PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

DPS ref: D25/259669

Senator Karen Grogan
Chair
Finance and Public Administration Committee

By email: fpa.sen@aph.gov.au

Dear Chair

In advance of the Department of Parliamentary Services' (the department's) forthcoming attendance at the continued Senate Estimates Hearing of the Finance and Public Administration Committee (the Committee) meeting later today, I would like to provide the Committee with additional information about data searches authorised or undertaken by the department associated with the fact finding investigation undertaken in relation to the Incentive to Retire Payment (ITR) made to a former Deputy Secretary.

In previous evidence given to the Committee, and referenced in my letter dated 03 November 2025, I have confirmed that in addition to the investigation conducted by Dr Fiona Roughley SC into the ITR payment (the Roughley investigation), that there is a related investigation being conducted by the National Anti-Corruption Commission (NACC).

The department has consulted further with the NACC in advance of our attendance and notes that, consistent with advice from the NACC and previously confirmed to the Committee, that there will be matters that the department cannot respond to due to the ongoing NACC investigation. If this occurs, the department will advise the Committee that the question will be taken on notice to consider whether a Public Interest Immunity claim is required on the basis of the ongoing NACC investigation. Any questions from the Committee about the NACC investigation should be referred to the NACC.

I confirm that no Parliamentarian or Parliamentary data has been provided from the data searches to either Dr Fiona Roughley SC or the NACC in support of any investigation that has been, or is being, undertaken about the ITR payment.

Further, I confirm, that Dr Roughley's investigation was in relation to DPS actions and the involvement of DPS staff. There was no focus on Parliamentarians. DPS has seen no evidence, and Dr Roughley's full report contains no reference to, any engagement of any Parliamentarian in the ITR calculation and payment process.

I have noted concerns raised by the Committee about the cybersecurity status of one of the department's legal providers, HWLE Lawyers to hold DPS data.

Firstly, it is important to note that data obtained as a result of the data searches has not been held or stored on the IT network of HWLE Lawyers. The data was held by the forensic IT specialist under engagement with HWLE Lawyers, TransPerfect.

Secondly, I can confirm that HWLE Lawyers nevertheless had provided suitable cybersecurity and other assurances to facilitate the provision of information, with mechanisms and protocols established to manage data and any related sensitivities.

To provide additional confidence to the Committee, I am providing details of HWLE Lawyers cyber security and other data protective mechanisms (**Attachment A**).

I also note that department sourced the services of HWLE Lawyers from Legal Services Panel managed by the Attorney-General's Department. I understand that the Attorney-General's Department engaged with HWLE about data protection and cyber security matters at the time of the last panel review process and were satisfied that HWLE met the security requirements necessary to secure reappointment to the panel.

The Legal Services Panel is a long-standing whole of government arrangement and is mandated for use by all non-corporate Commonwealth entities, including the department. A range of legal services are covered by the Panel arrangement, including Area of Law 1 – Workplace, Industrial Relations and Compensation.

The Attorney-General's Department's most recent approach to market to re-establish the Panel resulted in the current standing offer arrangement from 1 July 2024 to 30 June 2027. HWLE has a deed of standing offer under the current Panel arrangement for all areas of law covered by the arrangement and also had a deed of standing offer for all areas of law under the previous version of the Panel. A requirement of appointment to the Legal Service Panel is execution of the panel Head Agreement, including compliance with the Security clauses (clause 23 and its subclauses).

Of note, this includes:

- Compliance with security requirements specified in the PSPF (clause 23.1.1)
- Implementation of security procedures to ensure it meets obligations under clause 23 (clause 23.1.2)
- Restriction of access to and protection of Commonwealth Entity Material, Contract Material, Confidential Information or Personal Information (clause 23.2.1)
- reasonable efforts to detect, prevent and appropriately respond to the introduction of any Harmful Code into its systems (clause 23.3.1)
- reasonable efforts to detect, prevent and respond to any Cyber Security Incident or Cyber Security Event (clause 23.4)

HWLE has provided the required Data Security and Cyber Security plans to AGD that are compliant with the Head Agreement requirements. Further, HWLE's subcontractors are

bound by, and HWLE is required to ensure they comply with, a number of provisions to the Head Agreement, including clause 23 (Security).

I also note that HWLE Lawyers has provided outstanding support to DPS during Dr Roughley's investigation and in the department's engagement with other agencies, including the NACC.

To assist the Committee in their considerations, I provide the following technical overview about how data search activities, conducted by TransPerfect, are undertaken:

1. Logging into the M365 eDiscovery tool to prepare and export the specified evidence items. This includes search criteria of identified usernames against a specified date range. The data is then extracted in a bulk file or files.

2. The bulk files exported are copied to an encrypted USB hard drive and taken by safe hand to the forensic lab for processing.

3. Data is then transferred onto two encrypted drives and stored securely in the TP Sydney Forensic Lab safe, which is separately locked within the forensic lab.

4. Identified evidence items are transferred into the forensic eDiscovery tool where granular search filters only information directly relevant to the investigation.

5. Authorised HWLE lawyers are then granted access to the filtered information.

Only data that meets specific search criteria in the forensic eDiscovery tool is ever viewed. All other data is never used, viewed, or interacted with.

I can assure the Committee that the data forensic interrogation has only been undertaken in order to identify only that material relevant to the ITR calculation and payment and / or the involvement of identified public officials in the same. There was, and there remains, no focus on Parliamentarians.

Finally, I wish to assure the Committee that the department takes seriously the integrity of this process, against the background of the completion of Dr Roughley's fact-finding investigation, the related NACC investigation and separate considerations relevant to the DPS officers.

As I indicated in my opening statement of 31 October 2025, to facilitate a thorough investigation, which was to examine the role of DPS in the ITR payment and calculation process, Dr Roughley required access to DPS information and data about departmental employees.

Internal data searches were initially conducted by staff of the DPS ICT Division. These data searches were undertaken across the APH network, not limited to DPS staff and conducted in a timeframe that impacted the finalisation and delivery of Dr Roughley's report.

DPS confirms again that no Parliamentarian or Parliamentary data was provided to HWLE Lawyers and Dr Roughley from the internally conducted DPS searches. However, there were concerns that relevant data from the internally conducted searches had been intentionally filtered out, excluded or not provided.

On 28 October 2024, Dr Roughley wrote to me to express her concern that the data provided to her was not complete and that there were, in her words, "*surprising gaps in the documentary material that has been made available*". Dr Roughley recommended that DPS consider engaging an independent external expert to undertake further data extraction to ensure that all potentially relevant material is provided and that the forensic integrity of such material is maintained.

As a result of concerns raised by Dr Roughley, the NACC and senior DPS staff, I authorised on 30 October 2024, a TransPerfect representative to extract the employee data of identified DPS employees for searches to be conducted for relevant material for Dr Roughley's investigation.

To summarise the data collection process undertaken for the completion of the Roughley fact-finding investigation:

- On 21 June 2024, a request for a search to be conducted was made by a DPS Assistant Secretary. The then DPS Chief Information Officer asked me to authorise an internal DPS search to be conducted on the department's internal record keeping facility (Content Manager), to which I provided authorisation. Despite this authorisation, an APH systems wide search was undertaken by DPS ICT. Data returned totalled 299.70 MB of data, comprising emails and Microsoft Teams messages. No Parliamentarian or Parliamentary data was provided to HWLE Lawyers as part of this search. The data search took twenty-four days to complete.

- On 22 August, I authorised a data extraction to be undertaken on a small number of DPS employees for the date range between 1 February 2023 and 30 November 2023. After discussion with the then DPS Chief Information Officer, including in relation to a draft risk assessment he provided me, I subsequently authorised the data search to be separated into two parts with a full data extraction authorised for some DPS employees, and for DPS ICT to conduct the proposed searches on the remaining DPS employees. This resulted in a data return of 32.63 GB of date comprising emails and Microsoft Teams messages. No Parliamentarian or Parliamentary data was provided to HWLE Lawyers as part of this search.

- Finally, on 30 October, I authorised TransPerfect to attend the departmental premises to undertake a bulk extract process of material held by a number of DPS employees for the date range 1 February 2023 to 30 November 2023 and for searches against nominated search terms required by Dr Roughley. This resulted in

a data return of 136.95 GB comprising emails and Microsoft Teams messages and took two days to complete.

It is not acceptable that the first two internal data searches included searches across the APH network. The internal handling, by DPS staff, of the initial data retrieval process has been subject to independent investigation and are now resolved. In the context of an Estimates hearing, it would be inappropriate for the department to comment on the details of these investigations. However, I would be comfortable to outline the outcome of the investigations with the Committee.

I note the Committee's interest in the search terms used in the completion of the data searches. I am seeking advice from the NACC on whether the provision of these search terms would unreasonably prejudice their ongoing investigation. If the NACC indicates that it would, I will consider the need to make a public interest immunity claim in relation to those search terms.

Finally, following consultation with the NACC, I can confirm that similar data searches were undertaken by TransPerfect in accordance with a NACC notice to produce, and can also confirm that the searches were limited to DPS staff (not Parliamentarians or Parliamentary data). I also confirm that the NACC did not want DPS ICT staff to undertake the required searches. We will be unable to respond to any further questions about data searches undertaken for the NACC. Questions on this matter should be referred to the NACC.

I trust that this information is of assistance to the Committee and confirm that that I, and members of the department's Executive, will continue to openly and transparently respond to questions asked at the forthcoming Estimates hearing, within the bounds of the current NACC investigation.

I look forward to discussing these issues with the Committee.

Yours sincerely

Jaala Hinchliffe
Secretary

04 November 2025

HWLE LAWYERS

HWL EBSWORTH DATA SECURITY MEASURES STATEMENT

NOVEMBER 2025

Commercial-in-confidence

HWL EBSWORTH INFORMATION SECURITY SUMMARY

Information Security Practices

HWLE has a detailed Information Security Management System (ISMS) which operates as the firm's framework for managing information security. The ISMS covers information classification, appropriate data handling and usage, roles and responsibilities, acceptable use of IT, access control, business continuity, disaster recovery, people security, logging, monitoring, security incident response, cryptography and key management, malware prevention, risk assessments, network security, records management, system development lifecycle physical security, third-party security, controls testing, vulnerability management, policy enforcement, and handling of exceptions.

Information Security Governance Structure

HWLE has a dedicated information security team that manages the Firm's information assets and systems, as well as those of clients. The National Information Security Manager, who reports to the Chief Information Officer (CIO), is responsible for risk management, governance, compliance, and cyber operations.

The Information Security Team is supported by external service providers to deliver continuous 24*7*365 managed detection and response (EDR and SIEM/SOC), Privileged Access Management and third-party patching.

An information security committee chaired by the Chief Executive Officer oversees these efforts and submits reports on information security matters to the Board.

Information Security Assurance

The Firm holds a current ISO 27001:2022 certification. This is an international standard to manage information security that is published jointly by the International Organization for Standardization and the International Electrotechnical Commission (IEC). This certification standard requires 114 prescribed controls and measures which support our information security management system.

These controls are divided across 14 security fields which are:

a) Information security policies;

b) Organisation of information security;

c) Human resource security;

d) Asset management;

e) Access control;

f) Cryptography;

g) Physical and environment security;

h) Operations security;

i) Communications security;

j) System acquisition, development and maintenance;

k) Supplier relationships;

l) Information security incident management;

m) Information security aspects of business continuity management; and

n) Compliance.

To obtain ISO 27001 certification, HWL Ebsworth was required to establish that it had appropriate procedures and controls in each of the above fields.

External ISO 27001 audits are conducted annually by independent certification auditors, alternating between certification and surveillance audits each year. Internal audits are performed biannually by BluePrint (Cyber security professional services firm). The firm has implemented a first line assurance control testing to assess the adequacy and effectiveness of security controls which are reported to the Information Security Committee.

The firm engages an independent firm to undertake internal and external penetration testing on an annual basis. The most recent penetration test occurred in October 2025 with the outcome that privilege escalation attempts were not successful.

HWLE has been externally assessed as having an overall Essential Eight maturity level of Maturity Level Two. HWLE complies with at least Maturity Level Two on all Essential Eight mitigation strategies, and on most mitigation strategies complies with Maturity Level Three. Maturity Level Two is consistent with the maturity level mandated for Commonwealth Government entities.

HWLE is also accredited under the Defence Industry Security Program at the following levels - Level 2 Governance, Level 2 Personnel, Entry Level Physical and Entry Level Information and Cyber, meaning all offices can access, handle and store documentation/information at the OFFICIAL: SENSITIVE level.

Cyber Operations

Technical cyber operations controls include: 24x7x365 security operations monitoring, security information and event management, endpoint detection & response, vulnerability scanning, annual penetration testing, privileged access management, access control, multifactor authentication, threat intelligence, patch management, encryption, email security, application control, network segmentation, data loss prevention, and dark web monitoring.