



Headquarters
New Zealand Defence Force
Defence House
Private Bag 39997
Wellington Mail Centre
Lower Hutt 5045
New Zealand

OIA-2025-5621

26th March 2026

[REDACTED]@nzme.co.nz

Dear [REDACTED]

Further to the email to you of 9 February 2026, this response provides a redacted copy of the Operations Lifecycle Enhancement Programme Closure Report, and addresses the outstanding parts of your request.

The current NZDF policy, order, directive, or guidance governing retention, access, or repatriation of NZDF-generated information held on partner networks;

When New Zealand Defence Force (NZDF) personnel create or maintain information on systems owned by partners, it is subject to international agreements. These agreements are specific to the activities being undertaken, are based on the need to exchange information, and do not necessarily confer right of access to the information. The NZDF will undertake best efforts to transfer information to its own systems, however may not always be able to do so. NZDF Legal Services will carry out assessments and develop national policy caveats specific to the activity to ensure that New Zealand law is followed. The caveats are withheld pursuant to section 6(a) of the Official Information Act 1982 (OIA).

The most recent document that records any plan, decision, or action taken to index, catalogue, or digitise the East Timor era operational files or other unindexed historical operational material (particularly the material recovered from the former Defence House and stored on pallets in a warehouse);

No decision has yet been made to index, catalogue, or digitise the hardcopy files containing records of operations in East Timor. Similarly, no documented plans or actions relating to this part of your request exist, and it is therefore declined in accordance with section 18(e) of the OIA.

The document(s) that record the loss of email-search capability since May 2024, including any incident report, briefings, or update to senior leaders;

The document(s) that record the hybrid email system security-scan failure and any resulting uncertainty about the location of archived email;

The most recent document that records NZDF's expected timeline or plan for restoring full email-search capability;

The document that is most relevant to these parts of your request is a 30 June 2025 Dot-Point Brief, and two of its enclosures, that are provided at enclosure 2. Enclosures 1 and 4 of the Dot-Point Brief are withheld in full in accordance with section 6(a) of the OIA as they are descriptions of secure digital systems used by deployed personnel. Where indicated, information describing vulnerabilities or operational systems is withheld in accordance with

section 6(a) of the OIA; personal information is withheld in accordance with section 9(2)(a); information that would prejudice the NZDF's ability to carry on negotiations is withheld in accordance with section 9(2)(j); and, signatures are withheld in accordance with section 9(2)(k) to avoid the malicious or inappropriate use of staff information, such as phishing, scams or unsolicited advertising.

Any NZDF-held document - including drafts, internal emails, advice, or updates - relating to NZDF's response to the Chief Ombudsman's 2024 Operation Burnham case note, including preparation of a six-month progress update or any decision not to provide one.

An email response was provided by the NZDF in response to the Ombudsman's request for a progress update. While technically not considered official information by definition of the OIA, the following excerpt is from that correspondence with the office of the Ombudsman is provided for your information:

In respect of the applicable recommendation of the Expert Review Group, improving information management continues to be a priority for the NZDF. The Information Management Programme (IMP) Programme Business Case was approved by Cabinet in July 2023 and since then has continued to follow the appropriate process of developing a Detailed Business Case in order to return to Cabinet for funding. The Tranche 1 Detailed Business Case received Cabinet approval in December 2024 and the NZDF is now engaged with Treasury over the required budget uplift for Budget 2025.

You have the right, under section 28(3) of the OIA, to ask an Ombudsman to review this response to your request. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that responses to official information requests are proactively released where possible. This response to your request will be published shortly on the NZDF website, with your personal information removed.

Yours sincerely

GA Motley

Brigadier

Chief of Staff HQNZDF

Enclosures:

1. Operations Lifecycle Enhancement Programme closure report
2. Dot-Point Brief



OPERATIONS LIFECYCLE ENHANCEMENT PROGRAMME (OLEP) Closure Report

Approval of the Closure Report indicates an understanding of the purpose and content described in this deliverable. By signing this deliverable, each individual agrees that the information is accurate and complete.

Approved by:

Position	Name	Signature	Date
CDF	AM Tony Davies		25 JUN 25
SECDEF	Dr Brook Barrington		25 June 25

Independent Review by:

Position	Name	Signature	Date
Inspector-General (Defence)	Brendan Horsley	E-mail response received.	18 June 25

Endorsed by:

Position	Name	Signature	Date
OLEP Steering Committee Co-Chair (NZDF)	RADM Mathew Williams	Steering Committee Review Meeting.	12 June 25
OLEP Steering Committee Co-Chair (MoD)	Richard Schmidt	Steering Committee Review Meeting.	12 June 25

Consulted with:

Position	Name	Signature	Date
COMJFNZ	MAJGEN Rob Krushka	No comments.	N/A
Acting DEPSEC SMA (MoD)	Paul Arts	E-mail response received.	06 June 25
HIB (MoD)	Kathleen Pearce	E-mail response received.	08 June 25
Acting AC SCE	GPCAPT Rob Shearer	E-mail response received.	06 June 25
CoS HQNZDF	BRIG Grant Motley	No comments.	N/A

COMINFO	BRIG Esther Harrop	No comments.	N/A
CDSM	CDRE Brendon Oakley, RNZN	In person response received.	04 June 25
SOCC	COL Christopher Gray	No comments.	N/A
Director EPMO	Steve Cook	E-mail response received.	03 June 25

Submitted by:

Position	Name	Signature	Date
OLEP Co-Lead (NZDF)	GPCAPT s.9(2)(g)(i)	s.9(2)(k)	25 JUN 25
OLEP Co-Lead (MoD)	s.9(2)(a)	s.9(2)(a)	26 JUN 25

Version History

Version	Date	Initiated by	Description
V 0.1	03 June 2025	WGCDR s.9(2)(g)(i)	Draft Report
V 0.2	09 June 2025	WGCDR s.9(2)(g)(i)	Draft post completion of consultation
V 1.0	18 June 2025	WGCDR s.9(2)(g)(i)	Final version for signature

References

Ref	Document Name	Date of Issue	Version
A	Report of the Government Inquiry into Operation Burnham and related matters	July 2020	1.0
B	Report of the Expert Review Group into Operation Burnham	August 2021	1.0
C	Cabinet Paper and Minute [ERS-21-MIN-003]: Report of the Expert Review Group established in response to the Operation Burnham Inquiry	November 2021	1.0
D	ERG Implementation Programme Steering Committee Terms of Reference	April 2022	1.0
E	Operations Lifecycle Enhancement Programme: ERG Report Implementation – Blueprint on a Page	August 2022	1.0
F	NZDF – MoD Defence Policy Advisor (POLAD) Programme Memorandum of Arrangement	May 2024	1.0
G	NZDF – MoD Defence Operations Lifecycle Framework Memorandum of Arrangement	March 2025	1.0

CONTENTS

CLOSURE REPORT PURPOSE	1
BACKGROUND	1
The Government Inquiry into Operation Burnham and Related Matters	1
The Expert Review Group	2
REVIEW OF PROJECT OBJECTIVES AND MEASURES	3
OLEP Overview and Process	3
Desired Outcomes and Benefits	5
Time – Scope and Schedule	5
Budget/Cost	6
Personnel Resources	7
Risk	7
Observations and Lessons Identified	8
PROJECT CLOSE OUT	9
Project Artefacts	9
Follow-on Work for Functional Areas/Line Managers	9
Assurance Plan for Assessing System Health	10
CONCLUSION	10
RECOMMENDATION	11

CLOSURE REPORT PURPOSE

1. The Closure Report is the final document produced by the Operations Lifecycle Enhancement Programme (OLEP). It is intended to be used by the OLEP Steering Committee to confirm successful implementation of the Expert Review Group (ERG) recommendations across Defence agencies (NZDF and MoD) and recommend to CDF and SECDEF that the programme is formally closed. The key objectives of this report are to:
 - a. provide assurance that the intent of the ERG recommendations has been delivered;
 - b. verify user acceptance of the programme's products and outcomes;
 - c. review programme performance against baselines; and
 - d. close or establish the ongoing management of any risks.

BACKGROUND

The Government Inquiry into Operation Burnham and Related Matters

2. In 2018 the Attorney General established the Government Inquiry into Operation Burnham and Related Matters (the Inquiry), with the main focus being the August 2010 Operation Burnham in Afghanistan. The central matter of public importance the Inquiry was directed to examine was *"the allegations of wrongdoing by NZDF forces in connection with Operation Burnham and related matters."*¹
3. The Inquiry was an exhaustive and complex process supported by a range of internationally and domestically based forensic, legal, and intelligence experts. In summary, the Inquiry found *"the principal allegations in Hit & Run about the conduct of TF81² on Operations Burnham and Nova are not accurate"* and *"the operations were not conducted in the way alleged in Hit & Run."*³
4. However, the Inquiry report was critical of the NZDF's handling of the allegations of civilian casualties that were made following Operation Burnham. The Inquiry found *"NZDF's continued repetition of incorrect statements, both publicly and to ministers, resulted from the combined impact of frequent changes in key staff, failures to keep proper records and provide written briefings, and inadequate information storage and retrieval processes."*⁴
5. The Chief of Defence Force, in responding after the release of the Inquiry report in 2020 (ref A), publicly acknowledged and apologised for organisational and administrative failings that saw incorrect information provided to Ministers and the New Zealand public.

¹ In 2017 a book called Hit & Run was published that made a number of serious allegations against the New Zealand Defence Force about an operation conducted in August 2010 in Afghanistan. Operation Burnham was an operation by the New Zealand Special Air Service (NZSAS) and other nations' forces targeting insurgents in the Tirgiran Valley of Baghlan province. The book alleged that the NZSAS carried out war crimes, and that the NZDF mounted a cover-up of civilian casualties.

² TF81 (Task Force 81) comprised NZSAS personnel.

³ Report of the Government Inquiry into Operation Burnham and Related Matters, Chap 1, p.22.

⁴ Ibid p. 30.

6. The Inquiry further considered a detention operation (Operation Yamaha) in which the NZSAS partnered with Afghan forces to detain an insurgent. The Inquiry found that the transfer and transportation of the captured insurgent in Kabul was improper, and there were insufficient measures in place to protect the captured insurgent against the risk of torture or mistreatment in detention with Afghan authorities. The Inquiry found that New Zealand breached its duty of *non-refoulement* and related obligations to prevent torture in relation to the captured insurgent. This finding led to an Inquiry recommendation around the revision of detention policies and procedures.
7. The Inquiry concluded in July 2020 and made four recommendations:
 - a. Promulgation of a Defence Force Order setting out how allegations of civilian casualties should be dealt with – Action NZDF. Completed 2021. (*DFO 35 New Zealand Defence Force Response to Civilian Harm*).
 - b. The development and promulgation of effective detention policies and procedures – Action MFAT. Completed 2022 (*New Zealand Policy Framework for the humane treatment of detainees in offshore deployments*).
 - c. Establishment of an office of the independent Inspector-General of Defence – Action MoD/MoJ. (*CDF Directive 35-2024 authorises NZDF support to the new office of the IGD. An interim IGD was appointed and commenced in role January 2025*).
 - d. Appointment of an Expert Review Group and conduct of a review – Action NZDF/MoD. Completed 2021.

The Expert Review Group

8. The Inquiry recommended that the Minister of Defence establish an ERG to consider whether NZDF's "*organisational structure and record keeping and retrieval processes*" were in accordance with international best practice to avoid failures identified by the Inquiry re-occurring. The subsequent ERG Terms of Reference (ref B, appendix A) included a broader scope of matters the Minister considered important, including "*organisational, systemic and cultural issues*" and "*whether the NZDF is fit for purpose to meet the strategic challenges it is facing and will face in coming years.*"
9. ERG members were selected on the basis that they had wide ranging experience from the public service, defence, and security sectors, and were able to provide independent advice to the Minister. Appointed by Cabinet, members of the ERG included:
 - a. Lyn Provost CNZM (Chair). Former Deputy Police Commissioner and Auditor General.
 - b. Simon Murdoch CNZM. Former DPMC and MFAT Chief Executive
 - c. Tony Lynch. Former Deputy Chief Executive, Security & Intelligence, DPMC.
 - d. Richard Foy. Former NZ Chief Archivist, Department of Internal Affairs.
 - e. Carol Douglass. Deputy Secretary, Government, People & Executive Services, MoD

- f. Brigadier Hugh McAslan. NZDF. Former Commander 1 (NZ) Brigade and former Chief Defence Intelligence.
 - g. Air Marshal Philip Osborn (international military adviser). Retired Royal Air Force, former Chief of Defence Intelligence UK).
 - h. Dennis Richardson (international civilian adviser). Australian former Secretary of Defence.
10. The ERG reported publicly in November 2021 (ref B) and made nine recommendations (detailed at Annex A) across four dimensions:
- a. Strengthen integration between the NZDF and the MoD throughout the deployment lifecycle and at all levels of both organisations;
 - b. Review the suitability of particular elements of Headquarters NZDF for the future;
 - c. Integrate the NZSAS into the wider NZDF and national security sector, including through leadership development; and
 - d. Improve the NZDF's information management systems and practices and the flow of defence knowledge to the Minister of Defence.
11. Following initial high-level assessment by NZDF and MoD officials of the approach to implementation of the ERG recommendations, the Minister of Defence advised Cabinet that all recommendations would require changes across Defence and take time to embed (ref C). Additionally, the Minister highlighted that some key changes could be delivered through programmes already underway or ready to commence, for example an Information Management Business Case that was ready for Cabinet to consider at the end of 2021. The Minister also noted that some recommendations would require new work, for example developing new integrated strategic and military policy functions to support complex operations.
12. The Minister briefed Cabinet that they had accepted all the ERG Report recommendations, and on the indicative plan to implement the recommendations across an approximately three-year period (2022 – 2024) including a mid-point progress report from Defence to the Minister by June 2023.

REVIEW OF PROJECT OBJECTIVES AND MEASURES

OLEP Overview and Process

13. In early 2022, a jointly led NZDF-MoD (Defence) programme team⁵ was established to ensure recommendation implementation was fully integrated across the Defence agencies. This acknowledged and was consistent with the ERG advice that the recommendations were mutually reinforcing.
14. A Defence joint Steering Committee of five members was established to govern the implementation programme IAW ref D. VCDF and Deputy Secretary Policy & Planning

⁵ The programme was initially called the 'ERG Implementation Programme', then renamed 'Operations Lifecycle Enhancement Programme' (OLEP) in 2023 to reflect the forward-looking focus on actions to build and mainstream good practice.

- (DEPSEC PP) were appointed as Co-Chairs (responsible for steering implementation on behalf of the Chief Executives), supported by an additional tier-two representative from each agency, and one external participant from the Public Service Commission as committee members.
15. A programme blueprint (ref E) was created that set out the desired future state for Defence to deliver:
 - a. Improved collaboration between NZDF operational personnel and MoD policy staff;
 - b. Increased provision of timely and transparent information to decision makers; and
 - c. Improved decision-making regarding NZDF operations.
 16. These benefits would contribute to the vision: *“for the New Zealand Government, the national security sector, Defence leaders and the New Zealand public to have high levels of trust and confidence in the information provided to them”*; and *“Defence will retain a strong licence to operate because there is appropriate democratic oversight of the military and transparency of military activities is both appropriate and trustworthy.”*
 17. The approach to implementation of the ERG recommendations was an integrated framework across systems, people, and information assurance, recognising the interdependence of changes required to deliver blueprint benefits. It was intended to take place in three phases:
 - a. Phase 1: Building the frameworks and mechanisms to achieve the vision.
 - b. Phase 2: Establishing the systems and information flows to ensure the frameworks and mechanisms work seamlessly together to realise the vision, and
 - c. Phase 3: Testing the new frameworks, mechanisms and systems. The focal point for this phase was intended to be the NZDF-led Joint Readiness Exercise (JRE) in September 2024.
 18. All ERG recommendations have been substantially implemented and completed. Initiatives are now either embedded into existing processes and assessed as now mainstream ‘Business as Usual,’ or have achieved a maturation point where they are assessed as fully meeting the ERG intent. This aligns with the intended approach for Phases 1 and 2 above.
 19. Of note, the OLEP established two Memorandum of Arrangement (MoA) mechanisms between NZDF and MoD to support: (1) operationalisation of the Policy Advisor (POLAD) capability at ref F, and (2) implementation & application of the Defence Operations Lifecycle Framework (OLF) at ref G. Both these mechanisms highlight the benefits of enhanced integrated working practices between the agencies, and in the latter MoA, acknowledge the joint stewardship of the Defence OLF by VCDF and DEPSEC PP as part of their substantive roles.
 20. Phase 3 approach required reconsideration when it became apparent the JRE could not proceed under its planned format (single exercise activity in 2024) due to

organisational constraints. It would instead be replaced by a series of exercise activities (KIWI COMMAND 25 (KC25)), conducted during 2025. Noting continued uncertainty in the eventual execution of the KC25 series, in August 2024 the OLEP Steering Committee agreed to a conditions-based approach to specific aspects of testing the frameworks, mechanisms and systems to satisfy intent of ERG Recommendation 9.

21. A table detailing the ERG recommendations, the outcomes that have been achieved and evidence to support this assessment is attached at Annex B.

Desired Outcomes and Benefits

22. The vision and intervention approach was initially set in 2022 via the Blueprint on a Page (ref E) developed with the OLEP Steering Committee. An Intervention Logic Map (Annex C) further illustrates the pathway to benefit realisation by linking the flow from Problem Definition > Output Delivered > Outcome Desired > Benefit Realised.
23. The desired outcomes identified by the OLEP as central to on-going successful integrated working practices of the Defence agencies are:
 - a. cohesive management and policy integration;
 - b. clarity in roles, responsibilities and accountabilities;
 - c. organisational culture and behaviour generates consistent collaboration, trust and transparency;
 - d. understanding of operations lifecycle requirements, and
 - e. adherence to processes and protocols.
24. Through a process of observation and evaluation over time, the programme team assess the desired outcomes have been achieved and, through a structured process of continuous improvement and on-going scheduled assessment, will support enduring Benefit Realisation.

Time – Scope and Schedule

25. As previously mentioned, Cabinet was advised (at ref C) that it would take several years to implement and successfully embed all ERG recommendations across Defence, and this timeframe was indicated as Calendar Year (CY) 2022 – 2024. Once the OLEP Team was established in early 2022 and able to consider the scope and scale of work required, indicative planning timelines confirmed substantive completion of work was forecast by the end of 2024, with final administrative work and programme close-out occurring in early 2025. The Information Management Programme was highlighted as a dependency throughout, influenced by but outside control of core OLEP delivery.
26. The OLEP Schedule of Work occurred along the following lines:
 - a. CY2022-2023 – Implementation Phase 1. Key initiatives included:

1. Detailed design work on the Defence OLF.
 2. Establishment of the Defence Operations Consultation Committee.
 3. Establishment and formalisation of the Defence Policy Advisor (POLAD) programme.
- b. CY2023-2024 – Implementation Phase 2. Key initiatives included:
1. Trial, evaluation and embedding of the Defence OLF.
 2. Completion and Publication of the New Zealand Special Operations Forces (NZSOF) Operating Concept document.
 3. Review and changes to the structure and processes of the Office of CDF.
- c. CY2024-2025 – Implementation Phase 3. Key initiatives included:
1. Completion of all Defence OLF supporting resources.
 2. End-to-end evaluation and assessment of the Defence OLF process, using a recently completed NZDF operation.
 3. Independent assessment of OLF IM interim solution sufficiency by MoD (Defence Assessment Team (DAT)).
- d. 2025 – Final administrative work and Programme Close Out.

Budget/Cost

27. When Cabinet received the ERG Report it noted that while Defence would initially fund activities from baseline (in Financial Year (FY) 2022/23), additional funding would likely be needed for implementation of some recommendations to steady state, and this would be sought at future Budgets.
28. As the implementation of OLEP initiatives progressed, it was identified that any additional funding needed by the OLEP team, for example obtaining external contracted support, would need to be secured through re-assigned baseline. This subsequently occurred through re-prioritisation of savings at the NZDF Responsibility Centre level and from within MoD. Approximate total additional operating expenditure was \$568,176 (NZDF) and \$20,460 (MoD). Personnel expenditure was similarly absorbed in baseline staffing of both Defence agencies.
29. Any potential for significant, additional out-year funding in Defence portfolios/functional areas affected by OLEP initiatives (other than that already identified and scheduled by Defence agencies) was mitigated and modest uplifts were absorbed in baseline. s.9(2)(f)(iv)

Personnel Resources

30. Initially formed with just two co-leads, the OLEP team has largely maintained a core footprint of up to four people since late 2022, including three NZDF personnel (one programme Co-Lead and up to two Staff Officers) and one MoD member (programme Co-Lead). Further enabling support was provided by functional managers in both agencies, as required. A coordinator was contracted by NZDF for six months in 2022, and a civilian Programme Manager was employed (0.5 FTE assigned to OLEP) for approximately 12 months during CY2023/2024.

Risk

31. Throughout the period of the programme, the OLEP Steering Committee maintained a consistent view that all efforts must be made to mitigate a reoccurrence of the events identified in the Inquiry, in particular those relating to incorrect statements (information) provided to Ministers and the New Zealand public. At the end of the programme, the questions the OLEP Steering Committee sought assurance on are:
- a. Critical information – *can we find it?*
 - b. Provision of advice to Ministers – *is it accurate?* and
 - c. When agencies are under pressure – *will the system(s) work? and will people follow the process?*
32. The recommendation outcomes generated or assisted by the OLEP team (Annex B) are evidence that Defence agencies are now operating in a more integrated manner than when the Inquiry was being conducted. Improved systems and processes for information identification, capture, storage and retrieval are central to this enhanced way of working, supported by clearly articulated and proven user guides/procedures and information technology business rules. Additionally, the establishment of processes that support analysis and oversight during an operation help to ensure that accurate and timely information is provided to Ministers and the New Zealand public (e.g. responding to Official Information Act requests) and provide a mechanism to both build trust and ensure that people are following process. **s.6(a)**

33. **s.9(2)(g)(i)**

34. **s.9(2)(g)(i)**

s.9(2)(g)(i)

35. The IM Programme therefore remains a key dependency for OLEP as Defence will not be able to achieve full benefits realisation until the IM Programme is fully implemented. The recent assessment of the OLF IM Interim Solution provides examples of residual risk in both future system migration and external sharing functionality. The latest update from the IM Programme team indicates Tranche One will occur across four years (FY25/26-FY28/29) to address the current deficiencies in how NZDF manages data as a strategic asset. The objectives of the ERG Report relating to IM are cross-referenced in the IM Programme business cases, which provides confidence the intent has been embedded and will satisfy the IM Principles in Ref B. The IM Programme was also included in the Defence Capability Plan recently announced by Cabinet. This reinforces the importance of the IM Programme as an investment to improve NZDF's ability to store, retrieve and share information with our national partners and other government agencies. However, whilst approved by Cabinet, the IM Programme will be subject to bids as part of the Budget 25 process (and beyond) alongside other projects and initiatives.
36. One other risk lies in sustainment of the HQJFNZ POLAD position (refer paragraph 29). This has been a trial role to date and only made possible through the reassignment of existing staff funding. The HQJFNZ POLAD role has proven to be highly effective in supporting COMJFNZ and HQJFNZ planning staff, and there is consensus between NZDF and MoD on the value of maintaining the role, as evidenced by the establishment of a MoA (ref F). s.9(2)(f)(iv)

Observations and Lessons Identified

37. Over the period the OLEP was in operation, key lessons and observations were captured for future reference, in the event Defence embarks on another programme of similar scope and scale. Refer to Table 1.

Observation or Lesson Identified	Advantage (A) or Disadvantage (D)
Joint governance structure (OLEP Steering Committee) proved effective.	(A) Ensured Defence agencies perspectives were forthcoming and agreed upon. (A) Senior leadership invested in outcomes and ensuring respective agency 'buy in' to on-going success.
Integrated programme team worked collaboratively to co-design all implementation initiatives.	(A) Ensured a high level of continuous engagement between agencies. (A) Smoothed the way for change management processes to successfully roll out.
User/Practitioner resistance to process change was low. Pockets of concern were mitigated by the	(A) Increased successful implementation of initiatives (e.g. Defence OLF).

forward-looking 'better' vision for integrated working practices and information sharing.	(A) Easier to educate people on the benefits accrued from more integrated working practices.
Use of external consultants during detailed design phases.	(A) Access to commercial 'best practice' perspectives and subsequent results, where resources are not available within Defence. (A) Experienced facilitation of workshop sessions and/or time-constrained activities. (D) Financial cost (high) and products/services availability subject to competing priorities i.e. other clients' requirements. (D) Pace was still constrained by internal staff availability.
Employing an agile approach to rollout of initiatives.	(A) A 'learn by doing' rather than regimented or overly formalised methodology to process induction resulted in more effective user uptake. (A) Users/Practitioners brought along on the 'journey' and refined practice in new areas through experience.

Table 1. OLEP Observations and Lesson Identified

PROJECT CLOSE OUT

Project Artefacts

38. To support effective delivery of the Defence OLF, both for NZDF personnel and MoD staff directly involved in execution of the framework, and awareness for all other Defence employees, a resource site was established on the NZDF Intranet Launch Page. The site contains links to key documents that provide both an overview of the Defence OLF and detailed process diagrams to support practitioners. For context, a copy of The Report of the Expert Review Group (ref B) is also accessible via the site.
39. Following project closure, all OLEP working documents currently stored in the Defence Document Management System will be archived IAW extant policy.

Follow-on Work for Functional Areas/Line Managers

40. Aside from directed tasks that are specified in formal orders or instructions (e.g. CDF Directive), the OLEP identified several key capability areas and/or areas of focus that will require attention by functional leads and line managers to ensure sustained good practice, delivery and benefits realisation. These capabilities/areas are identified as:
 - a. The Defence OLF. Continuing to build capacity in the NZDF and MoD and understanding of the Defence OLF process, in order to ensure effective, on-going, strategic-level application of the framework throughout the full lifecycle of an operation. Responsibility – Assistant Chief Strategic Commitments and Engagements (AC SCE), Head international Branch (HIB), Director Strategy Management Office, MoD, and Director DAT, MoD.
 - b. The DOCC. To maintain the value derived from an effective, senior reference group function where issues can be raised and considered by cross-agency senior

leadership, commitment to holding and supporting the DOCC needs to be acknowledged & prioritised. *Responsibility* – HIB and AC SCE.

- c. The Defence POLAD capability. Noted as delivering significant benefit to Defence, the OLEP Steering Committee acknowledged that sustainment of the POLAD capability will require continued investment and proactive management to ensure a pipeline of suitably experienced POLADs. *Responsibility* – HIB, as specified in the Defence POLAD Memorandum of Arrangement (ref F).
- d. NZSOF capability. Increased transparency of NZSOF roles and activities now occurs amongst agencies of the National Security System. Emphasis will be on NZSOF to ensure this is maintained through a process of engagement and continuous improvement. Assistance to measure success in this area could be provided by the MoD Strategy Management & Assessment team as part of scheduled assessment activities in 2026 (refer paragraph 41). *Responsibility* – Special Operations Component Commander.
- e. The IM Programme. Significant benefits realisation hinge on the successful implementation of the IM Programme (refer paragraph 35) within current forecasted years. *Responsibility* – Commander Information Command.

Assurance Plan for Assessing System Health

41. The OLEP Steering Committee has acknowledged the requirement for, and benefits gained from, on-going assessment of the frameworks, mechanisms and systems implemented through this programme. Accordingly, the MoD Strategy Management & Assessment team intends to include assessment of OLEP benefits maturity as part of their 2026 assessment programme (subject to Minister of Defence approval), and this will further formalise the assessment processes as part of 'Business as Usual' practices. A range of Lead Measures to support the assurance assessment process is at Annex D.
42. Additionally, and where necessary, Defence functional areas and line managers have been instructed to, or given authority to, conduct continuous improvement activities within their respective areas of responsibility, to ensure systems and processes remain fit-for-purpose.

CONCLUSION

43. This Closure Report has detailed the background to the Inquiry; the Expert Review Group; the subsequent work of the OLEP team and the outcomes implemented in response to each of the ERG's recommendations. The report also specifies where responsibilities to complete action, continue embedding culture and behaviour change, or maintain new services is now mainstreamed with relevant functional areas and line managers. Where necessary an assessment of futureproofing work that will enhance initiatives and/or mitigate risk to on-going processes and benefits has been provided. Residual risk lies with initiatives outside our scope of control, for example the Information Management Project, however there is confidence that appropriate mechanisms are in place within those programmes to mitigate risk.
44. The OLEP team has now concluded all work (in scope) that it can deliver or directly influence and formally recommends programme closure.

RECOMMENDATION

45. It is recommended that the CDF and SECDEF:

- a. **approve** closure of the Operations Lifecycle Enhancement Programme.

Endorsed:

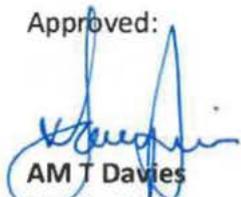

RADM M WILLIAMS
OLEP Steering Committee Co-Chair
New Zealand Defence Force

Date: 25 / 6 / 25


R SCHMIDT
OLEP Steering Committee Co-Chair
Ministry of Defence

Date: 25/6/25

Approved:


AM T Davies
Chief of Defence Force
New Zealand Defence Force

Date: 25 JUN 25


Dr B Barrington
Secretary of Defence
Ministry of Defence

Date: 25 June 25

Annexes:

- A. Expert Review Group Recommendations.
- B. Expert Review Group: Recommendations Implementation.
- C. Operations Lifecycle Enhancement Programme – Intervention Logic Map.
- D. Assurance – Lead Measures.

Expert Review Group Recommendations

#	Recommendation
1	<p>We recommend the Minister of Defence direct the Secretary of Defence and Chief of Defence Force to strengthen integration between the NZDF and Ministry of Defence throughout the deployment lifecycle and at all levels of both organisations.</p> <p>As part of this direction, the Chief of Defence Force's terms of reference and the Secretary of Defence's performance expectations should state that the statutory term "major matters of defence policy" includes complex military operations that impact on national or international security.</p>
2	<p>We recommend the NZDF and Ministry of Defence strengthen integration throughout the deployment lifecycle and at all levels of both organisations. In particular, we recommend:</p> <p>2.1 the Vice Chief of Defence Force and Deputy Secretary Policy and Planning, in consultation with other national security agencies, develop and document an integrated deployment lifecycle with clear accountabilities and participation rights for NZDF and the Ministry of Defence across the whole deployment.</p> <p>2.2 the Secretary of Defence and Chief of Defence Force, together with the Ministry of Foreign Affairs and Trade and the Department of the Prime Minister and Cabinet, institutionalise the use of senior reference groups for complex and extended deployments to strengthen interagency cooperation and knowledge sharing across relevant government agencies throughout the deployment lifecycle.</p> <p>2.3 the Secretary of Defence and Chief of Defence Force:</p> <ul style="list-style-type: none"> • work together to ensure measures of success are included in advice to Cabinet on the mandate for complex operational deployments; • put in place post-deployment reviews to evaluate performance against these measures. <p>2.4 the Chief of Defence Force ensure a senior Ministry of Defence representative is appointed to the Strategic Risk Assessment Board and representatives of other national security agencies as appropriate.</p>
3	<p>We recommend the Secretary of Defence and Chief of Defence Force work together to develop the capability required to embed the integrated deployment lifecycle. In particular, we recommend the:</p> <p>3.1 Secretary of Defence work with the Chief of Defence Force to build a policy adviser (POLAD) capability, including agreeing clear accountabilities, reporting lines and required skill sets. Other national security agencies could be involved in growing this capability.</p> <p>3.2 Chief of Defence Force mandate exposure to the broader policy context as part of a structured training and development programme for NZDF future leaders, including through secondments to other government agencies, the Office of the Minister of Defence and the Office of Chief of Defence Force.</p>

#	Recommendation
3.3	Commander Joint Forces New Zealand, NZDF Strategic Commitments and Engagements Branch and Ministry of Defence identify opportunities to test the effectiveness of integrated working arrangements, including the POLAD function.
4	<p>We recommend the Chief of Defence Force, in consultation with the Secretary of Defence, review the suitability of particular elements of Headquarters NZDF for the future. As part of this review, we recommend the Chief of Defence Force:</p> <p>4.1 establish with the Secretary of Defence an integrated strategic military and policy function that provides for the end-to-end strategic management of operations.</p> <p>4.2 reduce the span of control of the Office of Chief of Defence Force (OCDF) and prioritise its core functions, including those related to the Chief of Defence Force's operational and strategic responsibilities and external accountabilities for democratic oversight.</p> <p>4.3 direct that <i>NZDF Public Affairs Strategy 25</i> be revised to reflect key accountability relationships and position NZDF communications to meet contemporary accountability and transparency expectations.</p>
5	<p>We recommend the Chief of Defence Force ensure that steps continue to be taken to integrate the New Zealand Special Air Service (NZSAS) into the wider NZDF and national security sector. In particular, we recommend the Chief of Defence Force:</p> <p>5.1 integrate one or more Special Operations staff officer roles into the strategic military and policy function (see Recommendation 4) to enable appropriate transparency, oversight, assurance and strategic awareness of Special Operations.</p> <p>5.2 facilitate, in consultation with the Secretary of Defence, a broader discussion with other New Zealand defence, security and foreign affairs agencies about the role of the NZSAS in modern warfare and national security and its contribution to government priorities now and in the future</p> <p>5.3 take a strategic and proactive approach to developing NZSAS leadership capability for the future and regularly monitor the leadership climate created by NZSAS leaders; in particular, by providing current commanders and high-potential personnel with opportunities to develop political acumen and a better understanding of the wider government authorising environment, including policy advice processes, the importance of democratic oversight and how to develop networks across the national security sector.</p>
6	<p>We recommend the Chief of Defence Force improve the management of stored information by:</p> <p>6.1 defining and identifying NZDF's high-interest and high-value information and the records needed to support defence interests across all systems and locations (including legacy information)</p> <p>6.2 prioritising the appraisal, declassification and disposal (as appropriate) of high-interest and high-value information.</p>

#	Recommendation
7	[To] reconsider the balance of leadership, accountabilities and responsibilities between the Chief Information Officer and Chief Data Officer to ensure they properly reflect the importance of information and knowledge.
8	[That] Vice Chief of Defence Force be given overall accountability and responsibility for the end-to-end stewardship of the flow and fidelity of operational knowledge of public and political interest across the NZDF.
9	[That] Commander Joint Forces New Zealand identify opportunities to test information management systems and practices and knowledge flow, focusing on scenarios requiring the transfer of operational knowledge that is likely to be of public and political interest across multiple classifications and locations.

ERG Report Part One: Policy and Military Integration

- The Defence Act 1990 imposes broad consultation obligations on the Secretary of Defence and Chief of Defence Force within a framework of providing complementary yet contestable advice to the Minister.
- The NZDF and MoD require well-established joint working arrangements throughout the 'deployment lifecycle' with formally agreed roles and responsibilities. Policy needs to be grounded in reality.
- The Minister must be provided with both policy and military considerations to provide assurance they have information and advice required to properly exercise democratic oversight.
- Measuring and assessing whether an NZDF deployment is meeting or has met the Government's strategic objectives should be a key component of the mandate.
- New Zealand needs to align itself with international partners in terms of generating and maintaining a deployable Policy Advisor function.

ERG Recommendations	Outcome: What has been achieved	Evidence	Comments and Futureproofing
<p>Recommendation 1: We recommend the Minister of Defence direct the Secretary of Defence and Chief of Defence Force to strengthen integration between the NZDF and Ministry of Defence throughout the deployment lifecycle and at all levels of both organisations.</p> <p>As part of this direction, the Chief of Defence Force's terms of reference and the Secretary of Defence's performance expectations should state that the statutory term "major matters of defence policy" includes complex military operations that impact on national or international security.</p>	<ul style="list-style-type: none"> • The Defence Operations Lifecycle Framework (OLF) (see also Recommendation 2) codifies the requirement for MoD and NZDF to mutually consult on 'complex military operations.' • Jul 2023 – Defence OLF design agreed by CDF & SECDEF. • Sep 2023 – Defence OLF begins delivery (Planning & Decision stages) with existing NZDF operations mandate renewals. • OLF process design trials and rollout of remaining stages (In Operation & Post Operation Analysis) over the following 12-month period. • MoD/NZDF Defence OLF Memorandum of Arrangement (MoA) signed March 2025. • This intent has also been included in the CDF Directive 04/2025 to formally authorise implementation of the Defence OLF in NZDF. • Relevant expectations were issued to the SECDEF by Te Kawa Mataaho Public Service Commission in 2022, 2023, and 2024/25, and is reflected in the updated Position Description issued in 2024. • Relevant expectations were issued by the Minister of Defence to the CDF in 2021 and 2023. 	<ul style="list-style-type: none"> > 2022 SECDEF expectations: Implement the Expert Review Group's recommendations including: <ul style="list-style-type: none"> • with the NZDF, strengthen integration throughout the deployment life cycle. • embed in Ministry policies, procedures and culture that the statutory term "major matters of defence policy" includes complex military operations that impact on national or international security." > 2023 SECDEF expectations: Implement the Expert Review Group's recommendations including: <ul style="list-style-type: none"> • embed in Ministry policies, procedures and culture that the statutory term "major matters of defence policy" includes complex military operations that impact on national or international security. • with the NZDF, strengthen integration throughout the deployment life cycle. > 2024/25 SECDEF expectations: Implement the MoD recommendations of the Expert Review Group: <ul style="list-style-type: none"> • The Operations Lifecycle Enhancement Programme is embedded. • MoD takes leadership under the Operational Lifecycle framework integrated with NZDF and other government agencies. > 2024 updated SECDEF Position Description: <ul style="list-style-type: none"> • Co-lead (with NZDF) the Operations Lifecycle Enhancement Programme team to implement the recommendations of the Operation Burnham Inquiry and Expert Review Group. > 2021 CDF expectations: <ul style="list-style-type: none"> • Progress the implementation of the Government's responses to the Inquiry into Operation Burnham. • Implement the recommendations arising from the report of the Expert Review Group, established following the Inquiry into Operation Burnham. > 2023 CDF additional expectations: <ul style="list-style-type: none"> • Evidence that you have embedded in the NZDF culture, policies and procedures that consultation on "major matters of defence policy" between the Secretary of Defence and you include those complex military operations that impact on national or international security. • New working arrangements between the NZDF and the Ministry of Defence on deployments including senior 	<ul style="list-style-type: none"> ▪ The OLF codification process involved: <ul style="list-style-type: none"> ◦ detailed design phase (including workshop sessions with inter-agency partners, facilitated by external business process consultants) to document the OLF end-to-end process; ◦ process design phase to document the high-level and sub-level processes for each OLF stage, including identification of required artefacts; ◦ trial phase to evaluate each OLF stage, and ◦ rollout phase to formalise implementation of the OLF across the Defence agencies. ▪ Now that integration is codified in the OLF, specific wording in expectations documents are no longer necessary.

Released under the Official Information Act 1982
Expert Review Group: Recommendations Implementation.

		<p>reference groups being used for complex and extended deployments.</p> <ul style="list-style-type: none"> ➤ Approved MoD/NZDF Defence OLF MoA dated 25 March 2025. ➤ CDF Directive 04/2025, formally authorising implementation of the Defence OLF in NZDF. 	
<p>Recommendation 2: We recommend the NZDF and Ministry of Defence strengthen integration throughout the deployment lifecycle and at all levels of both organisations. In particular, we recommend:</p> <p>2.1 the Vice Chief of Defence Force and Deputy Secretary Policy and Planning, in consultation with other national security agencies, develop and document an integrated deployment lifecycle with clear accountabilities and participation rights for NZDF and the Ministry of Defence across the whole deployment.</p> <p>2.2 the Secretary of Defence and Chief of Defence Force, together with the Ministry of Foreign Affairs and Trade and the Department of the Prime Minister and Cabinet, institutionalise the use of senior reference groups for complex and extended deployments to strengthen interagency cooperation and knowledge sharing across relevant government agencies throughout the deployment lifecycle.</p> <p>2.3 the Secretary of Defence and Chief of Defence Force:</p> <ul style="list-style-type: none"> • work together to ensure measures of success are included in advice to Cabinet on the mandate for complex operational deployments. • put in place post deployment reviews to evaluate performance against these measures. <p>2.4 the Chief of Defence Force ensure a senior Ministry of Defence representative is appointed to the Strategic Risk Assessment Board and representatives of other national security agencies as appropriate.</p>	<ul style="list-style-type: none"> • The Defence Operations lifecycle Framework (OLF) has been codified and implemented. It comprises four deliberate stages: Planning, Approval, In Operation Monitoring and Post-Operation Analysis. The Defence OLF was co-designed in consultation with key functional teams in NZDF and MoD. • The Defence Operations Consultation Committee (DOCC) has been formalised and implemented. Core attendees represent the Defence Agencies (NZDF and MoD), MFAT and DPMC, with other government agencies attending as required. • The Strategic Risk Assessment Board has matured and now includes representation from NZDF, MoD (Head International Branch) and other agencies within the national security sector e.g. MFAT, on an 'Operation specific' basis. • NZDF continues to progress <i>Defence Force Instruction (DFI) 21.11 Special Access Programmes and Compartments</i>, which will set out the policies and direction to be followed when determining, authorising and managing NZDF Special Access Programmes and compartmented activities. Indications are DFI 21.11 will be completed in 2025. <p>Note: The ERG use of the term "complex operational deployments" was intended to contain the change workload to operations of high political and public interest. In practice, this intent was met by defining OLF design scope as 'Cabinet-mandated Operations.' This recognises that complexity is a continuum, can change rapidly, and not all Operations are overseas.</p>	<ul style="list-style-type: none"> ➤ The Defence OLF is supported by a Memorandum of Arrangement (signed in March 2025) between NZDF and MoD that gives effect to the implementation of the framework. ➤ Agency-specific processes have been completed to authorise the Defence OLF within each agency (CDF Directive in NZDF; dissemination within MoD) and assign specific tasks for on-going management of the Defence OLF where necessary. ➤ A Defence OLF resource site accessible via the Defence Intranet Launch Page provides guidance and awareness for all NZDF personnel and MoD staff, and supports those involved in using the Defence OLF. ➤ All current NZDF personnel and MoD staff that contribute to or participate in delivery of the Defence OLF have been briefed on the framework, including detailed process diagrams and DDMS archiving procedures. ➤ Introduction to the Defence OLF is now included in standard staff induction processes within both NZDF and MoD. ➤ The DOCC completed its inaugural meeting in October 2022. The forum is now on a tri-annual meeting schedule. ➤ Measures of Success (assessment of Strategic Objectives) are now routinely included in Cabinet submissions, as evident in recent paper on NZDF deployment under the Operation TIEKE (support to Ukraine) mandate. ➤ All stages of the OLF are now mainstreamed within NZDF and MoD. Strategic Planning processes initiate each deployment process, and operational advice provided supports these strategic aims. The POLAD at HQJFNZ, members of SCE, and IB consistently engage on issues arising during the conduct of deployments to determine how and whether Ministers should be advised s.6(a) <p>provide a good example of the day-to-day application of these ways of working.</p> <ul style="list-style-type: none"> ➤ In Operation monitoring of strategic objectives has been completed on all current NZDF Cabinet mandated operations as part of an enduring schedule. ➤ Post-Operation Analysis of completed NZDF deployments, including assessment of Measures of Success, has been completed for Operation S.6(a) 	<ul style="list-style-type: none"> ▪ Enduring success of the DOCC requires ongoing commitment from all agencies. The DOCC is currently administered by MoD International Branch but requires substantive agenda input and material support from all agencies. ▪ Anecdotal feedback indicates good practices are also now influencing routine operations and training. ▪ On-going knowledge development and regular training on the Defence OLF will enable the enduring benefit of this work. ▪ Trust and good working relationships, led from the top, between leadership (to build a culture of engagement) and at a more practical level (to facilitate flow of information and useful advice) between HIB, ACSCE and COMJFNZ are crucial to the effective ongoing implementation of the Defence OLF.
<p>Recommendation 3: We recommend the Secretary of Defence and Chief of Defence Force work together to develop the capability required to embed the integrated deployment lifecycle. In particular, we recommend the:</p> <p>3.1 Secretary of Defence work with the Chief of Defence Force to build a policy adviser (POLAD) capability, including agreeing clear</p>	<ul style="list-style-type: none"> • The Defence Policy Adviser (POLAD) programme has been implemented. • All NZDF personnel, and in particular NZDF Future Leaders, receive formal education on Defence policy via training programmes delivered through Single Service and NZDF (Command and Staff College) training establishments. 	<ul style="list-style-type: none"> ➤ The Defence POLAD programme is supported by a Memorandum of Arrangement (signed in October 2024) between NZDF and MoD that gives effect to the deployment of MoD POLADs to a military theatre. ➤ A lead POLAD has been appointed from within MoD International Branch, responsible for managing a cadre of POLADs. 	<ul style="list-style-type: none"> ▪ s.9(2)(f)(iv)

<p>accountabilities, reporting lines and required skill sets. Other national security agencies could be involved in growing this capability.</p> <p>3.2 Chief of Defence Force mandate exposure to the broader policy context as part of a structured training and development programme for NZDF future leaders, including through secondments to other government agencies, the Office of the Minister of Defence and the Office of Chief of Defence Force.</p> <p>3.3 Commander Joint Forces New Zealand, NZDF Strategic Commitments and Engagements Branch and Ministry of Defence identify opportunities to test the effectiveness of integrated working arrangements, including the POLAD function.</p>	<ul style="list-style-type: none"> • NZDF operates a structured approach to career development and a secondment/personnel rotation programme for selected individuals. (see also Recc. 5.3) • Renewed attention has been applied to the running of Strategic Planning Groups as a key enabling activity under the Defence OLF. • Military exercises provide opportunities to exercise integrated working arrangements between agencies at the strategic level and the flow of advice to/from HQ JFNZ. (see also Recc. 9) 	<ul style="list-style-type: none"> ➤ POLADs have deployed on NZDF operational missions e.g. Operation SIAS s.6(a), and they are planned to participate in a number of exercises in 2025 and 2026, s.6(a) ➤ s.6(a) ➤ Formal Defence Policy training in NZDF is supported by in-service publications, specifically the New Zealand Defence Doctrine Publication – Defence (4th Edition). ➤ Reference to the ERG Report and findings is included in specific formal training (<i>Introduction to Service Law and Legal Compliance</i> modules) to all NZDF personnel. ➤ NZDF Future Leaders undertaking studies at the NZDF Command and Staff College (selected Commissioned Officers and Warrant Officers) are required to read the ERG Report in full. The <i>Report of the Government Inquiry into Operation Burnham and Related Matters</i> is provided as supplementary reading. ➤ The NZDF uses the Education and Experience Framework (EEF) for career development of Lieutenant Colonel (equivalent) Commissioned Officers and above. ➤ The Secondment/Personnel Rotation Programme is supported by use of the Public Service Commission Sector Career Boards process for senior leaders, along with the EEF component focusing on <i>Significant External Networks</i>. 	<p>s.9(2)(f)(iv)</p> <ul style="list-style-type: none"> ▪ Building a wider POLAD cohort in MoD is also a continuous process, requiring on-going investment and pipeline management.
---	---	--	---

ERG Report Part Two: Headquarters NZDF

- The Office of the CDF needs to be better configured to support the CDF and VCDF on both strategic military and corporate matters. However, the focus needs to be on prioritisation of core functions, namely those related to CDF's operational and strategic responsibilities and external accountabilities for democratic oversight.
- Consider the opportunity to strengthen processes and resilience of the Office of the CDF and by consequence, alongside *Part One: Policy and Military Integration* initiatives, deliver greater integration between NZDF and MoD on complex operational deployments.
- Defence Public Affairs focus needs to strike the correct balance on protecting & enhancing the NZDF's reputation, while advancing transparency in its communications.

ERG Recommendations	Outcome: What has been achieved	Evidence	Comments/Futureproofing
<p>Recommendation 4: We recommend the Chief of Defence Force, in consultation with the Secretary of Defence, review the suitability of particular elements of Headquarters NZDF for the future.</p> <p>As part of this review, we recommend the Chief of Defence Force:</p> <p>4.1 establish with the Secretary of Defence an integrated strategic military and policy function that provides for the end-to-end strategic management of operations.</p> <p>4.2 reduce the span of control of the Office of Chief of Defence Force and prioritise its core functions, including those related to the Chief of Defence Force's operational and strategic responsibilities and external accountabilities for democratic oversight.</p> <p>4.3 direct that <i>NZDF Public Affairs Strategy 25</i> be revised to reflect key accountability relationships and position NZDF communications to meet contemporary accountability and transparency expectations.</p>	<ul style="list-style-type: none"> • The Defence Operations Lifecycle Framework (OLF) has been codified and implemented. It comprises four deliberate stages: Planning, Approval, In Operation Monitoring and Post Deployment Analysis. • The Defence Operations Consultation Committee (DOCC) has been formalised and implemented. Attendees represent the Defence Agencies (NZDF and MoD), MFAT and DPMC. • The Defence Policy Advisor (POLAD) programme has been implemented. • Office of CDF (OCDF) People, Process and Structure Review focusing on OCDF core functions, strengthening of process delivery and improving resilience, approved by CDF. <ul style="list-style-type: none"> ◦ <u>Note:</u> The recommended 'lift and shift' of Business Units and individual positions from the OCDF to other NZDF portfolios did not occur, following consultation with CJDS, CPO and CoS HQNZDF. • The <i>NZDF Public Affairs Strategy 25</i> was revised, renamed and issued in late 2022. 	<ul style="list-style-type: none"> ➢ Points above relating to: <ul style="list-style-type: none"> • the Defence OLF, • the POLAD programme, and • the DOCC. ➢ Key roles under the CoS HQNZDF, previously vacant, are filled and maintained, and acknowledged as integral to on-going process effectiveness. Additionally, the establishment and filling of a Deputy CoS position has enhanced information processing within OCDF and contributed to more effective integration with Office of VCDF (OVCDF) e.g. VCDF now briefed on all matters raised with CDF (enhanced situational awareness). ➢ Renamed the <i>NZDF Public Affairs Strategy</i>, the document cites "This second version of the strategy was approved on 21 September 2022 following revisions in response to the Expert Review Group report." 	<ul style="list-style-type: none"> ➢ Concurrent work on the NZDF Portfolio Change project is expected to result in further integrated working practices between OVCDF and OCDF personnel and strengthen the clarity of VCDF role in HQNZDF.

ERG Report Part Three: New Zealand's Special Forces

- The NZSOF (NZSAS) focus should be on improved integration with the wider NZDF and national security sector.
- The NZDF needs to continue to invest in training and development of future NZSOF leaders and high-potential personnel, particularly in terms of broader government awareness.
- NZSOF need to maintain strong and present leadership and well-understood values; collective (NZDF and NZSOF) reinforcement of both NZSOF tenets and NZDF values.
- Deployed NZSOF need to be well supported by NZDF leadership and have access to integrated policy and military advice.

ERG Recommendations	Outcome: What has been achieved	Evidence	Comments/Futureproofing
<p>Recommendation 5: We recommend the Chief of Defence Force ensure that steps continue to be taken to integrate the New Zealand Special Air Service (NZSAS) into the wider NZDF and national security sector. In particular, we recommend the Chief of Defence Force:</p> <p>5.1 integrate one or more Special Operations staff officer roles into the strategic military and policy function (see Recommendation 4) to enable appropriate transparency, oversight, assurance and strategic awareness of Special Operations.</p> <p>5.2 facilitate, in consultation with the Secretary of Defence, a broader discussion with other New Zealand defence, security and foreign affairs agencies about the role of the NZSAS in modern warfare and national security and its contribution to government priorities now and in the future.</p> <p>5.3 take a strategic and proactive approach to developing NZSAS leadership capability for the future and regularly monitor the leadership climate created by NZSAS leaders; in particular, by providing current commanders and high potential personnel with opportunities to develop political acumen and a better understanding of the wider government authorising environment, including policy advice processes, the importance of democratic oversight and how to develop networks across the national security sector. (see also Recc. 3.2)</p>	<ul style="list-style-type: none"> • To optimise scarce New Zealand Special Operations Forces (NZSOF) resources, direct engagement with the strategic military and policy teams (NZDF SCE Branch and MoD International Branch) now occurs via a nominated Special Operations Command point of contact. • Increased NZSOF representation at Inter-agency forums. • NZSOF has completed the NZSOF Operating Concept and briefed it to the National Security Board. • NZSOF Officers are included in the NZDF Education, Career Development and Secondment/Personnel Rotation processes. 	<ul style="list-style-type: none"> ➢ NZSOF represent NZDF (alongside SCE Branch personnel) on the Inter-agency Counter Terrorism Coordination Committee. ➢ NZSOF Operating Concept document (<i>Te Maia Hei Toa: The role of New Zealand Special Forces in modern warfare and national security</i>) was publicly released in April 2024. This increased transparency and public trust. Media commentary on the release of the document was positive. ➢ NZSOF senior Commissioned Officers are now seconded to posts within DPMC and MFAT ISED, and the NZSOF Officer career development model has been updated to incorporate specified secondment opportunities for selected individuals. 	<ul style="list-style-type: none"> ▪ Residual risk remains in respect to resources available to SOCC to enable strategic engagement. ▪ Acknowledging the importance of NZSOF secondments, these are approved at the NZDF Senior Appointments Board and managed by the Directorate of Career & Talent Management, in consultation with the Special Operations Component Commander.

ERG Report Part Four: Information Management and Flow of Defence Knowledge

- Information and knowledge are organisational assets and require careful management.
- NZDF is a large and complex organisation that relies on timely and accurate record-keeping, information storage and information flows both to properly advise and inform the MINDEF and for its strategic and operational decision-making and planning.

ERG Recommendations	Outcome: What has been achieved	Evidence	Comments/Futureproofing
<p>Recommendation 6: We recommend the Chief of Defence Force improve the management of stored information by:</p> <p>6.1 defining and identifying NZDF's high-interest and high-value information and the records needed to support defence interests across all systems and locations (including legacy information).</p> <p>6.2 prioritising the appraisal, declassification and disposal (as appropriate) of high-interest and high-value information.</p>	<ul style="list-style-type: none"> Codification of the Defence OLF has identified Minimum Viable Artefacts (MVA) that must be electronically retained and established a revised DDMS storage process in HQNZDF for all NZDF strategic level operations information. Acknowledgement across Defence agencies of the value and requirement for dedicated Information Managers embedded in key units. Upgraded storage of legacy physical documents from past NZDF operations has been put in place. Upgrade of HQJFNZ mission information sites is under action, within the constraints of the current DDMS architecture. Information Management practices on deployed NZDF operations are more structured and personnel are better aware of record keeping and disposal obligations. Existing intelligence production and recording for senior leaders by NZ Defence Intelligence IAW requirements of Output 6.2.1 remains extant. 	<ul style="list-style-type: none"> Shared NZDF & MoD access to the SCE Branch DDMS sites for NZDF operations, managed by the SCE Branch Information Manager (IM). MVA are detailed in the <i>Defence OLF: Guidelines & Process Document</i> and on each NZDF operation library within the SCE Branch DDMS site. Defence Assessment Team (MoD) are currently conducting a Discovery Assessment of the Defence OLF Information Management interim solution. Specialist IM staff reside in key areas e.g. SCE Branch and MoD Ministerial and Executive Services. Other NZDF portfolios have personnel undertaking IM duties to manage respective DDMS sites e.g. DSM, OCDF. MoD similarly has an IM expert on staff. As a pre-requisite for established Pre-Deployment Training (PDT) for NZDF operations, on-line formal training (Manage Information Fundamentals) now occurs. The PDT course content includes IM, Operational Security and Handling Sensitive Information modules. Pan-NZDF Disposal Authority approved by the Chief Archivist of New Zealand and promulgated in CIDS Administrative Instruction 02/2023. Chief Data Officer has delegated responsibility to support awareness of the disposal authority and monitor disposal activity NZDF-wide. 	<ul style="list-style-type: none"> The NZDF Information Management Programme is expected to deliver a system-wide uplift, including: <ul style="list-style-type: none"> Improved identification of high-interest/high-value information through metadata tagging on NZDF systems. Improved recording of high-interest/high-value information through NZDF Asset Registers. s.6(a)
<p>Recommendation 7: We recommend the Chief of Defence Force reconsider the balance of leadership, accountabilities and responsibilities between the Chief Information Officer and Chief Data Officer to ensure they properly reflect the importance of information and knowledge.</p>	<ul style="list-style-type: none"> CDF directed the implementation of changes to unify the NZDF Information Environment, including establishment of a new Chief of the Information Environment (CIE). NZDF Information Command (INFOCOM) has been created, including establishment of the appointment of Commander INFOCOM (previously intended as CIE). The post of CID has been disestablished. 	<ul style="list-style-type: none"> The INFOCOM structure and focus will provide a healthy tension under a military framework to ensure information assurance: protected, well managed, and available. The INFOCOM operating model is being optimised and there is a strong focus on culture enhancement. The need for an information worthiness function within INFOCOM has been identified, to assure CDF that systems that comprise the Defence Information Environment are Fit for Purpose, Safe to Operate, Resilient and Sustainable. A proposal to shift the existing Defence Information Security under INFOCOM may form the basis for this information worthiness function, subject to EXCO decisions in June 2025. 	<ul style="list-style-type: none"> Commander INFOCOM intends to have the information worthiness function & framework (to provide information assurance) operating by 1 July 2025. The effectiveness of info assurance will require ongoing investment.
<p>Recommendation 8: We recommend the Chief of Defence Force direct the Vice Chief of Defence Force be given overall accountability and responsibility for the end-to-end stewardship of the flow and fidelity of operational knowledge of public and political interest across the NZDF. The information and knowledge management principles set out in this report (pages 68–69) are intended to aid the VCDF in exercising this stewardship role.</p>	<ul style="list-style-type: none"> Stakeholders agreed that 'stewardship' is defined as a <i>monitoring and assurance</i> role across the system, akin to the responsibilities VCDF has under their appointment as the NZDF Inspector General (see Note 1). The stewardship role is broader than the (existing) OCDF <i>management</i> of the flow and fidelity of information to/from CEs and Ministers. VCDF role guides alignment pan-NZDF. 	<ul style="list-style-type: none"> A CDF Directive authorising VCDF (as the NZDF Inspector General) to exercise stewardship of military operations information (mil ops info) flow and fidelity by directing assurance reviews and/or continuous improvement initiatives that strengthen mil ops info flow throughout the NZDF and with partner agencies. The CDF Directive will also set expectations for managers to provide support to the mil ops info monitoring and assurance activities directed by VCDF. 	<ul style="list-style-type: none"> The stewardship role will be permanently included in updated VCDF roles and responsibilities (DFI/ToR/PD), as part of the subsequent NZDF Portfolio Change project, expected to be in place by end of 2025.

<p>Recommendation 9: We recommend the Commander Joint Forces New Zealand identify opportunities to test information management systems and practices and knowledge flow, focusing on scenarios requiring the transfer of operational knowledge that is likely to be of public and political interest across multiple classifications and locations.</p>	<ul style="list-style-type: none"> • The Joint Readiness Exercise (JRE) was cancelled in August 2024, with Exercise KIWI COMMAND 25 (KC25) identified as a suitable replacement to assess mainstreaming of ERG intent. • Acknowledging indications of risk to KC25 execution, the Steering Committee agreed to a conditions-based approach to satisfying the intent of this Rec. The following three conditions were set as minimum: <ul style="list-style-type: none"> ○ Four months monitoring delivery of Strategic Planning Groups (SPG) and record keeping ○ Assurance from COMJFNZ that appropriate scenarios will be included in Op → Strat Command Post Exercise (CPX) as standard, and ○ Defence OLF Post-Operation Analysis review includes fidelity of joint advice to Ministers. 	<ul style="list-style-type: none"> ➢ In period Oct 2024 – February 2025, seven SPGs completed relating to Operations SOLAR, TIEKE and RESOLUTION. ➢ SPG Record of Discussion forms for all activities confirmed completed. New HQNZDF Quality Assurance Form issued for all correspondence transacted through Office of CDF. ➢ HQJFNZ (J5) confirmation that the requirement for appropriate scenarios in Op → Strat CPXs as standard is being directed in the Joint Collective Training Annex of the Joint Campaign Plan. ➢ Defence Assessment Team (MoD) confirm all post-operation reviews include assessment of information quality and flow: (1) between Tac & Strat levels, (2) between NZ & coalition partners, and (3) between Defence and Minister(s). The latter, as advised by DEPSEC Strategy Management and Assessment, focuses on whether accurate and timely strategic information was provided to Minister(s). 	<ul style="list-style-type: none"> ▪ KC25 is proving to be a suitable & on-going series of Op → Strat CPXs that will generate appropriate scenarios to satisfy this recommendation. ▪ The 2025 KC25 trial reconfirmed the need for SCE and POLAD participation for optimum learning, capability development, and assurance.
--	--	--	---

Additionally implied by the ERG:

<p>Implement the Information Management Programme (IMP).</p>	<ul style="list-style-type: none"> • Business Case approved by Cabinet in CY2024. The drivers for change refer to ERG change recommendations. • Tranche One implementation is scheduled for FY2025/26-2028/29 and will address current deficiencies in how NZDF manages data as a strategic asset. • Each tranche is broken into phases to maximise flexibility and ensure each phase is as informed as possible by the preceding phase. 	<ul style="list-style-type: none"> ➢ Refer to the <i>Information Management Programme – An Overview</i> document provided by the IMP team. 	
--	---	---	--

Note 1:

The Operational Preparedness and Reporting System (OPRES) informs CDF on the forecasted delivery of Outputs Classes 1 – 5.

VCDF, in the capacity of NZDF Inspector-General, is responsible for:

- (1) providing overall portfolio leadership for the OPRES solution;
- (2) coordinating the presentation of amalgamated Service OPRES results to CDF through the Outputs Committee;
- (3) independent audit of single Service OPRES data;
- (4) analysis of OPRES results and other relevant reports to assess the ability of the NZDF to deliver appropriate military response options in support of government policy; and
- (5) reporting of NZDF output preparedness performance, including OPRES summaries, to government.

Output 6 (Advice to Government) is not currently subject to OPRES. Retrospective performance assessment occurs annually as part of the NZDF Annual Report.

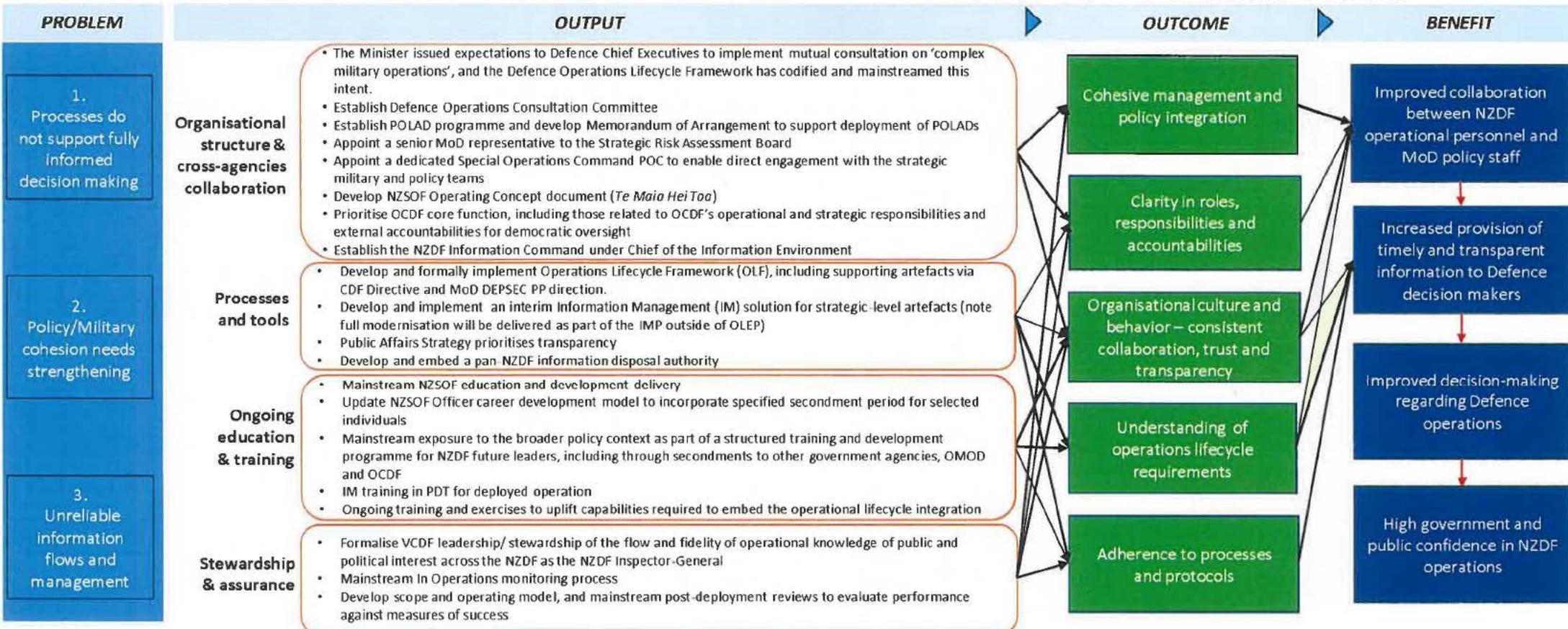
Operations Lifecycle Enhancement Programme - Intervention Logic Map

PROGRAMME MISSION

To create, improve or codify the systems, clarity, and integration across NZDF and MOD (and where appropriate the wider sector) to lift the quality, timeliness, and accessibility of information required to enable high quality and transparent decisions and actions.

VISION FOR THE FUTURE

Our vision is for the NZ Government, the national security sector, Defence leaders and the New Zealand public to have high levels of trust and confidence in the information provided to them. Defence will retain a strong social license to operate, because there is appropriate democratic oversight of the military, and transparency of military activities is both appropriate and trustworthy.



Assurance - Lead Measures

1. Lead measures tell us how likely we are going to achieve our goals by observing the drivers required to succeed. These are arranged into four output categories, with associated Key Performance Indicators (KPIs) and measures.

Output Category	KPI	Measure
Organisational structure & cross-agencies collaboration	Forums for cross-agencies collaboration	Forums enabling ongoing cross-agencies collaboration are in place.
	Capabilities	Number of POLADs ready for deployment.
		[%] OCDF positions filled to support operational and strategic governance responsibilities and democratic oversight.
Processes & tools	Access to and suitability of information flow system and supporting artefacts	Critical Incident Notification (CIN) system SOPs are up-to-date and accessible.
		[%] Knowing how to access Operations Lifecycle Framework (OLF) Guidelines and Process document when needed.
		[%] Able to store information in the Strategic Commitments & Engagements DDMS site when needed.
		[%] Able to easily locate information from the Strategic Commitments & Engagements DDMS site when needed.
Ongoing education & training	Education and training opportunities	Number of NZDF Exercises incorporating scenario that triggers practicing of the functional integrated lifecycle, including information flow, at the operational to strategic level.
		Number of NZDF Exercises including POLADs.
		[%] New NZDF personnel and MoD staff involved in the application of the OLF are introduced to the framework as part of their induction.
	Quality of education and training	Feedback from NZDF Exercises participants on the extent to which the exercises support good practice.
		Feedback from PDT participants in Information Management training for deployed operations.
	Capabilities	[%] Understanding of operations lifecycle requirements.

		[%] Perceived importance of adhering to information management processes and protocols.
		[%] Adherence to processes and protocols.
Stewardship & Assurance	Assurance	In Operations monitoring processes, post-deployment reviews and internal audits are undertaken to monitor process adherence and evaluate performance.
	Transparency	[%] operations-related OIAs are responded to within prescribed timeframe, with full and complete information available to responders.

A Suggested Reporting System for Assurance.

s.9(2)(g)(i)



30 Jun 2025 D0-0746

DOT-POINT BRIEF FOR DEPS and DCOMINFO

RESPONSE TO INFORMATION MANAGEMENT ISSUES IN NZDF AS RAISED BY COS HQNZDF

Purpose

1. The purpose of this Dot Point Brief is to outline the issue regarding the perceived loss of email search functionality, as it impacts ability to respond, in a timely and accurate manner to OIA requests and other obligations under various legislative acts and, to outline recommendations for remediation.

Executive Summary

2. NZDF is upgrading email functionality. Due to this, data searches on Restricted and Below (R&B) email now has heightened complexity, and the searches are hindered by shifting systems and fragmented repositories. Despite data search processes becoming increasingly sophisticated, data retrieval is still able to be completed.
3. The complexity of multiple Email enclaves require changes in the way in which data searches are enacted to ensure all the correct enclaves are being searched, particularly for recent data.
4. The timeframes of data searches will need to be extended at times due to deployed data instances, critical system upgrades, migration activities, and the breadth of the search requirements. The delay is expected to be for short periods e.g. days not weeks.
5. A resolution is not expected until the Information Management business case delivers the Enterprise Archive solution, and all users have been migrated to Exchange Online.

NZDF Email Environments

6. NZDF has ^{s.6(a)} Email environments, across all classifications, and one Email Archiving solution for Restricted and Below (R&B) email. There are ^{s.6(a)} enclaves within NZDF, including:

- R&B –A hybrid environment that is both On Premise (Exchange On-premise) and within Microsoft’s cloud service (Exchange Online).

- s.6(a)

- s.6(a)

- s.6(a)

7. The email archive solution, Quest Email Archive, stores emails archived from prior to 2013 through to April 2024. ^{s.6(a)}

Transformation of R&B Email and Email Archive

8. The Enterprise Architecture direction created during CIS Transformation Programme (CTP) identified the following two key transformations:
 - The need for an all-encompassing NZDF Information Archiving solution.
 - Migration of Microsoft 365 and Microsoft Exchange Online.
9. NZDF upgraded its email system from Exchange 2010 to 2016, then to Exchange Online. Quest Archive was incompatible with Exchange 2016, so emails are now stored under litigation hold. Litigation hold will continue in Exchange Online until a new archive solution is implemented. Business change impacts, especially for the Data Search team, were identified late, causing operational issues.
10. s.6(a)

Data Searching

11. Most data searches are required across R&B enclaves. Due to the changes and the transformation process that is underway, the Data Search team are having to search in multiple areas, while the transformations are completed, this includes:
 - Quest Email Archive for any emails prior to April 2024.
 - Exchange 2016 for any emails post April 2024 and for users who are not on Exchange Online.
 - Exchange Online for any users that have been migrated to Exchange Online.
 - s.6(a)
12. The OIA report commissioned in March identified several areas that needed to be improved to complete the required data searches. A Service Improvement Plan (SIP) is in place.

Recommendations:

13. Complete the SIP for OIA searches – under action with Deputy Director Cyber Security and Product Manager End User Compute.
14. Data Search processes updated to include searching of all enclaves – recommended this is owned by either Deputy Director Cyber Security or Ministerial Services.
15. Confirm ownership of Data Searches for OIA – recommend this is owned between Director Integration & Cyber Operations and Ministerial Services.
16. Completion of the Problem Management investigation and remediation activities for Deployed Emails – under action with Deputy Director Service Management, Product Manager Deployed and Product Manager End User Compute.
17. Advance the Application Migration (DIXS to Modern Desktop) line of effort - under action with Service Portfolio Product Managers.
18. Bring forward the delivery of the Enterprise Archive Solution – recommend this is owned by Chief Data Officer.

19. Investigate alternate options to simplify the searching process - recommend this is owned by Chief Data Officer.



K LOUGHLIN

Ms

PRODM EUD

Enclosure(s)

1. [Email Product Health with Email Enclave information](#)
2. [NZDF R&B Exchange Searching Report](#)
3. [OIA Service Improvement Plan](#)
4. [Deployed Problem case](#)

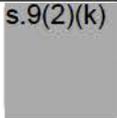
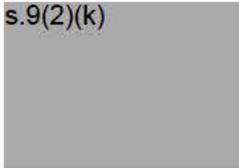


NZDF Exchange Searching Inquiry Report

Release Date:	24/02/2025
Version:	1.0
Project Reference:	
File Name	NZDF Exchange Searching Inquiry Report
Classification	Restricted
Status	Finalised

AUTHORISATION PAGE

This form records the approval and acceptance of this report for the NZDF Exchange Searching Inquiry. By signing this deliverable, each individual indicates an understanding of the purpose and acceptance of the content described in this deliverable.

Position	Name	Signature / Date
Product Manager End User Compute	Kim Loughlin	 s.9(2)(k) _13_ / _03_ / 2025
Deputy Director Cyber Security	Sue Critchlow	 s.9(2)(k) 11 / 03 / 2025

AMENDMENT RECORD

It is certified that the under mentioned revisions have been incorporated in this copy of the Report.

Amendments

Proposed amendments to this publication are to be forwarded in the first instance to the Product Manager End User Compute and Deputy Director Cyber Security.

Version History

Version	Change History	Incorporated by	Date
0.1	Initial Report Draft	s.9(2)(a)	24/02/2025
0.2	Report reviewed by Kim and Sue, track changes are on, Scott to review and approve or reject.	Kim Loughlin	10/03/2025
1.0	Final Version	Kim Loughlin and Sue Critchlow	11/03/2025

INTELLECTUAL PROPERTY OWNERSHIP

This document is a product of the New Zealand Defence Force (NZDF), is issued by the Product Manager End User Compute and Deputy Director Cyber Security..

The information is owned by NZDF Product Manager End User compute and Deputy Director Cyber Security.

REFERENCES

Ref	Document Title	Date of Issue	Version

Table of Contents

Authorisation Page	2
Amendment Record	3
Amendments	3
Version History	3
Intellectual Property Ownership	3
References.....	4
exchange mailbox searching inquiries	6
Background.....	6
Questions (EUC Management).....	6
Questions (Cyber security)	8
Questions (EUC team)	13
Additionally.....	16

EXCHANGE MAILBOX SEARCHING INQUIRIES

BACKGROUND

NZDF is modernizing the existing email infrastructure. Currently, the team is managing to migrate user mailbox from the on premise Exchange server 2016 to MS Exchange online email service. During the migration process, the internal teams are facing some issues which require to be clarified.

NZDF requires assistance from s.9(2)(j) to investigate the Exchange email searching issue on purged user mailboxes, Litigation hold configuration, existing email archive issue, and cyber security team permission issues.

The list of the questions is provided by the EUC support, Cyber security and EUC management teams. s.9(2)(j) will provide the solutions for each question and recommendations or provide workaround solutions to resolve the current issues.

QUESTIONS (EUC MANAGEMENT)

➤ ***Is the Litigation hold set up correctly***

Based on the conversation with Senior Engineer Enterprise Applications, the user offboarding script will enable the litigation hold and disconnect the user mailbox. If the user offboarding script is configured correctly, the process should satisfy the business requirements.

➤ ***Are the retention policies set up correctly?***

As I don't have visibility to the current retention policies, Senior Engineer Enterprise Applications can provide the details of the retention policies. As far as I can tell, the policies are in place for a long period without any issues. I assume the policies are meeting the business requirements.

➤ ***Does the Server Data Search Engineer is using have enough grunt or capacity or resources?***

Data Search Engineer demonstrated the issue he is facing, and s.9(2)(j) can confirm that the server that Data Search Engineer was using has no issue with resource, e.g. CPU, memory and disk capacity, etc. And Data Search Engineer is using the same management server with Senior Engineer Enterprise Applications and the rest of other team members. As a result, it's not server related issue but user account permission.

Recommendation:

At this stage, s.9(2)(j) recommend that we need to focus on the Data Search Engineer's access permission, especially on the exchange admin centre, eDiscovery permission settings.

➤ Does Data Search Engineer have the right level of access?

For exchange search, Data Search Engineer's user account is configured slightly different with the EUC team members due to his role and responsibilities.

For Archive manager, the account permissions are different between s.9(2)(a) and EUC team. Especially, after the Archive manager was restored from the major incident middle of last year. And Data Search Engineer indicated that he had to raise incident with EUC team to restore his Archive manager access permission manually. In addition, the archive manager searching issue is affecting all the Cyber team not Data Search Engineer only.

Overall, both issues are related to user account permission not the workstation level.

Recommendation:

Grant Data Search Engineer same privileged permission with EUC team on both Exchange admin centre and Archive manager, then test exchange and archive search. If the issues are cleared, progressively drop the Data Search Engineer's permission level and grant them the minimum required privilege to both exchange and archive manager.

➤ Why are people turning off litigation hold on emails? s.9(2)(g)(i)**Recommendation:**

- Enable litigation hold on all email accounts,
- Disable user AD account and disconnect user mailbox, **DO NOT** delete user AD account or mailbox for a time period depending on the organisation requirements,
- Run litigation hold check script to report on the litigation hold state on daily basis and raise alert when litigation hold is disabled,
- Organise an email distribution list and send the litigation hold report to all the relevant parties.

➤ Can we put in place alerts when Litigation hold is turned off?

Yes, Senior Engineer Enterprise Applications or any EUC team member can develop a PowerShell script to check Litigation hold state on daily basis. and organise an email distribution list and send the litigation hold report to all the relevant team members.

➤ ***Is Cyber Security over searching – the OIA requests are very clear***

Based on the demonstration the Data Search Engineer provided, the cyber security exchange email searching is reasonable and acceptable. Besides, both email archive and exchange searching reports are standard for security team.

QUESTIONS (CYBER SECURITY)

❖ Exchange Server:

➤ ***Misuse of Litigation Hold as Archive / No Archive***

Litigation Hold is primarily designed to preserve mailbox items for legal and compliance purposes by preventing the deletion of any emails. When a litigation hold is enabled on a mailbox; when any email is deleted it will be stored in the recoverable items folder. The emails will both be visible in the Outlook application on the user side, but the email will still be recoverable. Litigation hold does not fully replace an online archive. However, it can be a temporary work-around to ensure that the emails in the mailbox are not lost. Email archiving solutions typically offer more comprehensive features, such as easier search and retrieval, better storage management, and compliance with various regulations.

[In-Place Hold and Litigation Hold in Exchange Server | Microsoft Learn](#)

Recommendation:

Due to the delays with the Information Management Business Case Archive solution, it is recommended that NZDF investigate continuing to utilise Quest for the Archiving solution for all environments.

➤ ***Litigation Hold directly impacts ability to remove Data Spills***

Depending on the data retention policy, the litigation hold is a temporary solution or a workaround for the current archive issue. However, it should not be the long-term email archive solution.

Recommendation:

- Enable litigation hold on all user accounts until the email archive issue is fully resolved,
- Log a service support request with the Quest archive manager vendor to resolve the current email archive issue,

➤ ***Searches are missing records due to mailboxes being removed as part of offboarding***

Based on the information which provided by Cyber team, the disconnect user mailbox data should be kept in archive system for at least 15 years (legal reason). Due to the mailbox archive issue with current archive manager the archive service has failed after the email migration project was kicked off.

Recommendation:

Under current circumstances, ideally the offboarding policy should be updated. E.g. the offboarded user account should be disabled instead of deleted from both AD and exchange server until the email archive issue is fully resolved.

- Staff offboarding PowerShell script should be modified to disable user AD account and disconnect user mailbox instead of purging the user data,
- Disabled user account needs to move to “disabled user OU” and user group membership is “users” only,
- Litigation hold should be enabled on all user mailbox,
- PowerShell script to report disconnect user mailbox litigation hold state on daily basis,
- Enable litigation hold on the user mailbox which has been disabled.

➤ ***No present way to restore removed / archived mailboxes if needed as part of investigation, as there is limited space available, especially at scale and speed (restore all mailboxes for people that have left in past 12 months)***

Archive issue is fully resolved, however ensuring there is enough space on the server for the Data Search team is recommended.

➤ ***Demonstrated error in Running PowerShell script – likely cause being a combination of difference in Server or Permissions***

Based on the demonstration and the error message and user experience, it's not a local workstation policy related issue, but more user account permission problem. After further investigation on the error message, the user must be added as a member of the eDiscovery manager role group.

Recommendation:

- In Exchange Server, members of the Organization Management role group can create an In-Place Hold to place all mailbox content on hold. However, to create a query-based In-Place Hold, the user must be a member of the Discovery Management role group or have the Mailbox Search role assigned,

- PowerShell script to add user to the Discovery Management role group, Example: “Add-RoleGroupMember -Identity "Discovery Management" - Member <Identity>”,
- PowerShell script to add the members of the mail-enabled security group, example: “Add-RoleGroupMember -Identity "Discovery Management" - Member "Cyber Security",

Reference: [Assign eDiscovery permissions in Exchange Server](#)

- **When support is needed from Enterprise Applications Team due to above issues sometime these TickIT's are closed off without providing support – leaving the Data Search Engineer in a place where they are unable to action the request – impacting obligations.**

It could be a communication issue between the 2 teams. s.9(2)(j) suggest that both teams can sit together and resolve the problem..

Recommendation:

- Agree Operational Level Agreements between the Ministry, the Data Search team and the Enterprise Applications team
 - Arrange a meeting (could be virtual as many teams are working across Camps and Bases) with the assigned Enterprise Applications engineer,
 - Explain the current exchange search issue,
 - Cyber Security team follow the Privileged Access Process,
 - Cyber team tests PowerShell script during the meeting.
- **New errors encountered since some users migrated to Exchange Online – likely due to changes in SID.**
Example the Data Search Engineer is unable to search their email for any emails received from someone who has been migrated to Exchange Online.

Both Exchange Online and Exchange On Premise server are Microsoft products, however, they are different platform and different design concept. During the demonstration meeting, format of the primary SMTP in Exchange server 2016 is firstname.surname@nzdf.mil.nz, but the primary SMTP is changed to s.6(a) in exchange online, which caused the exchange mail searching issue.

According to Quest archive manger website, Quest archive manager supports system below:

- Supports Servers: Microsoft Exchange 2010 / 2013 / 2016 / 2019 and Office 365
- Access - Windows: Microsoft Outlook 2010 / 2013 / 2016 / 2019

- Archive Database (for metadata): Microsoft SQL Server 2008 R2 or newer / Oracle 11g R2 and above
- Access - Mac: Microsoft Outlook 2011 for Mac
- On Premise Archive Storage: All current media (DAS, NAS, SAN, Jukebox, Tape, EMC Centera, NetApp Filer, Hitachi HCP, DVD, CD-ROM, IBM Tivoli Storage Manager, Compliance, etc.)
- Access - Web: MS Outlook Web Access / Outlook Web App
- Cloud Archive Storage: Amazon S3, EMC Atmos, Rackspace, Windows Azure, Google Drive
- Access - Mobile: Access via IMAP server
- 32- and 64 bit Server support

If the organisation are planning to migrate to Office 365 and are currently using Archive Manager to archive messages from your current environment, the largest factor to consider is how NZDF plan to handle archiving in the future. If NZDF is planning to continue using Archive Manager to archive messages, the software can be configured to connect to your Office 365 account. After the configuration steps are completed to connect the software to NZDF account and mailbox settings are updated, Archive Manager handles mailboxes in Office 365 the same as on-premise Exchange mailboxes.

Reference: [Connecting Archive Manager to Office 365 \(4305654\)](#)

Recommendation:

- Enterprise application team should raise a request with Archive manager vendor and explain the current situation,
- Archive manager vendor to provide any possibilities to transfer or merge the current Onprem archive manager data to the future cloud version of archive manager,
- Archive manager vendor provides an estimated cost and system requirements to NZDF for further consideration,
- Enterprise application team provides the cloud version of archive manager to exchange migration team for the design decisions,

❖ **Exchange Online**

➤ ***Misuse of Litigation Hold in Exchange Online as Archive / No Archive***

Same comment with the On Premise exchange question,

➤ ***Litigation Hold directly impacts ability to remove Data Spills***

Same comment with the Onprem exchange question,

➤ ***Assumption that same issue with On Premise Searches missing records due to mailboxes being removed as part of offboarding will occur with Exchange Online Mailboxes***

Same comment with the On Premise exchange question,

❖ **Archive Manager: [2018 – 2024]**

- *As demonstrated the search functionality does not consistently work, where the Data Search team can see an email is in the archive but searching for it with keywords or subject doesn't return results.*
- *Also noting that additional testing with EA Engineers with same search criteria netted a difference in the number of results that returned.*
- *The Data Search teamgut feel is when that Archive failed and had to be rebuilt in 2024 everything was not restored as it was, the Data Search team know this as at that time their permissions didn't work.*
- *The Data Search team believe either that they are missing permissions that would provide them with the ability to see all results, or that there is an issue with the search functionality that has not been fixed.*

According to the demonstration and comments from Cyber team, the issue affects every team member in Cyber team and the issue occurred after the Archive manager server major incident happened last year. And user archive manager access permissions were recovered manually after the incident.

Recommendation:

- EUC engineer can provide Cyber team member same privilege with EUC team,
- Cyber team test the archive email search,
- EUC engineer can reduce the Cyber team access permission if required,

❖ **Exporting of Search Results:**

- *When results are exported, the Data Search team need to provide a way for the requestor to view them without risking that the results get reimported into exchange.*
- *Ideally a tool that can export search results in HTML or MIME format*

For email search results, EUC engineer can investigate and develop PowerShell script to export the search results in different format.

- **Change Management**

- ***Poor Communications regarding change / change management. While this isn't a technical Issue time and time again, the Data Search team encounters issues only to find out that changes have been made. All they are asking for is a heads up as an affected party / stakeholder.***

Normally, the Cyber team should get involved in every major change, even an FYI change request. Ideally, Cyber team should have permission to access all the change records. And Cyber team doesn't have to be a change approver, but the change requestor should seek technical advice from security perspective.

Recommendations:

- Cyber Security team attend the final day of PI Planning to understand what is occurring in the next 90 days
- Cyber Security are change reviewers of changes,

QUESTIONS (EUC TEAM)

- ***Search for content of existing mailbox the way it should be done (on-prem),***

The PowerShell script is working as expected and no issue found in the script. Moreover, the outcome of the script provides required details of the existing mailboxes.

Recommendation: keep the current PowerShell script and develop it only if new business requirement comes through.

- ***Search for the delete account (mailbox) is the correct way to run after the mailbox is delete after 30 days retention,***

```
<{$Disconnected = Get-MailboxDatabase | ForEach { Get-MailboxStatistics -Database $_.Name | Where-Object { $_.DisconnectReason -ne $Null } }>
```

Normally, by default, the keep deleted mailboxes limit is set to 14 days, but it can be updated to maximum 30 days. In general, the user mailbox will be permanently purged from the email system after the mailbox is deleted after 30 days. In other words, no matter what searching tools or power shell script we utilize to search the mailbox, it **will not** return any result.

➤ ***Litigation hold is not changing anything is there any retention for the litigation hold, (litigation hold policy),***

Litigation hold feature will help to preserve all the mailbox content, including deleted items, user archive mailbox and original version of modified items. With litigation hold feature, the items are preserved for a specific period or until you remove the mailbox from litigation hold. All mailbox items are returned in an In-Place eDiscovery in Exchange Server search.

In Exchange configuration, Litigation Hold can be turned on for individual users or an entire organization, and it can be set to automatically activate when certain conditions are met. And the litigation hold will apply on the user mailbox, and it can be enabled by using PowerShell script before the user AD account is disabled or deleted.

A mailbox becomes inactive when a Litigation Hold is placed on it and after this mailbox is deleted. In **Exchange Online**, the litigation hold is relied on the O365 license. After the litigation hold is in place, the license can be removed, and mailbox can be purged. However, the content of the deleted user mailbox can be searched by using mailbox search PowerShell script.

In addition, PowerShell script can generate a disabled user mailbox report which contains the litigation hold state. Without litigation hold and email backup, the user mailbox is unrecoverable after 30 days of deletion period.

If you delete a user account that has a mailbox, the Exchange Information store will eventually detect that the mailbox is no longer connected to a user account and mark that mailbox for deletion, even if the mailbox is on hold. If you want to preserve the mailbox, you have to do the following:

- Instead of deleting the user account, disable the user account.
- Change the properties of the mailbox to restrict the use and access to the mailbox. For example, set send and receive quotas equal to 1, block who can send messages to the mailbox, and restrict who can access the mailbox.
- Retain the mailbox until all data has been removed or until preserving the data is no longer required.

Reference: [In-Place Hold and Litigation Hold in Exchange Server](#)

To place all mailboxes on litigation hold, we can run the PowerShell command below:

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq 'UserMailbox'" |  
Set-Mailbox -LitigationHoldEnabled $true -LitigationHoldDuration 2555
```

This command places all mailboxes on hold with a hold duration of 2555 days (approximately 7 years).

Risk:

- Placing all mailboxes in an organization on hold can significantly impact mailbox sizes. In an Exchange Server deployment, plan for adequate storage to meet your organization's preservation requirements.
- Preserving mailbox data for a long duration will result in growth of the Recoverable Items folder in a user's primary mailbox and archive mailbox. The Recoverable Items folder has its own storage limit, so items in the folder don't count towards the mailbox storage limit. In Exchange Server, the default storage limit for the Recoverable Items folder is 30 GB. We recommend that you periodically monitor the size of this folder to ensure it doesn't reach the limit.

Reference: [Place all mailboxes on hold](#)

Recommendation:

- Enable the litigation hold on all the organization,
 - Create PowerShell script to provide litigation hold state report on daily basis and email to the related team for further investigation.
 - In exchange online, enable litigation hold before remove the user O365 license (save the organization cost),
 - Convert the disabled user mailbox to shared mailbox if required.
- ***The recovery process for disconnected user mailbox requires a new AD account, search will not be able to complete until the AD account is recovered.***

The prerequisite of recovering a disabled user mailbox is to restore the users AD account. Anyuser account can be restored from Active Directory recycle-bin (60 days). After 60 days period, the deleted user account can be created from AD manually then link the user mailbox account via exchange management console.

Be aware that the manual created user AD account has different GUID with the original one

Please refer to the link below for the recovery process details.

[Restore a Deleted User Mailbox](#)

Recommendation:

- Enable Active Directory recycle-bin,
- Email backup and restore application to satisfy the business requirements,
- Email recovery guide or documentation in Standard Operating Procedures

- ***If there is a need to recover the user mailbox from database backup, the process will be complicated,***

Based on the comment from Senior Engineer Enterprise Applications, the current backup solution will recover the mailbox database instead of individual user mailbox. During the limitation of the restore process, the restored mailbox database needs to be imported in separated exchange environment and recover the user mailbox from there.

Recommendation: Considering the limitation of the current backup solution, the organization will require a solution design for mailbox backup to replace the current backup solution in order to satisfy the business requirements.

ADDITIONALLY

The following questions were raised in MS technical forum website by s.9(2)(j) and the answers were provided by Microsoft expert.

- ***Is the litigation hold feature the right solution to replace email archive?***

Litigation Hold is primarily designed to preserve mailbox items for legal and compliance purposes by preventing the deletion of any emails. when a litigation hold is enabled on a mailbox; when any emails is deleted in will be stored in the recoverable items folder. The emails will both be visible in the outlook application to the user side, but the email will still be recoverable. litigation hold does not a full replace online archive. however, it can be temporary work around to ensure that the emails in mailbox are not lost. Email archiving solutions typically offer more comprehensive features, such as easier search and retrieval, better storage management, and compliance with various regulations

[In-Place Hold and Litigation Hold in Exchange Server | Microsoft Learn](#)

- ***With litigation hold enabled, how to search the user emails after the user mailbox is purged (after 30 days)?***

When a mailbox is placed on Litigation Hold, all items, including deleted and modified items, are preserved in the Recoverable Items folder. Even if the mailbox is purged, you can use eDiscovery search Microsoft purview to search and retrieve these items. The Content Search and eDiscovery features in the Microsoft 365 compliance centre allow you to search for and export the preserved items in entire mailbox including recoverable items folder.

[Recoverable Items folder in Exchange Online | Microsoft Learn](#)

In exchange server 2016, an item is considered to be soft deleted in the following cases:

- A user deletes an item or empties all items from the Deleted Items folder.
- A user presses Shift+Delete to delete an item from any other mailbox folder.

Soft-deleted items are moved to the Deletions subfolder of the Recoverable Items folder. This provides an additional layer of protection so users can recover deleted items without requiring Help desk intervention. Users can use the Recover Deleted Items feature in Outlook or Outlook on the web to recover a deleted item. Users can also use this feature to permanently delete an item. For more information, see:

- [Recover deleted items in Outlook for Windows](#)
- [Recover deleted items or email messages in Outlook on the web](#)

Items remain in the Deletions subfolder until the deleted item retention period is reached. The default deleted item retention period for a mailbox database is 14 days. You can modify this period for a mailbox database or for a specific mailbox. In addition to a deleted item retention period, the Recoverable Items folder is also subject to quotas. To learn more, see [Recoverable Items mailbox quotas](#) later in this topic.

When the deleted item retention period expires, the item is completely removed from Exchange Server.

The *Don't permanently delete items until the database is backed up* setting can affect this behavior. If this setting is not enabled (default), only the deleted item retention period is considered to remove items from the Deletions subfolder. If this setting is enabled and the deleted item retention period is reached, items are not deleted until after the mailbox database on which the mailbox is located has been backed up.

[Recoverable Items folder in Exchange Server | Microsoft Learn](#)

➤ ***Is the litigation hold still functional after the user mailbox is permanently removed from exchange database (on-prem)?***

If the mailbox is permanently removed from the on-premises Exchange database, the Litigation Hold is preserved on the mailbox as both the exchange server and exchange online have litigation hold feature

[In-Place Hold and Litigation Hold in Exchange Server | Microsoft Learn](#)

If you have an Exchange hybrid deployment, the following conditions are true when you move (onboard) an on-premises Exchange Server mailbox to Exchange Online in Microsoft 365 or Office 365:

- If the on-premises mailbox is on Litigation Hold or In-Place Hold, the hold settings are preserved after the mailbox is moved to Exchange Online.
- If the on-premises mailbox is on Litigation Hold or In-Place Hold, any content in the Recoverable Items folder is moved to the Exchange Online mailbox.

Hold settings and content in the Recoverable Items folder are also preserved when you move (offboard) an Exchange Online mailbox to your on-premises Exchange Server organization.