



# Defence Force Remuneration Tribunal

## DECISION

*Defence Act 1903*

s.58H—Functions and powers of Tribunal

### **JOINT CAPABILITIES GROUP: CYBER WARFARE EMPLOYMENT CATEGORIES** (Matter 5 of 2025)

MS B O'NEILL, PRESIDENT

MS A LESTER, MEMBER

CANBERRA, 23 MAY 2025

MAJGEN G FOGARTY AO RETD, MEMBER

[1] This decision arises from a listing application from the Australian Defence Force (ADF) for a determination to be made under Section 58H of the *Defence Act 1903* (the Act). The listing application<sup>1</sup> seeks to establish Cyber Warfare employment categories for use within the Officer Aviation Pay Structure (OAPS).

[2] We considered this matter in a hearing on 10 April 2025. Ms K Hagan appeared for the ADF and Mr K Wong for the Commonwealth. Major General R Watson CSC, Commander Cyber Command, and Colonel H Ashman CSM, Acting Commander, Cyber Forces Group, gave evidence for the ADF.

### **Background**

[3] The Tribunal previously considered employment categories for members working in cyberspace in Matter 12 of 2017 – *Royal Australian Navy: Cryptologic sailors*<sup>2</sup> and Matter 3 of 2019 – *Joint Cyberspace Warfare Employment Categories*.<sup>3</sup> These matters resulted in consolidating members into designated specialist career pathways.

[4] Cyber Warfare employment categories are currently remunerated through the Graded Officer Pay Structure (GOPS) and Graded Other Ranks Pay Structure (GORPS). The Chief of Defence Force (CDF) has directed a common approach to Cyber Warfare employment categories to ensure Defence builds a fit-for-purpose cyber workforce in the ADF, acknowledging that traditional workforce management techniques must be adapted given the competition for cyber security talent.<sup>4</sup>

[5] The *Defence Cyber Security Strategy 2024* emphasises the need for ‘innovative approaches to talent management and professional development to strengthen the workforce pipeline and develop future leaders’.<sup>5</sup> It outlines initiatives including seeking universal pay outcomes for the workforce, providing new pathways into Defence Cyber, and offering differentiated career models to assist with retention, all of which appear in this application.

## Submissions

### ADF

[6] The ADF submission proposes to establish Cyber Warfare employment categories within the OAPS and transition specified Cyber Warfare employment categories in their entirety from GOPS and GORPS to appropriate career pathways under the OAPS.

[7] The ADF specifically seeks to:

- a. adopt the 38-increment salary spine in the OAPS for the Cyber Warfare employment category;
- b. establish two competency streams for Cyber Warfare employment categories – one for officers and one for other ranks;
- c. establish three career progression pathways (Command, Specialist, and Staff) for the Air Force Cyber Warfare Officer employment category within the OAPS;
- d. establish a single Cyber Warfare career progression pathway for use by the Other Ranks Cyber Warfare Specialist employment categories;
- e. conduct initial placement into the OAPS for eligible members; and
- f. establish simple internal transfer protocols between the career progression pathways and competency streams that allow flexible movement without financial detriment to members.

[8] The ADF submits the Deliberately Differentiated Package Research Report, published by Defence People Group in 2022, “recognises that the ADF faces strong competition with industry to attract and retain Cyber specialists” and “many research participants expressed a desire to remain ‘on the tools’ as technical specialists and not progress to leadership roles”. Additionally, the report acknowledges ‘frustrations that career progression policy and the current pay structure do not adequately acknowledge the technical skillsets’ of Cyber specialists.<sup>6</sup> This submission addresses these concerns, whilst acknowledging the need for remuneration competitiveness and increased recruitment options.

[9] The ADF considered three main options for creation of the Cyber Warfare employment category with use of the OAPS being preferred. The ADF submits this is the optimal course, as use of the OAPS structure facilitates the following employee value propositions:

- common pay structure across the Services;
- commercial offers will have less influence on people's decisions to leave the ADF;
- multi-pathway careers including alternative career entry for all Service Categories;
- personnel can remain in operational/technical roles at rank, to meet capability demand, without detriment to future career options;
- reduce separation of skilled personnel from the ADF;
- reduce cost associated with replacing ADF personnel lost to separation;
- greater staffing achievements reduces hollowness, work tempo and personal stress, and meets structural growth; and
- create the conditions for workforce growth over time.<sup>7</sup>

[10] The ADF states that *'some inequities exist in the salaries currently earned by members of different Services who have similar skill sets and experience'*.<sup>8</sup> In order to deliver a common pay outcome for Cyber Warfare personnel, regardless of Service, the submission proposes to *'empower a Transition Management Board'* to provide assistance with initial placements into the OAPS. The Transition Management Board *'cannot place a member on an OAPS increment that is lower than their salary on the date of implementation'*, and will thus ensure no member will receive a negative salary placement. Personnel are intended to transition at, or at the closest increment above, current equivalent salary, which will be maintained until progression is justified by the gaining competency stream, pathway or rank.<sup>9</sup>

[11] The ADF submission also details the intended process for initial placements of civilians with cyber industry experience who seek to join the ADF. These *'alternate career entry'* applicants will have their skills and experience assessed by the Space and Cyber Career Management Directorate who will place them in the OAPS increment best aligned with their function, role and experience as described in the ADF Cyber Professional Framework.<sup>10</sup>

[12] The ADF submission seeks to implement the proposed pay structure with effect from 3 July 2025. This time imperative is driven firstly by the current high separation rate of experienced and talented personnel to industry and government agencies, which must be significantly reduced in order to grow cyber warfare capability. Secondly, service obligations related to relevant retention bonuses implemented in 2021 and 2022 have begun to expire, and this proposal provides further retention initiatives.

## Commonwealth

[13] The Commonwealth does not oppose the submission, recognising the *‘high priority of the matter, which seeks to develop a uniform approach to Cyber Warfare capability, a capability that is integral to each of the other warfighting domains, and necessary for the defence of national priorities as set out in the Defence Strategic Review 2023.’*<sup>11</sup>

[14] The Commonwealth also recognises the recruitment and retention issues faced in the workforce, noting *‘it is clear the ADF submission is appropriately justified, and delivers upon government direction on ADF capability’*.<sup>12</sup>

[15] The Commonwealth supports the proposal to implement the Transition Management Board to ensure no members are disadvantaged on transition into the OAPS.<sup>13</sup>

## Witness Evidence

[16] Major General (MAJGEN) R Watson, CSC, Commander, Cyber Command provided written and oral evidence in support of the proposal. He outlined the importance of cyber warfare in modern defence and the need for integration of cyber personnel, noting *‘the cyber domain touches every aspect of maritime, land, air and space. None of those domains can function without that critical support of, and reliance on, the cyber domain’*.<sup>14</sup>

[17] MAJGEN Watson acknowledged the type of people who excel in cyber roles are often drawn to the problem solving aspects inherent in technical cyber tasks, explaining staff are given *‘great problems to solve, but then we tell them the only way to increase your standing in this organisation, or enjoy greater remuneration, is to take on leadership and management responsibilities’* requiring a move away from the technical tools.<sup>15</sup> He elaborated *‘this submission today to the Tribunal is all about reflecting an emerging requirement’*, which is to offer a pay structure adequately acknowledging technical skillsets and providing a technical stream for advancement.<sup>16</sup>

[18] MAJGEN Watson gave evidence of the challenges for retention in the cyber warfare employment category, noting the high quality ADF training produces *‘some of the best cyber warfare or cyber security specialists in the country and they are in high demand...they can do a lot of these things elsewhere’*.<sup>17</sup>

[19] Colonel (COL) H Ashman CSM, Acting Commander, Cyber Forces Group, then gave oral evidence in addition to his affidavit provided in support of this matter. COL Ashman noted pay is not the only answer for recruitment and retention in this employment category, and stated *‘the value proposition of joining the ADF, the unique ability to do certain things, that idea of service to the nation is strong in the people who we do recruit. Retention in many ways relies on meeting some of those other expectations as well as the salary component’*.<sup>18</sup> He outlined what he perceived to be the benefits of the proposal, including offering opportunities for technical specialisation or promotion into leadership positions. He further noted the proposal is expected to assist with recruitment to these roles and *‘having the ability to continue to develop down a particular technical bent, to be able to become a true expert and share that knowledge amongst the community, without being detrimented or having a perception of detriment, is a key piece to that.’*<sup>19</sup>

## Consideration

[20] We accept this proposal has been made in the context of the recommended initiatives and control measures presented in the Deliberately Differentiated Package Research Report, the Cyber Workforce Action Plan, and the Cyber Professional Framework. We note this material's current assessment of the state of the cyberspace specialist workforce, and the justification presented for change, including delivery of competitive remuneration and the development of a technical career stream focussed on career and capability development.<sup>20</sup>

[21] We accept the submission that *'the need for the ADF to attract and retain its share of an in-demand and growing workforce in Australia requires a new, multi-faceted approach to Cyber Warfare employment'*.<sup>21</sup> We note the evidence of the attraction of industry salary, the need for salary progression in lieu of rank recognition, and the preference of highly skilled technical operatives to 'remain on the tools'.

[22] During the hearing we sought advice on aspects of lateral recruitment and the creation of a Cyber Reserve workforce. We accept the response that flexible and creative pathways are planned for both recruitment and retention issues, including recruitment of externally trained and experienced cyber specialists. We further note use of the OAPS will provide progression pathways in Command, Specialist and Staff structures and link remuneration points to times where members have developed significant technical experience and/or supervisory skills when they are most attractive to external options.

[23] We acknowledge the challenges of implementing an integrated ADF employment category through GOPS and GORPS and note this was considered as an option, however ultimately was not preferred due to its reliance on specific course completion for pay grade progression. We accept the submission that progression through GOPS and GORPS is problematic in the cyber workforce as *'it is counterproductive for the ADF and disenfranchising for the individual to maintain a requirement to learn a skill that is redundant'* and that *'Cyber Warfare employment categories would be better served within a skills-based pay structure, rather than a rank and competency-based structure of the graded pay structures'*.<sup>22</sup>

[24] In relation to use of the OAPS as the preferred model in this proposal, we are cognisant that whilst the OAPS provides the means to move entire employment categories into a single remuneration structure, that this will not be appropriate in many cases. We note our decision in the development of the OAPS in Matter 5 of 2016, wherein the Tribunal stated that the outcome is not to be used as a binding precedent, and persuasive justification needs to be presented on a case by case basis for any future relevant proposals.<sup>23</sup> We accept in this case the Cyber Warfare employment categories constitute a complex workforce which would benefit from the common pay structures available within the OAPS, and the ability to provide for annual pay increments to reflect accumulation of skills and experience over time.

[25] In doing so, we also refer to the transition of the Nuclear Submariner Workforce into the OAPS as determined in Matter 7 of 2024 and consider there may be a need to *'test and adjust'* the subsuming of the workforce into the OAPS with consideration *'given to workforce trends, attraction and retention data, transfers, and loss rates, all of which will combine to provide the workforce health, and identify areas likely to need further attention'*.<sup>24</sup>

## Conclusion

[26] In closing, we agree that the employment market for cyber workers is competitive, and in order to deliver on strategic recruitment and retention targets, the ADF must provide an employee value proposition attractive to workers who will excel in a Cyber Warfare employment category. We accept the proposal needs to go beyond remuneration reform.

[27] We agree that the creation of a uniform Cyber Warfare workforce through the OAPS is justified by the increased depth in knowledge, skills and experience this will offer members and the expected improvements to recruitment and retention.

[28] We accept the protocols to be followed for the initial transfer and placement of members into the OAPS, noting no member will experience a negative salary impact, and progression will be justified by the gaining competency stream, pathway or rank.<sup>25</sup>

[29] We note the ADF intends to provide us with a review of the implementation of these changes within two years of their commencement. Noting the criticality of this workforce, we ask them to report back to us at that time with a focus on workforce trends and the effect of the remuneration changes into the OAPS as indicated in paragraph 25 of this decision.

[30] We note our decision in this matter supersedes the final review report back requirement stated in Matter 3 of 2019 Joint Cyberspace Warfare Employment Categories.

[31] Determination 7 of 2025 gives effect to our decision from 3 July 2025.

MS B O'NEILL, PRESIDENT  
MS A LESTER, MEMBER  
MAJGEN G FOGARTY AO RETD, MEMBER

*Appearances:*

*Ms K Hagan for the ADF assisted by Flight Lieutenant L Hawkett*

*Mr K Wong for the Commonwealth assisted by Mr C Johnson*

*Witness:*

*Major General Robert Watson CSC, Commander, Cyber Command.*

*Colonel Hamish Ashman CSM, Acting Commander, Cyber Forces Group.*

---

<sup>1</sup> DMR BN97613083/2025 *Listing Application Cyber Warfare Employment Category* dated 12 March 2025

<sup>2</sup> [Navy: Cryptologic Sailors](#); DFRT Matter 12 of 2017

<sup>3</sup> [Joint Cyberspace Warfare Employment Categories](#); DFRT Matter 3 of 2019

<sup>4</sup> Chief of Defence Force Directive 15/2022

<sup>5</sup> [Defence Cyber Security Strategy | About | Defence](#)

<sup>6</sup> ADF Submission Matter 5 of 2025 *Joint Capabilities Group Cyber Warfare Employment Categories* dated 25 March 2025 (ADF 1) page 19 paragraphs 4.1-4.3

<sup>7</sup> ADF 1 pages 31-32, paragraph 5.14

<sup>8</sup> ADF1 page 53 paragraph 7.31

<sup>9</sup> ADF1 page 53 paragraph 7.32-7.34

<sup>10</sup> ADF1 page 54 paragraph 7.35

<sup>11</sup> Transcript Page 7 lines 3-7

<sup>12</sup> Transcript page 7 lines 9-10 and 25-26

<sup>13</sup> Commonwealth Submission Matter 5 of 2025 *Joint Capabilities Group Cyber Warfare Employment Categories* dated 1 April 2025 (Commonwealth 1) page 14 paragraph 51

<sup>14</sup> Transcript page 13 lines 40-43

<sup>15</sup> Transcript page 15 lines 28-31

<sup>16</sup> Transcript page 15 lines 26-38

<sup>17</sup> Transcript page 16 lines 6-7 and 16

<sup>18</sup> Transcript page 24 lines 7-8

<sup>19</sup> Transcript page 32 lines 37-40

<sup>20</sup> ADF 1 page 20 paragraphs 4.4 and 4.5

<sup>21</sup> ADF 1 page 27 paragraph 4.22

<sup>22</sup> ADF 1 page 28 paragraph 5.4

<sup>23</sup> [Air Force – Officer aviation pay structure](#); DFRT Matter 5 of 2016

<sup>24</sup> [Nuclear Submariner Workforce Tranche 1](#); DFRT Matter 7 of 2024

<sup>25</sup> ADF 1 page 47 paragraph 7.1-7.5