA has examined whether CFNCIU and/or ADM(IM) interfered with individuals' reasonable expectation of privacy in the circumstance(s) through the course of CI investigation. NSIRA closely examined searches conducted by Department of Information Management End-User Services (DIMEUS), Directorate of Information Management Engineering and Integration (DIMEI), and Canadian Forces Network Operations Center (CFNOC).

SUBJECT INTERVIEW

17. NSIRA also conducted an in-depth examination of the 2014 CFNCIU Subject interview in order to understand the lead up to the interview, what happened during the interview, the possible consequences, and what was done by DND/CAF after the incident. NSIRA reviewed CFNCIU's case file and its compliance with relevant legislation, Ministerial Directives, DND/CAF policy, as well as the legal advice provided by the Office of the Judge Advocate General (OJAG) and the Canadian Forces Legal Advisor (CFLA).

18. As a direct result of NSIRA's inquiries, the Canadian Forces Intelligence Command (CFINTCOM) issued a directive on September 9th 2021, [redacted] **contains information related to DND/CAF operations** [redacted][5]

19. In NSIRA's view these measures have addressed the initial concerns exemplified in the 2014 Subject interview referenced above. As a result, NSIRA has suspended further

[4] *R. v. Cole*, 2012 SCC 53, at para 2 [*Cole*].

[5] D.634 - CFINTCOM Directive - [redacted] 9 Sep 2021, p. 1.

inquiry into the matter, however, NSIRA may choose to re-examine this investigative practice in future reviews after an updated functional directive is provided by CFINTCOM.

CFNCIU HISTORICAL CONTEXT

20. Since 1997, Counter-intelligence (CI) and security functions within the DND/CAF have experienced continuous transformation in an effort to find efficiencies and de-conflict with other security, intelligence, and law enforcement stakeholders. Since inception, the CFNCIU has been the subject of ten internal studies, each of which have identified the Unit as having suffered from resource and policy limitations (among others), resulting in an inability to fully meet its mandate.[6] Very few of the recommendations presented in these reports have be implemented. When asked why so many recommendations were ignored the Unit cited resourcing shortfalls.[7]

21. In 1997, the security and criminal investigative services that had resided within the Special Investigations Unit (SIU)[8] were separated into two new and distinct units, the CFNCIU and Canadian Forces National Investigative Service (CFNIS). This was a direct result of the tabling of the *Report of the Special Advisory Group on Military Justice and Military Police Investigation Services*, and the *External Review of the Canadian Forces Special Investigation Unit*.[9]

22. The separation mirrored the bifurcation that occurred in the mid-eighties between the Royal Canadian Mounted Police (RCMP) and CSIS. For the first time, separate and distinct mandates within the DND/CAF were created for law enforcement, security and counter intelligence, and security clearance functions.[10]

23. The newly created CFNCIU assumed the role of the security and counter intelligence functions within the DND/CAF. The CFNIS focused solely on criminal investigations. Finally, the security clearance function was established and now known as the Director General Defence Security, the Director Personal Security and Identification Management (DGDS/DPSIM).

LEGAL AND POLICY AUTHORITIES

24. The formation of the CFNCIU is authorized by the Minister of National Defence (MND) through a Ministerial Organization Order. Subsequently, the Chief of the Defence Staff (CDS), through a Canadian Forces Organization Order, established the CFNCIU as a regular force unit allocated to the Canadian Forces Intelligence Group (CF INT GP).

25. Issued in March of 2003, under the authority of the Deputy Chief of the Defence Staff, the 8002 series *Defence Administrative Orders and Directives* (DAOD) established the main

---

[6] S.03-NSIRA2019-01, D.08 [redacted] July 04, 2014.

[7] S.05-NSIRA2019-01 Written Submission, Aug. 14, 2020, p. 1.

[8] S.02-NSIRA2019-001, D.02 CFNCIU Background, Sept. 26, 2019 and S.03-NSIRA2019-01, D.07 CFNCIU Updated Needs Assessment, Thaler Group Inc., Aug. 12, 2013) p. 67.

[9] S.03-NSIRA2019-01 D.08 [redacted] Jul 4, 2014, p.5.

[10] Ibid.

policy framework for defence CI activities by reaffirming responsibilities of the MND, DM and CDS in safeguarding the resources of DND/CAF. [11] [redacted] **contains information protected by solicitor-client privilege** [redacted] [12] [redacted] would be equivalent to those undertaken by departmental security officers in other federal government departments.

26. There are no provisions of the *National Defence Act* (NDA) that authorize the conduct of defence intelligence activities.[13] CFNCIU investigations are the only area of defence intelligence that is squarely focused on Canadian citizens (DND employees/CAF members). [redacted] **contains information protected by solicitor-client privilege** [redacted] [14] [redacted]

27. In addition, Canadian law imposes legal constraints under the *Privacy Act,* the *Criminal Code* and the *Charter* on intelligence activities conducted in support of domestic operations. For example, the application of the interception of private communications provisions under the *Criminal Code* and the application of section 8 *Charter* protections against unreasonable search and seizure, would apply to domestic activities of DND/CAF.

28. Issued in July of 2012, under the authority of the Assistant Deputy Minister (Information Management) and the Chief Information Officer, the 6002 series *Defence Administrative Orders and Directives* (DAOD) establishes the main policy framework for operational, technical and security authorities for communications and information systems within the DND/CAF.

29. DAOD 6002-2, *Acceptable Use of the Internet, Defence Intranet, Computers and Other Information Technology Systems*, provides users with instructions on official, authorized, unauthorized and prohibited uses of IT systems. It is this policy that defines authorized use and a user's expectation of privacy.[15]

30. In DAOD 6002-2, users are advised that authorized use includes communication with family, friends and other persons, conducting personal banking transactions, as well as shopping for personal and family items, and would fall within the other than official uses category. Users are also advised that that there is only a limited expectation of privacy afforded due to the department's responsibility for monitoring IT systems for the purposes of system administration, maintenance and security, and to ensure compliance with Treasury Board,

---

[11] Ibid, p. 7.

[12] [redacted]

[13] It is important to note that the National Security and Intelligence Committee of Parliamentarians (NSICoP) in their 2018 Annual Report recommended that serious consideration be given to providing explicit legislative authority [a statutory basis] for the conduct of DND/CAF's defence intelligence activities (NSICoP, Annual Report 2018, p. 95 and 98). NSIRA has worked – and will continue to work – with NSICoP to on matters of joint concern to ensure that the broadest range of perspectives are brought to bear and efforts are not duplicative.

[14] [redacted]

[15] D.148 - DAOD 6002-2 Acceptable Use of IT Systems, 07 Oct 2016.

DND/CAF policies, instructions, directives and standards.[16]

INVESTIGATIVE PROCESS

31. Threat related information comes from a variety of sources to CFNCIU. Such information can originate from different detachments as well as from external partners. On initial receipt of threat-related information about a DND/CAF employee and/or incident, the Regional Detachments (RD) drafts an Intelligence Report (IntRep) to Headquarters (HQ), which centrally manages all investigations.[17]

32. Following the initial identification of this security concern, there are two key determinatives to launch an investigation:

    1. there must be a suspicion linking an activity/individual as a threat (i.e. Terrorism, Extremism, Subversion, Sabotage, and Organized Crime) known as a TESSOC;[18] and,

    2. the suspected threat must have a clear "nexus" to DND/CAF information, people and/or assets.[19]

33. When operating within this scope, the nexus must be established for every investigation. **contains information protected by solicitor-client privilege**

    [redacted][20] If the TESSOC and nexus determinations are sufficiently justifiable, the Regional Detachments will submit a request outlining the proposed investigative level.

34. The investigative framework for CFNCIU is unique insofar as it covers security intelligence concerns similar to those of CSIS (i.e. TESSOC, in addition to organized crime), yet is limited in investigative scope to DND/CAF information, people and assets (i.e. nexus). Unlike CSIS, CFNCIU does not collect expansively on threats given the need for a nexus; and unlike a Departmental Security Officer, CFNCIU does not conduct investigations on issues regarding policy compliance, or security issues involving inappropriate behaviour by employees that do not point to an obvious TESSOC.[21] Furthermore, CFNCIU does not have responsibility for security screening (which is the responsibility of DGDS/DPSIM), or

---

[16] D.148 - DAOD 6002-2 Acceptable Use of IT Systems, 07 Oct 2016.

[17] This management role is performed by the senior case manager (SCM) on behalf of the Commanding Officer (S.05-NSIRA2019-01 Written Submission, Aug. 14, 2020, p.5).

[18] S.01-NSIRA-01, Document D.21 CFNCIU Operations Plan FY18-19, May 15, 2018, p. 3.

[19] DAOD 8002-0, Counter-Intelligence sets out the guidance and boundaries of conducting and participating in CI activities. Section 3.3 sets out that a clear DND or CAF nexus must be met: an event or situation involving DND employees or CAF members, DND or CAF property or information, or foreign military members or foreign military property on a defence establishment; or, a request or imminent request from another federal department or civil authority for DND or CAF assistance (*Defence Administrative Orders and Directives,* 8002-0, *Counter-Intelligence*, Context, 3.3).

[20] [redacted]

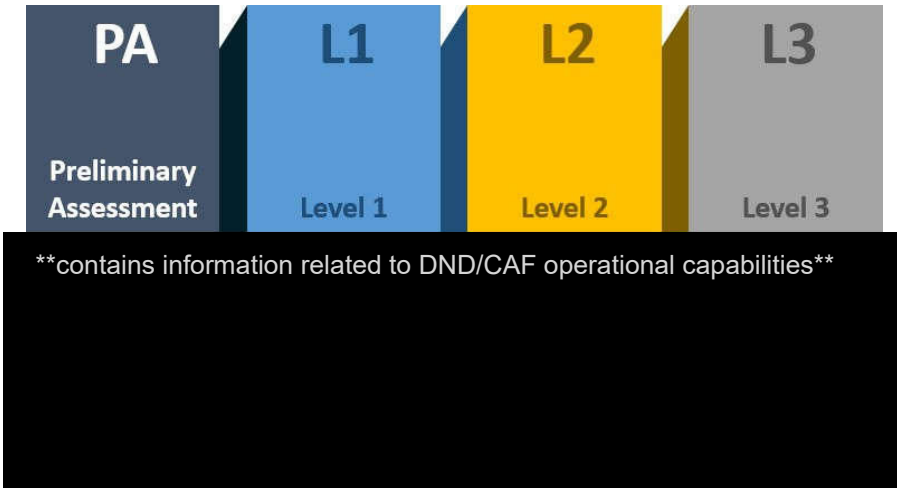
[21] Responsibility for discipline falls to individual commands, who have the authority to launch their own investigations, and based on the findings, determine what disciplinary measures are required.

for criminal investigations, which is the responsibility of the Canadian Forces National Investigation Service (CFNIS).

35. The investigative scope of CFNCIU is therefore best understood as occupying a very narrow space above those related to discipline and security screening, yet falling below criminal thresholds.[22] Prior to the authorization of a counter-intelligence investigation or operation, DND/CAF must determine that:

    1. The investigation complies with the law;
    2. Any investigative techniques are related to the threat posed and the probability of its occurrence;
    3. The need to use intrusive techniques is weighed against any possible breach of constitutionally protected rights and freedoms; and
    4. The least intrusive technique of information collection are used, taking into account the specific circumstance.[23]

36. The following text box summarizes the various investigative levels and what activities are authorized by departmental policy to be performed within that investigative threshold:



37. Although the levels of investigation are temporal, the review observed that most investigations are contained within the lowest investigative thresholds (i.e. PA or L1).[24] This is not due to an absence of serious TESSOC threats but rather, this is due, in part, to CFNCIU's [redacted] legal authorities **contains information related to DND/CAF operational capabilities**[25]

[22] This is not to suggest that CFNICU cannot find, over a course of an investigation, issues that will require discipline and/or of a screening concern; rather, the Unit's investigations are not launched if these issues are not backstopped by a suspected TESSOC threat (S.05-NSIRA2019-01 Written Submission, Aug. 14, 2020, p. 2, 16, 17, 18, 21).

[23] DAOD 8002-1 (National Counter-Intelligence Program), s. 4.3; DAOD 8002-0 (Counter-Intelligence), s. 3.6.

[24] For instance, [redacted] of investigations were PAs, [redacted] were L1, and [redacted] were L3 (S.05-NSIRA2019-01 Written Submission, Aug. 14, 2020, p.21).

[25] In a written submission, the Unit claimed that another reason for the [redacted] investigative levels was to ensure that [redacted] Refer to: DND/CAF "Consolidated Factual Accuracy Input Tracker," December 2, 2020, p.6.

38. When CFNCIU was created in 1997, the legal landscape with regard to the *Charter* was much different than it is today, and technology has expanded in a way that computers have become an all-encompassing tool. In addition, surveillance capacity and techniques have evolved. The law has evolved accordingly to protect *Charter* rights by requiring the State to obtain specific judicial authorizations (warrants) where there is a reasonable expectation of privacy.

39. **contains information protected by solicitor-client privilege**

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. [redacted]
8. [redacted]
9. [redacted][26]

40. **contains information protected by solicitor-client privilege** [redacted][27] Warrantless searches that interfere with a reasonable expectation of privacy are presumptively unreasonable, unless the *Collins* test criteria is satisfied.[28] CFNCIU has not identified a clear lawful authority that would permit warrantless searches for section 8 purposes during CI investigations.

41. It is clear that under this evolved legal landscape that CFNCIU's authorities have not kept up with the articulated mandate. The Unit, and largely CFINTCOM, have acknowledged that policy is outdated in terms of both terminology and content. NSIRA notes, however, that updating internal policies would not provide adequate authorities to conduct activities that would amount to a lawful interference with *Charter* rights. Amendments to allow CFNCIU to conduct most activities that would fall under a Level 2 or Level 3 investigation

[26] D.568 - [redacted]

[27] S.06-NSIRA2019-001, Written Submission, Oct. 16, 2020, p. 2.

[28] A warrantless search or seizure is presumptively unreasonable, and the Crown bears the burden of rebutting this presumption. *R. v. Reeves*, 2018 SCC 56, at para 14 [*Reeves*]. To establish that a search or seizure was reasonable and thus in compliance with section 8 of the *Charter*, on the balance of probabilities the following criteria must be satisfied (1) that search was authorized by law; (2) that the authorizing law was itself reasonable; (3) that the authority to conduct the search was exercised in a reasonable manner. R. v. Collins, [1987] 1 S.C.R. 265 at paras 22-23; *R. v. Nolet,* 2010 SCC 24 at para 21 [*Nolet*].

would require legislative amendments. This was documented within a number of internal reports identifying significant discrepancies in policy.[29]

42. This explains why the Unit relies on the policies and legal authorities of external investigative bodies when carrying out certain functions, including those that would require a warrant.[30] For example, CFNCIU cannot [redacted] these investigative techniques are all facilitated through other investigative bodies and these bodies' mandates (i.e. CFNIS, CSIS, etc.).[32]

43. This contemporary review *NSIRA REVIEW 2021-10* should be viewed as a continuation to NSIRA's 2019 review, *the Canadian Forces Counter-Intelligence Unit (2019-01)*. As a result of the challenges posed by the COVID-19 pandemic and access to DND/CAF's IT/IM infrastructure, NSIRA elected to bifurcate the review. This separation allowed for the provision of findings and recommendations to the Minister of National Defence in February of 2021. While the DND/CAF have accepted all of the findings and recommendations from the 2019 review, NSIRA recognizes this current review follows in relatively short succession and changes may already be underway. The intent of this review is not to restate previous findings and recommendations, but to provide additional observations viewed through an operational context.

44. This review examined a cross-section of CFNCIU case files, and has focused on a contemporary, high level (Level III) case file [redacted] to illustrate CFNCIU and ADM(IM)'s practices when conducting searches on IT systems (Please refer to Appendix 1 for more on this case file).

45. Through the lens of [redacted] NSIRA has examined whether CFNCIU and/or ADM(IM) interfered with an individuals' reasonable expectation of privacy in the circumstance(s) through the course of CI investigation. NSIRA closely examined searches conducted by Department of Information Management End-User Services (DIMEUS), Directorate of Information Management Engineering and Integration (DIMEI), and Canadian Forces Network Operations Center (CFNOC) on behalf of CFNCIU for CI purposes.

46. NSIRA selected a sample of CFNCIU's IT system searches, to assess whether CFNCIU, in the course of its activities, acted in compliance with the law, ministerial direction, and internal directives, policies and procedures, and had exercised its powers in a manner that is

---

[29] Through the course of NSIRA interviews, we were made aware that the DAODs and Standard Operating Procedures are in a perpetual state of re-visioning, with little consideration of, or consultation with RDs (NSIRA interview with CFNICU Halifax, Sept. 24, 2020).

[30] Although capacity to perform functions such as [redacted] do not exist within CFNCIU, they do exist within DND/CAF and other government departments (e.g. CSIS). This capacity has been relied upon in the past. External organizations receiving CFNCIU request for support must prioritize these against their own operational requirements and mandates. No formal agreements with external organizations to provide these services exist, however efforts are ongoing to achieve such agreements. (S.05-NSIRA2019-01 Written Submission, Aug. 14, 2020, p.28).

[31] [redacted]

[32] The common impression received from NSIRA interviews with Regional Detachments, as well as with DGDS/DPSIM and CFNIS, is that CFNCIU may limit investigative levels for reasons of limited investigative capacity and expertise. CFNCIU HQ, however, noted that DGDS/DPSIM and RD personnel "are not privy to all the factors that go into making a decision on the level of investigation." (NISRA interview with DPSIM, Feb. 11, 2020 and NISRA interview with CFNIS Feb. 18, 2020; NSIRA interview with CFNICU Halifax, Sept. 24, 2020; NSIRA interview with CFNCIU Kingston, Sept. 15, 2020; and refer to DND/CAF, "Consolidated Factual Accuracy Input Tracker," December 2, 2020, p.7.)

consistent, reasonable and necessary.

FINDINGS AND RECOMMENDATIONS

47. This review focuses on CFNCIU searches of the Defence Wide Area Network (DWAN). This unclassified network allows for personal use by DND/CAF employees in accordance with internal policy. CFNCIU submits requests to three units which have the capability to query the DWAN activity and provide reports on specific users, and Subjects of investigation(s). The three internal units reviewed included the Department of Information Management End-User Services (DIMEUS), Directorate of Information Management Engineering and Integration (DIMEI), and Canadian Forces Network Operations Center (CFNOC).

48. Through the course of the review NSIRA has identified three (3) areas of concern tied to the requests for, and conduct of, CI information technology network searches. These are arranged under the following categories:

    1. **DWAN searches:** CFNCIU's search [redacted]
    2. **Multi-point Checklist:** The CFNCIU checklist used to identify and restrict search parameters, and how applicable stakeholders define search parameters; and,
    3. **Expanded Search:** How the acquisition of information is used to expand supplementary searches.

DWAN NETWORK SEARCHES

49. CFNCIU requests advanced IT system searches as an investigative tool when conducting CI investigations. This potentially includes searches across [redacted] networks across multiple classification levels (*See Annex F: IT SYSTEMS MATRIX*). In the

context of investigations, searches are best described as mosaics compiled from the previously mentioned distinct internal groups: DIMEI[33] CFNOC[34], and, DIMEUS. [35]

50. When conducting a CI investigation, CFNCIU must engage these groups individually through separate requests. Each group has a separate process for searching, collecting and reporting information. DIMEI, DIMEUS and CFNOC may lawfully access and monitor IT system searches for the purpose of "the management or protection of computer systems," and may take reasonable measures for such purposes, including the interception of private communications. However, DIMEI, DIMEUS and CFNOC's access to DND/CAF IT systems for network security activities does not provide an authority to access those IT systems for the purposes of [redacted]

51. The process for IT system searches, as described by CFNCIU, is illustrated by the figure below:

[33] Department of Information Management Engineering and Integration (DIMEI) is responsible for leading DND/CAF engineering efforts of its IM/IT infrastructure and is subdivided into a number of groups; DIMEI 3 is responsible for Cyber Security Engineering and Architecture, DIMEI 4 Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) - Engineering and Architecture, and DIMEI 5 is tasked with Systems Architecture. These groups assist with DND/CAF IT system searches on both classified and unclassified networks. DIMEI receives tasks directly from CFNCIU and uses commercial-off-the-shelf (COTS) cyber defense tools to conduct its searches. DIMEI primarily uses user identifiers, together with wildcards, to conduct its searches against IT systems sources such as [redacted] and email metadata. DIMEI also utilizes an 20-point checklist, to guide its activities.(CFNCIU Ops Review: IT Processes Presentation to NSIRA, ADM(IM) Support to CFNCIU, Presentation to NSIRA from ADM(IM) September 02, 2021, slides 14-28, and slide 5.)

[34] Canadian Forces Network Operations Center (CFNOC) conducts defensive cyber operations with the DND/CAF cyberspace, and of the three groups, CFNOC clearly has [redacted] when responding to CFNCIU requests. From the initial intake, CFNCIU requests are triaged to ensure that the search parameters are understood and that CFNOC has the ability to fulfil the request. [redacted] it is then sent to Canadian Forces Information Group Head Quarters Judge Advocate General (CFIOG HQ JAG) for legal review. A legal opinion is provided, where it will be later captured in the tasking order. It is only when CFIOG HQ JAG has provided a [redacted] (CFNCIU Ops Review: IT Processes Presentation to NSIRA, ADM(IM) Support to CFNCIU, Presentation to NSIRA from ADM(IM) September 02, 2021, slides 30-34.)

[35] Department of Information Management End-User Services (DIMEUS) is the service management center for the National Capitol Region and is responsible for IM/IT, server and Infrastructure support, as well as account and IT asset management. DIMEUS receives tasks directly from CFNCIU, where an Information System Security Officer translates the task and assigns an analyst. DIMEUS has advised NSIRA that support is limited to email metadata. Email metadata is a set of email attributes that includes the sender, recipient(s), date, time, subject line and any attachment names. Metadata however, does not include email content. [redacted] CFNCIU Ops Review: IT Processes Presentation to NSIRA, ADM(IM) Support to CFNCIU, Presentation to NSIRA from ADM(IM) September 02, 2021, slides 36-45.)

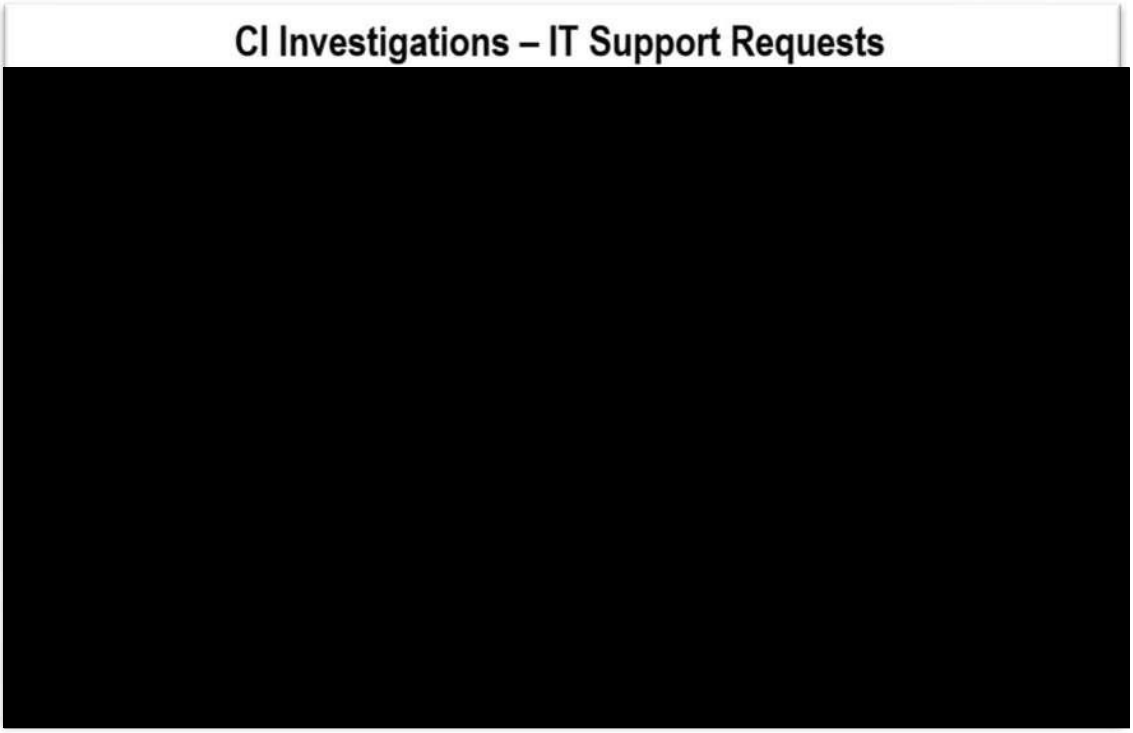


Figure 2: CI Investigations – IT Support Requests[36]

52. Generally DIMEI, DIMEUS and CFNOC utilize similar processes for providing "remits" – i.e. the collected product – to CFNCIU across IT systems.[37] At the collection and filtering stage it is the IT analyst (DIMEI, DIMEUS, CFNOC) that decides what information is included as part of the remit. Analysts retrieve data from the Subject's repositories based on a set of predefined selectors which is stipulated in a multi-point checklist (discussed further below) and relevance to the request is ultimately determined by the analyst's post-collection review. [redacted]

[redacted][38]

53. While CFNOC engages its legal counsel with the initiation of CFNCIU's request, they do not appear to be engaged with, or consulted through the course of the investigation [redacted]

[36] CFNCIU Ops Review: IT Processes Presentation to NSIRA, ADM(IM) Support to CFNCIU, Presentation to NSIRA from ADM(IM) September 02, 2021, slides 30-34.

[37] Departmental policy, security orders and user acknowledgements are similar in how they relate to regular monitoring of IT systems for the purposes of system administration, maintenance and security.

[38] D.563- [redacted].

[redacted] DIMEUS and DIMEI do not have assigned legal review, or oversight, and rely on the checklist to support their collection and filtering activities. DND/CAF notes that legal advice is sought by CFNOC and may be requested by DIMEUS and DIMEI, including verbally, [redacted][39] However, NSIRA cannot verify this claim.

A Reasonable Expectation of Privacy when using IT Systems

54. Importantly, CFNCIU IT searches may not interfere with an individual's *Charter* rights. As noted above, this review examined whether searches of the unclassified DWAN network for CI purposes had the potential to infringe upon an individual's reasonable expectation of privacy in the informational content[40] included on workplace computers. Case law recognizes that an individual's use of workplace computers for personal purposes may give rise to a reasonable, though diminished expectation of privacy, protected by s. 8 of the *Charter*.[41] A reasonable expectation of privacy inquiry is fact-sensitive and fact-specific, and depends on the "totality of the circumstances".[42]

55. It is likely that users of DND/CAF unclassified[43] IT systems have a reasonable expectation of privacy when using such systems for personal use. DND/CAF policy on acceptable use of computer systems and devices permits limited personal use of such systems for a range of personal activities that are not necessary to carry out duties and official functions in furtherance of DND and CAF goals and objectives. This can include communicating with family, friends and other persons, for other than official use; shopping for personal and family items; or accessing news and other electronic network information sources.[44] Such authorized activities (i.e, those for personal purposes) can generate revealing and meaningful private information that falls within the "biographical core" of information protected by section 8 of the *Charter*.[45] A Subject under investigation by CFNCIU, therefore, would be able to establish a direct interest and a subjective expectation of privacy in any information content searched related to the personal use of DND/CAF networks.

56. DND Employees and CAF members have a reasonable expectation of privacy when using work computers for personal use. DND/CAF policy recognizes that:

---

[39] [redacted]

[40] Informational privacy has been defined as "The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communications to others." *R. v. Tessling*, 2004 SCC 67, at para 23, [*Tessling*], quoting A. F. Westin, Privacy and Freedom (1970) at p. 7.

[41] *Cole* at para 9. Section 8 of the *Charter* protects individuals against unreasonable search and seizure. Only where state examinations intrude upon the reasonable privacy interest of individuals does the government action in question constitute a search within the meaning of s. 8. *Tessling* at 18; *Evans* at para 11.

[42] A reasonable expectation of privacy is determined by four lines of inquiry: "(1) an examination of the subject matter of the alleged search; (2) a determination as to whether the claimant had a direct interest in the subject matter; (3) an inquiry as to whether the claimant had a subjective expectation of privacy in the subject matter; and (4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances". *Tessling* at para 32; *Cole* at para 40.

[43] There may be differing expectations of privacy when using a classified versus an unclassified IT system, as a reasonable expectation of privacy may be extremely limited when using classified systems. NSIRA focused this review on CFNCIU's searches of unclassified IT systems.

[44] DAOD 6002-2, Acceptable Use of the Internet, Defense Intranet, Computers and Other Information Technology Systems, section 4.3

[45] *Cole* at paras 46 – 49.

> *"[t]here is only a limited expectation of privacy when using IT systems because they are subject to monitoring for the purposes of system administration, maintenance and security, and to ensure compliance with the Treasury Board, DND and CAF policies, instructions, directives and standards."*[46]

57. A limited, or diminished, expectation of privacy is nonetheless a reasonable expectation of privacy protected by section 8 of the *Charter*.[47] [redacted] **contains information protected by solicitor-client privilege** [redacted][48]

58. NSIRA acknowledges that DND/CAF has a legitimate interest in safeguarding the resources of DND and the CAF. However, the "finer points" of an employer's right to monitor computers issued to employees has been left by the Supreme Court for another day.[49] While the law on *employee* computer searches continues to evolve, a reasonable expectation of privacy is subject to state intrusion only under the authority of a reasonable law.[50]

59. A search carried out without a warrant is presumptively unreasonable and contrary to s. 8 of the *Charter*.[51] In the absence of a warrant, the Crown must establish on a balance of probabilities (1) that the search was authorized by law; (2) that the authorizing law was itself reasonable; and (3) that the authority to conduct the search was exercised in a reasonable manner.[52] NSIRA is concerned that CFNCIU has not adequately considered their legal authorities to determine whether they have reasonable lawful authority to conduct warrantless searches for CI purposes.

60. As CFNCIU [redacted] **contains information protected by solicitor-client privilege** [redacted][53] and therefore CI activities would not constitute an unreasonable search within the meaning of s. 8 of the *Charter*.

61. [redacted] **contains information protected by solicitor-client privilege** [redacted]

---

[46] DAOD 6002-2, Acceptable Use of the Internet, Defense Intranet, Computers and Other Information Technology Systems, section 3.8.

[47] *Cole* at paras 8-9, 58. "While workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the expectation entirely: The nature of the information at stake exposes the likes, interests, thoughts, activities, ideas and searches for information of the individual user." *Cole* at para 3.

[48] D. 118 [redacted]

[49] *Cole* at para 60.

[50] *Cole* at para 9.

[51] *R. v. Nolet,* 2010 SCC 24, at para 21; *Reeves* at para 14

[52] *R. v. Collins,* [1987] 1 S.C.R. 265 at paras 22-23; *Nolet* at para 21.

[53] D. 113 – [redacted] page 2.

[54]

[55]

62. **contains information protected by solicitor-client privilege**

[56]

[57]

63. CFNCIU for CI activities, and is not clearly authorized by law to intrude upon a Subject's reasonable expectation of privacy. NSIRA notes that the objective of the Treasury Board Policy is to manage government security, which is distinct from intelligence-gathering. Further, NSIRA emphasizes that internal policies– even those that "reflect and instantiate broader Treasury Board Policy on Government Security" – are likely not adequate authorities to conduct CI activities that allow for an interference with *Charter* rights.[58] [59] **contains information protected by solicitor-client privilege**

[60] While the CFNCIU search is not for criminal purposes, the strict requirement

---

[54] See D.124 - Charter Considerations, . D.126 - D.569 –

[55] D.569 –

[56]

[57] Ibid.

[58]

[59] D.569 –

[60]

to report wrongdoing to the authorities would likely raise the standards for protections under section 8 of the *Charter.*

64. **contains information protected by solicitor-client privilege**
[61]

Searches

65. In , the Counter-Intelligence Oversight Committee (CIOC) authorized a Level III CI investigation codenamed **contains information related to national security investigations**
[62]
[63]

66. **contains information related to DND/CAF operations**
[64]
[65]

[61]

[62] D.126 - p. 3.

[63] D.124 - Charter Considerations, p. 1-2. Note that

[64] D.124 - Charter Considerations, D.126 - D.569 – As noted by DND/CAF - Consolidated Factual Accuracy Input Tracker – Nov. 26, 2021, page 14, these three opinions referenced in relation to in should be considered together, as they were provided to CFNCIU contemporaneously and dealt with the same subject-matter. CFNCIU also claims that verbal advice was provided in the relation to this investigation (DND/CAF - Consolidated Factual Accuracy Input Tracker – Nov. 26, 2021, page 17 and 21), however NSIRA cannot verify this claim.

[65] D.569 – page 6.

[redacted][66]

67. **contains information protected by solicitor-client privilege**

[redacted][67]

[redacted][68]

[redacted][69]

[redacted][70]

68. **contains information protected by solicitor-client privilege**

[redacted]

---

[66] Ibid.

[67] D.126 - [redacted]

[68] [redacted]

[69] D.126 - [redacted].

[70] [redacted] at paras 61-62.

[redacted][71][redacted][72][redacted]

[redacted][73]

69. **contains information protected by solicitor-client privilege** [redacted][74]

[redacted][75]

70. **Finding 1: NSIRA found that CFNCIU is inappropriately relying on DND/CAF policies as lawful authority to interfere with a Subject's reasonable expectation of privacy.**

---

[71] [redacted]

[72] Note that [redacted]

[73] *Cole* at para 2.

[74] [redacted]

[75] R v. Spencer, 2014 SCC 43 [redacted] page 3

MULTI-POINT CHECKLIST

71. The multi-point checklist[76] is applied as a standard operating procedure that sets out the parameters used to capture CFNCIU IT search requests, by aligning technical search capabilities with DND/CAF's existing cyber defence tools.[77]

72. The checklist identifies IT inquiry questions to be answered in retroactive analysis reports on Subjects of investigation.[78] The multi-point checklist is viewed as a list of pre-consulted IT support requests and associated search criteria that has been reviewed [redacted] The checklist serves as a basis for all CFNCIU requests to DIMEI and DIMEUS by aligning the specific information request to the allowable search criteria, all the while falling within CFNCIU's mandate and legal authorities. CFNCIU has indicated [redacted]

73. [redacted]**contains information protected by solicitor-client privilege**[redacted][79][redacted][80]

74. [redacted] DIMEUS and DIMEI do not have imbedded legal counsel, and rely on legal counsel from Directorate of Law/ Intelligence and Information Operations (DLAW/I&IO), or legal counsel from headquarters within ADM(IM) through CFNCIU.[81]

75. CFNCIU distinguishes metadata from content as "…the attributes of the content without revealing the content."[82] Their view is that because the metadata does not include

---

[76] NSIRA notes that the checklist is referred by DND/CAF as the 18-point checklist. When asked how the checklist was used to guide IT support requests, NSIRA was advised that the list actually contained 20 items. [redacted]

[77] D.633 - September 24, 2021, Written Responses, p. 2. D.619 - CFNCIU RFIs, [redacted] p. 1. D.164 - IT Inquiry Process, [redacted] p. 10-19.D.552 - [redacted] p. 1-6.

[78] D.633 - [redacted] .D.552 - [redacted]

[79] [redacted]

[80] [redacted]

[81] D.633 - September 24, 2021, Written Responses, p. 2. Note that DLAW/I&IO is an internal directorate of the Operational and International Law division (DJGA Ops) of the OJAG.

[82] D.633 - September 24, 2021, Written Responses, p. 6. [redacted] at page 6.

content, it is claimed by CFNCIU to be less sensitive.[83] Metadata, [redacted] is returned to CFNCIU as a list of all emails sent or received by the Subject, including all the email metadata attributes such as the sender, the recipient, as well as the subject line[84] and any attachment names.

76. NSIRA notes that metadata can be just as revealing as content about a Subject's biographical core, depending on the context. Information that might appear outside of the biographical core of a Subject may be revealing or intrusive when coupled with other information.[85] When viewing the information compiled by the checklist in its entirety, it is possible that intimate personal information related to the Subject under investigation may be revealed beyond what was initially contemplated or authorized. Additionally, email subject lines are akin to content rather than metadata. An email subject line can reveal the content of the communication that it describes, and it can be just as sensitive as any communication contained within an email. Therefore, it is inaccurate to consider email subject lines as metadata, rather than content.

77. It is important to note that DIMEUS analysts, during the filtering process, assesses relevance based on the Subject's email metadata, [redacted][86] DIMEI has a similar process where returns are filtered to include only metadata related to the Subject. DIMEUS and DIMEI, as mentioned above, do not have integrated legal support.[87] NSIRA notes that the practice of DIMEUS and DIMEI analysts filtering information for relevance – and in some cases, to ensure the results do not include content – is an inappropriate method for conducting IT searches, as it is likely to intrude upon the Subject's privacy interests (further discussed below).

78. The proposed checklist selectors are applied to all DIMEI and DIMEUS search requests by means of a standardized template. These selectors are used as filters that are applied to each search. Data returns only include the selector, or an iteration of that selector.[88] Noteworthy, is the practice of DIMEI, which if a date range is not specified by CFNCIU, all records irrespective of time period are provided. In practice, there is in fact no constraint on

---

[83] Ibid.

[84] Regarding email subject lines as metadata, DND/CAF writes that; "Based on industry standard IT Security definitions, subject lines are metadata (information about information). This does not change the fact that they may need to be handled differently during CI investigations; however it also does not invalidate the standing definition of metadata." DND/CAF - Consolidated Factual Accuracy Input Tracker – Nov. 26, 2021. In support of the standing definition of metadata, DND/CAF has provided to NSIRA an infographic from the Office of the Privacy Commissioner (OPC), dated October 2014. Importantly, the OPC infographic provided notes: "In many cases, courts have recognized that metadata can reveal much about an individual and deserves privacy protection, while recognizing that context matters."

[85] For example, in *R. v. Spencer, 2014 SCC 43,* at para 47, the accused's IP address, coupled with Internet activity associated with the IP address, in combination with the name and address of the IP address user, was revealing of the accused's biographical core.

[86] CFNCIU Ops Review: IT Processes Presentation to NSIRA, ADM(IM) Support to CFNCIU, Presentation to NSIRA from ADM(IM) September 02, 2021, slides 30-34. However, in the email exchange with CFNICU, DIMEUS clearly indicates that they [redacted] D.130 - Email0949-RE NCIU [redacted] DIMEUS, [redacted]

[87] D.633 - September 24, 2021, Written Responses, p. 3-6.

[88] Selectors are always searched as wildcards.

the metadata being provided to CFNCIU in this scenario.[89] This appears to contradict two checklist items which limit the information requests to the inquiry period.

79. **contains information protected by solicitor-client privilege**

[redacted][90]

80. Ultimately, current CFNCIU IT policy [redacted] on IT searches [redacted] **contains information protected by solicitor-client privilege** [redacted].[91] Further, IT searches based on use of the checklist are not subject to additional legal consultation or oversight (beyond the creation of the checklist template) [redacted][92] This is problematic as the checklist items as drafted may capture information that has the potential to reveal intimate details of the lifestyle and personal choices of the Subject, which would be protected by section 8 of the *Charter*.

81. For example, item 8 of the checklist is [redacted] **contains information protected by solicitor-client privilege** [redacted][93] Such an approach may still reveal information for which a Subject has a reasonable expectation of privacy.[94] [redacted] **contains information protected by solicitor-client privilege** [redacted]

82. It is important to note that CFNCIU, during the course of the [redacted] investigation, submitted a request to CFNOC that included [redacted] **contains information related to DND/CAF operations** [redacted] CFNOC reminded CFNCIU that a reasonable expectation of privacy existed and 'fishing expeditions were prohibited.'[95] This resulted in the withdrawal of the request for [redacted] with CFNOC. By contrast, CFNCIU requested similar information

---

[89] D.633 - September 24, 2021, Written Responses, p. 2.

[90] D.115 - [redacted]

[91] D.164 - IT Inquiry Process, 10 Sep 2019.

[92] D.633 - September 24, 2021, Written Responses, p. 2.

[93] D.115 - [redacted]

[94] The Supreme Court has recognized that an individual's use of the Internet gives rise to a privacy interest: "In my view, the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address, and telephone number." *R. v. Spencer,* 2014 SCC 43, at para. 47.

[95] D.176 - [redacted]

from DIMEI who complied and provided [redacted][96] Although these two requests were not issued concurrently, they clearly demonstrate two separate outcomes based on very similar CI requests.

83. In contrast to DIMEUS and DIMEI's approach, CFNOC operates under their own policies, directions and standard operating procedures, and need to meet specific requirements before a CFNCIU request can be initiated. For example, unlike DIMEI and DIMEUS, the CFNOC process includes an initial legal review by their CFIOG JAG [redacted]

84. [redacted] **contains information protected by solicitor-client privilege** [redacted][97] [redacted][98] [redacted][99] NSIRA notes that the CFNOC approach to receiving initial legal review by their CFIOG JAG in the context of an investigation is preferable to DIMEUS and DIMEI's approach [redacted]

85. Given the risk that the checklist items and proposed selectors have the potential to capture intimate and personal information that touches upon a Subject's biographical core, the use of the checklist outside of the initially agreed upon parameters and without additional legal guidance or approval is problematic.

86. ***Finding no. 2: NSIRA found that the DND/CAF checklist applied as a standard investigative operating procedure risks capturing information that is protected by s. 8 of the Charter.***

87. ***Finding no. 3: NSIRA found that DND/CAF is applying a definition of metadata that captures information that could be subject to a reasonable expectation of privacy.***

EXPANDING THE SEARCH

88. CFNCIU has taken measures to constrain its search parameters over the course of the [redacted]. Initial Requests For Information (RFI) (before the multi-point checklist was constituted) included far-reaching and extensive search parameters. From 2014, to the introduction of the checklist RFI items included [redacted] **contains information related to DND/CAF operations** [redacted] was included as part of the RFI. The [redacted]

[96] D.478 - [redacted]
[97] D.645 - [redacted]
[98] [redacted]
[99] D.645 - [redacted]

[redacted][100]

89. In [redacted] a month prior to the authorization of the [redacted] investigation, CFNCIU investigators discussed the contents of the associated RFI and highlighted their preference to **contains information related to DND/CAF operations** [redacted]

[redacted][101]

90. DND/CAF has made attempts to constrain the search parameters with the implementation of the multi-point checklist. However, even with the checklist, the CFNCIU IT inquiry requests for the [redacted] investigation utilized broad search parameters which may have included information not relevant to the investigation.

91. **contains information protected by solicitor-client privilege** [redacted][102]

92. Filtering the data for relevancy after this initial collection and search has occurred poses legal risks, as any potential interference into the Subject's reasonable expectation of privacy would have already occurred by state action. The post-filtration of the information by the IT analyst before it is returned to CFNCIU does not negate that this initial search and seizure of the information by the IT analyst already constitutes a 'search' and 'seizure' within the meaning of s. 8 of the *Charter*, if this search interfered with a reasonable privacy interest.[103]

93. These parameters are applied as broad approvals with no specific internal controls or oversight at both the operational and working levels. [104] Collection techniques, due in part to the [redacted] result in a wide net

---

[100] D.118 - [redacted]

[101] D.117 - Email0856-Re [redacted] as requested [redacted] And, D.118 - [redacted]

[102] D.567 - [redacted] (Duplicate), pages 2, 9. And, D.124 - [redacted] Charter Considerations, [redacted] page 3. D.126 - [redacted] pages 10, 12-13.

[103] An inspection is a search and a taking is a seizure where a person has a reasonable privacy interest in the object or subject matter of the state action and the information which it gives access. *Cole* at para 34.

[104] DND/CAF notes that CFNOC is required to seek legal advice when it is assessed that a CFNCIU request to expand or adjust the search parameters falls outside of the scope of the original request, and that CFNOC consultation with their legal counsel is also conducted verbally (DND/CAF - Consolidated Factual Accuracy Input Tracker – Nov. 26, 2021, page 20) However, NSIRA could not verify this claim.

being cast. It is left to the analyst/investigator to determine what is relevant and filter results after the information/data has been collected.

94. NSIRA has observed six instances of expanded search criteria, either outside of the stipulated checklist criteria or outside the initial request to CFNOC, as illustrated in *Appendix II: Expanding the Search:* [redacted] *– Specific Examples,* with no additional legal consultation, yet with clear risk of intruding upon *Charter* interests. As previously mentioned, the use of broad search parameters and then subsequent filtration of 'relevant' information is not an appropriate investigative technique. Furthermore, this approach does not align with DND/CAF policy on the CI program to ensure that prior to investigation or operation, the need to use intrusive techniques is weighed against a possible breach of constitutionally protected rights; and the least intrusive technique of information collected is used, taking into account the specific circumstances.[105]

95. ***Finding 4: NSIRA found that CFNCIU risks breaching protected privacy interests by not having clear policy guidance based on lawful authority for IT searches, and by expanding IT searches beyond the approved search parameters.***

96. ***Finding 5: NSIRA found that the investigative IT system practices it observed in the context CFNCIU's CI investigations contradict the Office of the JAG and the Department of Justice's legal advice,*** [redacted]**contains information protected by solicitor-client privilege**[redacted]

Recommendation 1: NSIRA recommends that DND/CAF suspend investigative IT system practices in the context of CFNCIU CI investigations until a reasonable legal authority has been established.

Recommendation 2: Once a reasonable legal authority has been established DND/CAF should create a new policy framework that is reflective of the noted findings, namely, the multi-point checklist, the categorization of metadata, the expansion of IT searches and the principle that these searches be as minimally invasive as possible.

[105] DAOD 8002-1, section 4.5

APPENDIX I: [redacted]

97. On [redacted] **contains information related to national security investigations** [redacted]

98. [redacted] **contains information related to national security investigations** [redacted][106] [redacted][107].

99. In [redacted] the CIOC authorized a Level III CI investigation codenamed [redacted] **contains information related to DND/CAF operations** [redacted][108]

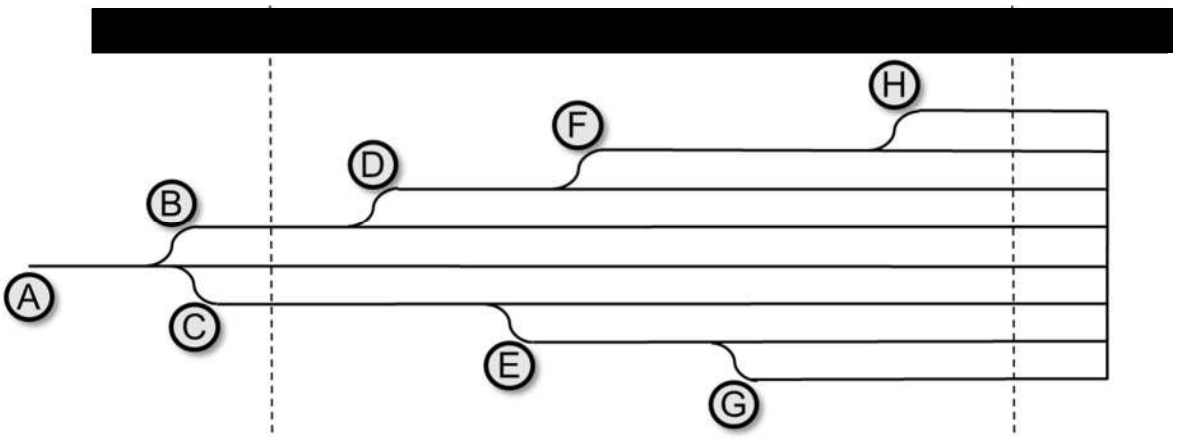
100. DND/CAF, through its coordination body National Security and Intelligence Review and Oversight Coordination Secretariat (NSIROCS), has provided a large amount of documents in response to our Requests for Information. It is however also important to note that the information provided has not been independently verified by NSIRA.

---

[106] D.124 - [redacted] Charter Considerations, [redacted] p. 1-2. Note that [redacted]

[107] D.119 - [redacted] v02_SCM_Reviewed, [redacted] slides 24-28.

[108] D.126 - [redacted] p. 3.



	A	**contains information related to DND/CAF operations**
	B	
	C	
	D	
	E	
	F	
	G	
	H	

APPENDIX II: [redacted] - SPECIFIC EXAMPLES

[redacted]

101. **contains information protected by solicitor-client privilege** [redacted][109] [redacted][110]

102. DIMEI 3-5 provided [redacted] in [redacted] DIMEI 3-5 further elaborated with the release of the information that the report was generated from [redacted] **contains information related to DND/CAF operations** [redacted][111]

[redacted]

103. Between [redacted] CFNOC provided CFNCIU with information in response to the IT inquiry request. This included [redacted] **contains information related to DND/CAF operations** [redacted]

104. On [redacted] CFNCIU requested from CFNOC "a master spreadsheet of all emails with subject headings to date."[112] This request did not include the initially agreed upon search criteria. CFNOC agreed to this change and provided an additional report

---

[109] D.176 - [redacted].

[110] [redacted]

[111] D.478 - [redacted]

[112] D.274 - [redacted]_Email0852 FW [redacted]

containing [redacted] This change also affected all subsequent [redacted] reports generated by CFNOC and provided to CFNCIU on a periodic basis.

105. In [redacted] CFNCIU requested from CFNOC [redacted][113] They also requested [redacted] **contains information related to DND/CAF operations** [redacted][114] [redacted][115]

106. In [redacted] DIMEI 3-5 provided a report to CFNCIU containing [redacted] The search criteria used was more than the [redacted] previously identified by CFNCIU. DIMEI 3-5 also state that: "If there is an [redacted] **contains information related to DND/CAF operations** [redacted][116]

[redacted] *ACTIVITY*

107. In [redacted] CFNCIU requested CFNOC with a search of [redacted] CFNOC performed the search and provided the results, which included [redacted][117]. This additional request appears to have expanded the search criteria for all subsequent [redacted] activity reports. The new search criteria now included activity from any user where the device matched one previously used by the Subject of investigation[118].

[redacted]

108. In [redacted] CFNCIU requested from DIMEI 3-5 Security Information and Event Management (SIEM) data from **contains information related to DND/CAF operations** [redacted][119]. SIEM data includes [redacted] DIMEI 3-5 later confirmed that [redacted][120]

109. On [redacted] CFNCIU requested from DIMEUS IT inquiries for [redacted] **contains information related to DND/CAF operations** [redacted]

---

[113] D.348 - [redacted]_Email1248 RE [redacted] UPDATE - [redacted]

[114] They requested the [redacted] Initially, CFNOC provided [redacted] D.349 - [redacted]_Email1253 RE [redacted] Update, [redacted]

[115] This opened up an internally discussion between CFNCIU, CFNOC, DIMEI 3-5 and DIMEUS about the availability of [redacted] The three support functions all stated they did not have [redacted] They stated that [redacted] (D.405 - [redacted]_1835 [redacted] RFI). It is also the impetuous to the expansion of the [redacted] D.353 - [redacted]_Email1428 FW [redacted]

[116] D.448 - [redacted]1339 [redacted] Report [redacted]

[117] D.364 - [redacted]_Email1345 FW Questions [redacted]

[118] D.367 - [redacted]_Email0731 FW [redacted] Update, [redacted]

[119] D.409 - [redacted]_0920 RE [redacted] CFNCIU - Requested Info, [redacted]

[120] D.424 - [redacted]_0737 RE [redacted] NCIU, [redacted]

as well as any [redacted][121]. A few days later, DIMEUS shared with CFNCIU that they "are seeing [redacted][122]

110. In [redacted] DIMEI 3-5 internally discuss a pending CFNCIU request for "identify [redacted][123]. They further indicate that this is possible by [redacted] At this point, it is unclear why the scope of the investigation includes more than the [redacted]. In a subsequent correspondence, DIMEI 3-5 defined the exact search criteria used to response to the 20 "IT Inquiry"[124] questions. It included the [redacted][125] identified by CFNCIU has having been [redacted]

111. In [redacted] CFNCIU provided a list of [redacted] to CFNOC. The list of **contains information related to DND/CAF operations** [redacted][126]. The list was provided alongside a request to CFNOC [redacted]

112. In [redacted] CFNCIU requested from DIMEUS a search of [redacted] **contains information related to DND/CAF operations** [redacted] One month later, DIMEUS replied with a report containing [redacted][127]. Of the [redacted]

113. DIMEI 3-5 continued to generate reports containing [redacted] **contains information related to DND/CAF operations** [redacted] The search criteria for both reports was observed to be [redacted]

[121] D.130 - [redacted]RE NCIU [redacted]DIMEUS, [redacted]
[122] D.130 - [redacted]RE NCIU [redacted]DIMEUS, [redacted]
[123] D.409 - [redacted]_0920 RE [NCIU [redacted] CFNCIU - Requested Info, [redacted]
[124] D.422 - [redacted]_1205 [redacted] Query, [redacted]
[125] D.423 - [redacted]_0722 RE File Transfer SOP, [redacted]
[126] D.376 - [redacted]_Email1218 RE [redacted]
[127] D.137 - Email1029-EFW NCIU [redacted]

ANNEX A: FINDINGS AND RECOMMENDATION

Finding 1: NSIRA found that CFNCIU is inappropriately relying on DND/CAF policies as lawful authority to interfere with a Subject's reasonable expectation of privacy.

Finding 2: NSIRA found that the DND/CAF checklist applied as a standard investigative operating procedure risks capturing information that is protected by s. 8 of the Charter.

Finding 3: NSIRA found that DND/CAF is applying a definition of metadata that captures information that could be subject to a reasonable expectation of privacy.

Finding 4: NSIRA found that CFNCIU risks breaching protected privacy interests by not having clear policy guidance based on lawful authority for IT searches, and by expanding IT searches beyond the approved search parameters.

Finding 5: NSIRA found that the investigative IT system practices it observed in the context CFNCIU's CI investigations contradict the Office of the JAG and the Department of Justice's legal advice, [redacted]

Recommendation 1: NSIRA recommends that DND/CAF suspend investigative IT system practices in the context of CFNCIU CI investigations until a reasonable legal authority has been established.

Recommendation 2: Once a reasonable legal authority has been established DND/CAF should create a new policy framework that is reflective of the noted findings, namely, the multi-point checklist, the categorization of metadata, the expansion of IT searches and the principle that these searches be as minimally invasive as possible.

ANNEX B: LIST OF ACRONYMS

ADM(IM)	Assistant Deputy Minister Information Management
CDS	Chief of the Defence Staff
CF INT GP	Canadian Forces Intelligence Group
CFINTCOM	Canadian Forces Intelligence Command
CFIOG	Canadian Forces Information Operations Group
CFIOG JAG	Canadian Forces Information Operations Group Judge Advocate General
DND/CF Legal Advisor	Office of the Department of National Defence and Canadian Forces Legal Advisor
CFNCIU	Canadian Forces National Counter-Intelligence Unit
CFNIS	Canadian Forces National Investigation Service
CFNOC	Canadian Forces Network Operations Center
CI	Counter-intelligence
CIOC	Counter-Intelligence Oversight Committee
DAOD	*Defence Administrative Orders and Directives*
DGDS/ DPSIM	Director General Defence Security, the Director Personal Security and Identification Management
DIMEI	Directorate of Information Management Engineering and Integration
DIMEUS	Department of Information Management End-User Services

DLAW/I&IO	Directorate of Law/ Intelligence and Information Operations
HRLS	Human Rights Law Section
IntRep	Intelligence Report
OJAG	The Office of the Judge Advocate General
LEGAD	Office of the National defence and Canadian Forces Legal Advisor
MND	Minister of National Defence
NDA	*National Defence Act*
TESSOC	Terrorism, Extremism, Subversion, Sabotage, and Organized Crime

ANNEX C: CFINTCOM DIRECTIVE[128]

SECRET//CANADIAN EYES ONLY

Canadian Forces Intelligence Command
National Defence Headquarters
101 Colonel By Drive
Ottawa, ON K1A 0K2

Commandement du renseignement des Forces canadiennes
Quartier général de la Défence nationale,
101 promenade Colonel By
Ottawa, ON K1A 0K2

2014-0 (J2X)

9 September 2021

Distribution List

[redacted]

M.C. Wright
Major-General
Commander

1/2

SECRET//CANADIAN EYES ONLY

[128] D.635 - CFINTCOM Directive - [redacted] 9 Sep 2021

SECRET//CANADIAN EYES ONLY

Action

[redacted]

2/2

SECRET//CANADIAN EYES ONLY

ANNEX D: 20-POINT CHECKLIST[129]

The checklist is defined as:

1. [redacted]
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.

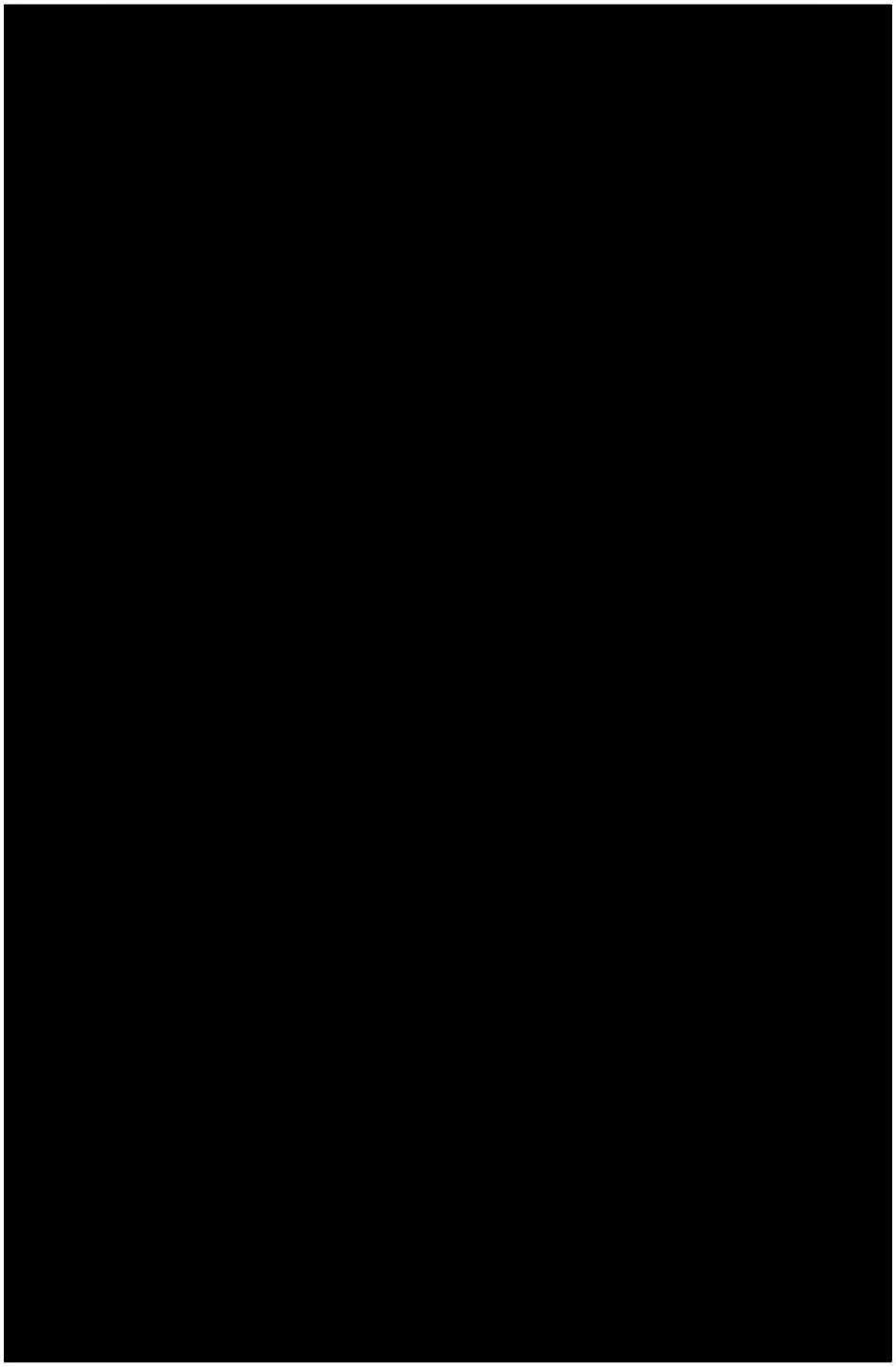
[129] D.164 - IT Inquiry Process, 10 Sep 2019.

ANNEX E: [redacted][130]

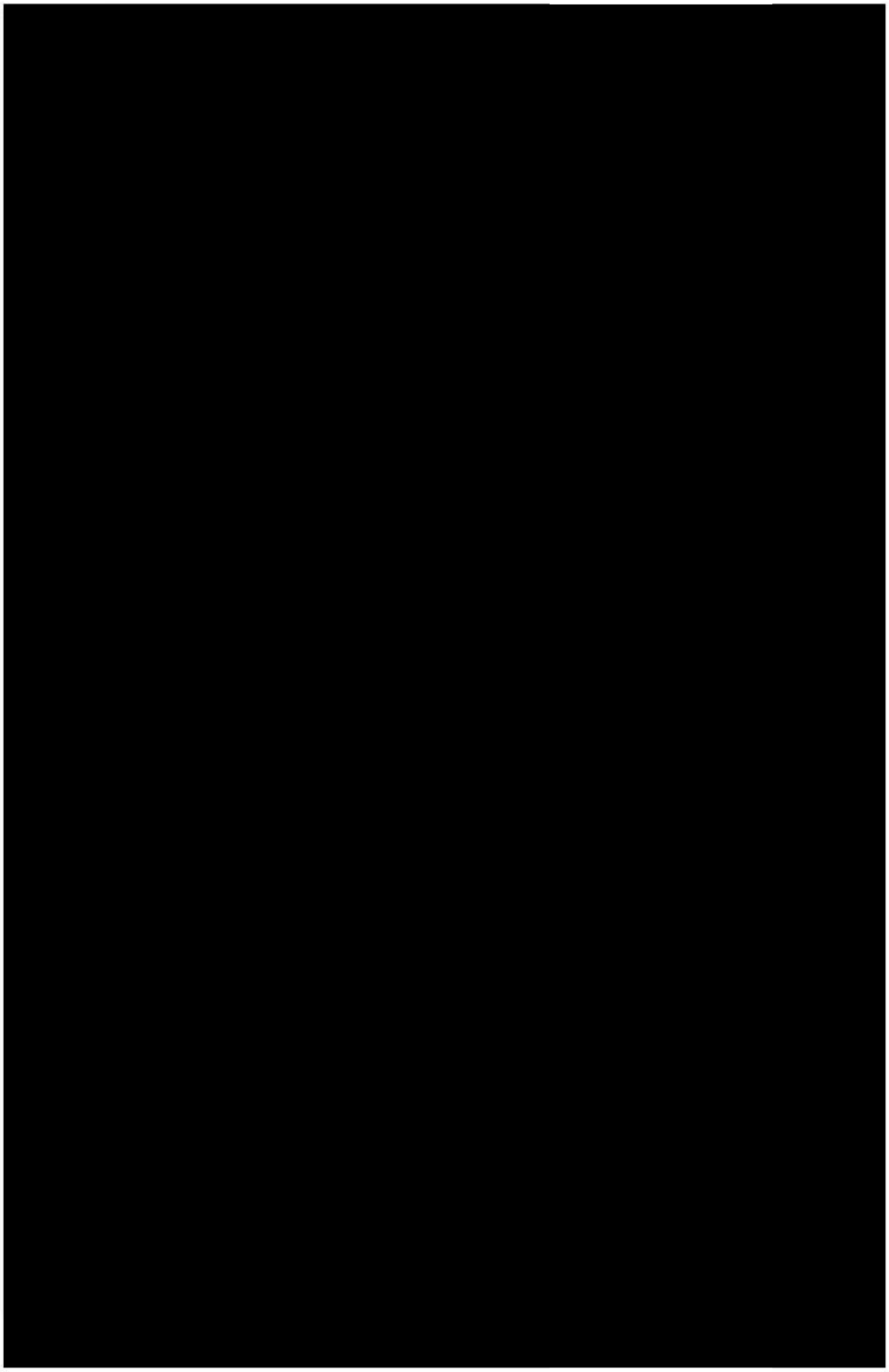
[130] D.115 - [redacted]

[redacted]

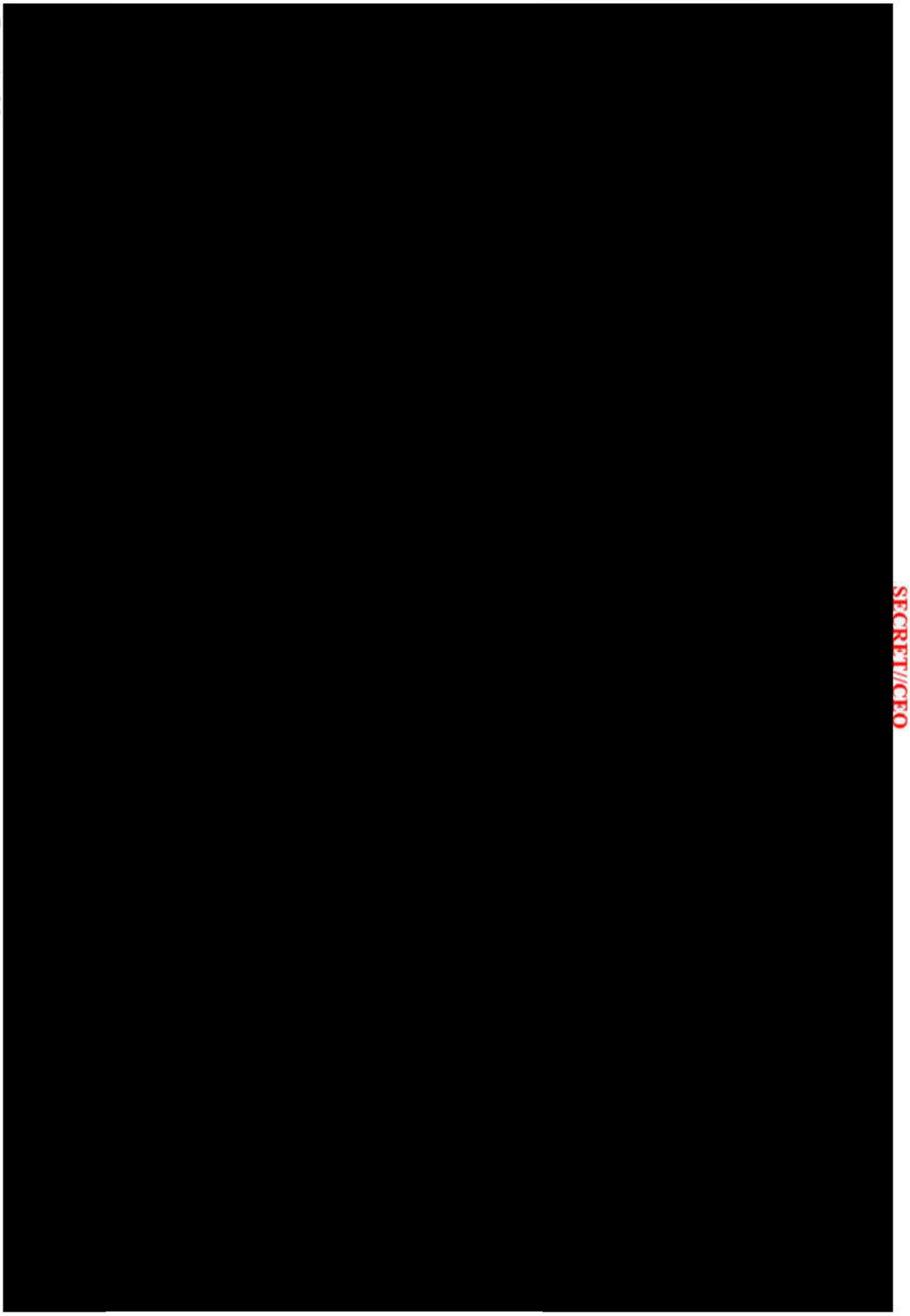
SECRET//CEO



SECRET//CEO



SECRET//CEO



SECRET//CEO

SECRET//CEO

SECRET//CEO

SECRET//CEO

SECRET//CEO

ANNEX F: IT SYSTEMS MATRIX

The table below highlights the networks within the DND/CAF IM/IT infrastructure as well as the areas of responsibility for each group described above.

	DIMEI	***CFNOC***	***DIMEUS***
[redacted]			
[redacted]	X	-	-
	X	-	-
	X	-	-
	X	-	-
	X	-	-
	X	-	-
	X	-	-
	X	-	-
[redacted]			
[redacted]	X	X	-
	X	X	-
	X	X	-
	X	X	-
	X	X	-
	X	X	-
[redacted]			
[redacted]	X	X	X(NCR)
	X	X	-