PARLIAMENT OF AUSTRALIA

DEPARTMENT OF PARLIAMENTARY SERVICES

Submission to the Senate Standing Committee of Privileges

23 January 2026

Contents

Acronyms and Abbreviations

AFP	Australian Federal Police
APH	Australian Parliament House
APS	Australian Public Service
APSC	Australian Public Service Commission
CCTV	Closed Circuit Television
CIO	Chief Information Officer
CM	Content Manager (DPS official record keeping management system)
Code	Code of Conduct
Commissioner	Commissioner of the National Anti-Corruption Commission
CoP	Code of Practice
Cth	Commonwealth
The department/ DPS	The Department of Parliamentary Services
EACS	Electronic Access Control System
FPA Committee	Senate Standing Committee on Finance and Public Administration
HWLE	HWL Ebsworth Lawyers
ICT	Information and communication technology
ISD	Information Services Division
ISM	Information Security Manual
ITR	Incentive to Retire
Microsoft 365	Microsoft cloud-based productivity suite (previously called Office 365 of O365)
MoU	Memorandum of Understanding

NACC	National Anti-Corruption Commission
NACC Act	*National Anti-Corruption Commission Act 2022*
NV1	AGSVA Negative Vetting Level 1 (NV1) clearance
MOU	Memorandum of Understanding
PCN	Parliamentary Computing Network
The Precincts Act	*Parliamentary Precincts Act 1988*
Presiding Officers	The President of the Senate and the Speaker of the House of Representatives
The Privileges Act	*Parliamentary Privileges Act 1987*
PS Act	*Parliamentary Services Act 1999*
SCEC	Security Construction and Equipment Committee
Secretary	References to the Secretary in this submission refer to the current Secretary (Ms Jaala Hinchcliffe) of the department whilst in previous roles including Deputy Secretary and Acting Secretary.
SES	Senior Executive Service
SMB	Security Management Board
TPL	TransPerfect Legal

Introduction

The Department of Parliamentary Services (DPS/the department) welcomes the opportunity to provide this submission to the Senate Standing Committee of Privileges (Privileges Committee), in reference to the Senate's referral of 25 November 2025 inquiring into the *Department of Parliamentary Services handling of documents and communications*.

The department is one of four Parliamentary departments established under the *Parliamentary Service Act 1999* (PS Act) that collectively serves the Parliament by providing professional support, advice and facilities to each house of Parliament, to parliamentary committees and to Senators and Members, independent of the Executive Government of the Commonwealth.

The key strategic purpose of DPS, as outlined in the Corporate Plan 2025-2026, is to support the functioning of the Parliament, facilitate community access to Australian Parliament House (APH) and the parliamentary process, and the stewardship of APH.

Delivering on our purpose relies on the commitment, professionalism, judgement, and expertise of our staff. The department's unique operating environment requires a strong focus on the Parliamentary Service Values, service delivery, integrity, stakeholder feedback and continuous improvement enabling it to effectively deliver its activities for the more than 12,000 APH passholders and screening of 1.6 million people to enter APH each year.

Over the past eighteen months the department has been subject to significant scrutiny. Operational, service delivery, integrity and cultural issues have been identified that have warranted our close and ongoing attention.

On 17 December 2024, the President of the Senate and the Speaker of the House of Representatives (the Presiding Officers) terminated under section 61 of the PS Act, the appointment of the former Secretary, Mr Rob Stefanic, due to a loss of trust and confidence.

Ms Jaala Hinchcliffe was appointed acting Secretary on 4 October 2024,[1] and following a competitive merit-based recruitment process, was formally appointed by the Presiding Officers as DPS Secretary on 11 March 2025 (for a five-year term).

The Secretary is an experienced public sector leader with a background in complex legislative, compliance and integrity issues. The Secretary's previous roles include Deputy Commissioner of the National Anti-Corruption Commission (NACC), Integrity Commissioner (agency head) of the Australian Commission for Law Enforcement Integrity and Deputy Commonwealth Ombudsman. Prior to her senior executive roles, the Secretary had an extensive career as a lawyer specialising in Commonwealth criminal law with the Commonwealth Director of Public Prosecutions.

Since her appointment as Secretary, efforts have been directed towards enhancing transparency with the Presiding Officers, the Parliament, Parliamentarians, Parliamentary Department colleagues and the wider community about matters within her responsibilities.

[1] *Note: References to the Secretary in this submission refer to the current Secretary (Ms Jaala Hinchcliffe) of the department whilst in previous roles including Deputy Secretary and Acting Secretary.*

While both the Secretary and DPS' leadership team acknowledge that further improvement is required, significant progress was achieved through 2025, including:

- supporting the commencement of the 48th Parliament
- transitioning to a new telephony platform and rollout of a new Information and Communications Technology (ICT) Allocations Policy supporting Parliamentarians and their staff
- security screening of over 1.6 million people entering APH and maintaining the physical security of APH
- broadcasting more than 976 hours of parliamentary proceedings
- completing seven capital works projects
- planting over 4,700 new plants in the APH gardens and courtyards
- responding to over 6,000 property maintenance requests
- facilitating over 8,000 deliveries at the APH loading dock
- supporting ICT operations, including over 43,600 telephone calls received via the ICT service desk and supporting the operations of more than 4,300 people on the Parliamentary Computing Network (PCN)
- facilitating over 3,000 school tours for more than 114,000 school children and their teachers and educators
- completing over 8,300 client requests received by the Parliamentary Library
- delivering over 30 public programs and performances at APH; and
- facilitating over 380 events in APH venues.

In recognition of the essential role the department plays in delivering impartial, efficient and effective services we are focused not only on ***what*** we do as a service delivery agency, but ***how*** we do it.

Since the Secretary's commencement, the department has a renewed focus on service delivery in alignment with the Parliamentary Service Values. At the commencement of 2026, all Senior Executive Service (SES) leadership roles are substantively filled for the first time in many years. The SES leadership team is highly experienced with expansive and diverse career knowledge gained across the Australian Public Service (APS).

Having a stable leadership team in place allows the department to focus on the six priorities the Secretary has set for the department:

- Embedding our values and behaviours even further into our work
- Improved governance through reviewing our legislative, regulatory, compliance and policy obligations
- Establishing and maintaining relationships with the 48th Parliament
- Delivering sustainable, efficient, timely services that meet best practice
- Demonstrating financial sustainability and capability, and
- Deepening partnerships with key stakeholders and clients.

The Secretary, the department's leadership and staff have actively engaged in a process of reflection and adaptation and have responded constructively to issues and challenges. This collective effort has strengthened collaboration and unity across the department, lessening siloed based work practices and addressing the previous 'delivery at any cost' approach.

These efforts have been reflected in DPS' 2025 APS Employee Census results. Between the 2024 DPS Staff Survey and the 2025 APS Employee Census, there have been notable improvements in culture, goals, innovation and direction. The recommendation of DPS as being a good place to work increased by 6% (to 68%). Furthermore, 63% of staff (an increase of 7% on the previous year) believe that over the 12 months, DPS has moved in the right direction to meet its goals and improve as an organisation. These results highlight the efforts made over the year to enhance the department's culture and work practices. Additional information about DPS' results in the 2025 APS Employee Census, including our 2025 Action Plan, is available at APS Census – Parliament of Australia.

While it is important to acknowledge, promote and celebrate the progress made, the department recognises that further work remains. Accordingly, this submission demonstrates the department's strong commitment to addressing challenges identified in DPS' 2025 APS Employee Census results and driving future advancements in service delivery for the Parliament, Parliamentarians, Parliamentary Department colleagues and all who work and visit APH.

To support this submission, the department has provided (as attachments), supporting material including responses to questions taken on notice and/or written and directed to the department, through the Senate Standing Committee on Finance and Public Administration (FPA Committee) Estimates process, and Opening Statements made by the DPS Secretary to these hearings.

Background

Incentive to Retire Payment to former DPS Deputy Secretary

It is important to provide the Privileges Committee with context as to the origins of the concerns that have led to the establishment of its inquiry into the department's handling of documents and communications.

On 13 October 2023, an Incentive to Retire (ITR) payment was made to a former DPS Deputy Secretary. In early 2024, media reports and parliamentary scrutiny led to questions relating to this payment.

In June 2024, formal concerns were raised with the Secretary by a DPS staff member about the ITR, including whether the department had followed correct processes about its payment. As information available to the Secretary did not allow her to determine whether the correct process had been followed, and given the seriousness of the concerns raised, the Secretary considered it necessary to engage an independent investigator to consider the matter.

On 11 July 2024, the department engaged Dr Fiona Roughley (SC) as the independent external investigator, supported by Junior Counsel, Mr Christopher Tran.

Engagement with the National Anti-Corruption Commission

ITR payment

It has been publicly acknowledged that the National Anti-Corruption Commission (NACC) is undertaking an investigation related to the payment of the ITR to a former Deputy Secretary. This investigation remains ongoing. Any matters relating to the NACC investigation must be referred to the NACC.

DPS has however sought the agreement of the NACC to provide the following information as it is relevant to considerations of DPS, and the fact-finding investigation undertaken by Dr Roughley.

On 24 July 2024, the Secretary wrote to the Commissioner of the NACC (the Commissioner) advising that Dr Roughley had been engaged to undertake the ITR investigation. The Secretary noted that while she had not yet reached the threshold of suspecting that the issue involved serious or systemic corrupt conduct, if Dr Roughley's investigation identified information that raised such a suspicion, that the NACC would be notified.

On 5 August 2024, the Commissioner responded, noting that he was considering issuing either a 'stop direction' in relation to Dr Roughley's investigation or considering whether a joint investigation could be undertaken by the NACC and DPS. After a period of consultation, a joint investigation between the NACC and DPS was agreed. The joint investigation commenced on 6 September 2024.

On 2 October 2024, the Secretary received a letter from the Commissioner (dated 1 October 2024), which set out an expansion of the NACC's investigation and noted that some practical issues had been identified with a joint investigation approach. As a result, the Secretary was advised that the Commissioner had decided to terminate the joint investigation but noted that a stop direction over the whole of the investigation being conducted by Dr Roughley would not be necessary, i.e. that DPS could continue its investigation, at least in part, while the NACC investigation concurrently occurred.

Also on 2 October 2024, the NACC informed the Secretary that it intended to execute warrants on DPS on 3 October 2024. The Secretary sought confirmation from the NACC that the Clerks and Presiding Officers had been advised, which she was advised they had been. On 3 October 2024, the NACC executed search warrants on DPS.

On 17 December 2024, the Commissioner issued a stop direction under section 43 of the *National Anti-Corruption Commission Act 2022* (Cth) (NACC Act) to stop a small number of people being interviewed as part of Dr Roughley's investigation. The letter also noted that this direction did not preclude Dr Roughley from finalising her report.

The NACC has also been provided with DPS employee information relevant to the payment of the ITR, pursuant to a compulsory notice to produce issued by the NACC. Ultimately, this information was extracted on behalf of DPS by TransPerfect Legal (TPL) and is canvassed later in this submission.

HWL Ebsworth Lawyers (HWLE) have supported the department in its engagement with the NACC, compliance with its notices to produce and search warrants, in addition to support provided to Dr Roughley's fact-finding investigation.

Further non-DPS employee investigation

In addition to the publicly confirmed NACC investigation into issues related to the payment of the ITR to a former DPS Deputy Secretary, the department confirms that a TPL forensic specialist was authorised to attend APH between 19-21 and 24 March 2025 to undertake a data extraction process to facilitate DPS' compliance with a NACC notice to produce unrelated to DPS employees. This occurred following concerns about the adequacy of searches and completeness of material provided by DPS in response to the NACC notice to produce.

Any matters relating to the NACC investigation must be referred to the NACC.

Fact-finding investigation – Dr Fiona Roughley SC

Dr Roughley's investigation was commissioned to examine the processes that led to the ITR payment being made, including:

- The role of DPS in the ITR payment process
- If the processes followed by DPS were appropriate
- If the amount of the ITR payment was calculated correctly and was appropriate in the circumstances

- Any conduct by DPS officials that might be the subject of a referral for further investigation or other action, and
- Recommendations to DPS on its processes and, if the investigation concludes that processes followed were not appropriate, any recommended actions as a result of that finding.

The agreed date for the provision of Dr Roughley's initial report of the results of the investigation, including any recommendations for early consideration, was September 2024. However, due to significant delays relating to the provision of information sourced from data searches (canvassed later in this submission), Dr Roughley's report was not provided to the department until 12 March 2025.

Engagement of HWLE Lawyers and TransPerfect Legal

To assist Dr Roughley in the independent investigation, HWLE received instruction from DPS to provide support. Through the mandated whole of government panel arrangement for legal services (managed by the Attorney-General's Department), DPS had an established legal services work order in place with HWLE (and a number of other providers).

A copy of the head agreement under the legal services panel is available at: Head Agreement (www.ag.gov.au/sites/default.files/2025-04/head-agreement-template-2025.pdf)

More information about the panel is at: Purchasing legal services | Attorney-General's Department.

Among other obligations established under the Head Agreement, HWLE Lawyers is required to:

- *not subcontract on terms that would permit the subcontractor to do something that would constitute a breach of the Head Agreement or a Contract (clause 6.3.1(b))*
- *ensure any subcontractor/s (if used) complies with relevant clauses from the Head Agreement, including clauses about confidentiality, security and privacy (clause 6.3.1(d)), and*
- *advise the Attorney-General's Department and DPS if their subcontractor breaches certain obligations under the Head Agreement (clauses 23.1.3 and 24.1.5).*

HWLE had established contractual arrangements with TPL for specialised e-discovery and electronic forensics. These contractual arrangements included, among other things, confidentiality obligations over all materials, data or information received by TPL.

In the event that TPL acted in an inappropriate manner, did not comply with directions from HWLE or the department, or with HWLE obligations under their contract with the department, the department would have the right to terminate the contract or reduce the scope of services.

It is important to highlight that at all times DPS retained and did not waive ownership of its data held by TPL on its behalf.

Information required to support Dr Roughley

To enable Dr Roughley to undertake an objective and comprehensive investigation into the ITR payment, access to emails, decisions, teams messages and other information from DPS employees involved in the ITR payment contained on DPS ICT networks was necessary. The required information specifically related to DPS employees, and not that of parliamentarians or their staff.

Authorisations were made by the Secretary on 21 June 2024 and 22 August 2024 to the then DPS Chief Information Officer (CIO) to conduct searches for the required DPS information. Significant deviations from the authorisations have subsequently been identified.

As noted in the response to Supplementary Budget Estimates 2025-2026 FPA Committee Question on Notice 79 (**Attachment A**), DPS is now aware that 22 individual variations of data searches and four duplicated searches, across the PCN (which included Parliamentarians and their staff) were performed by DPS Information Service Division (ISD) staff.

DPS has acknowledged that these data searches were inappropriate and not in accordance with authorisations provided. The internal management by some ISD staff relating to this matter has been subject to independent investigation and is canvassed later in this submission.

Following concerns raised with DPS on behalf of Dr Roughley that there were deficiencies in the employee data provided in response to the Authorisation of 21 June 2024, a second Authorisation was provided by the Secretary to the then CIO. On 28 October 2024, Dr Roughley wrote to the department to raise concerns about the data provided in response to the second authorisation and, as a result, a subsequent third Authorisation using an external third party – TPL was approved by the Secretary.

DPS notes that the use of third-party data forensic firms to undertake data extractions of this nature is not unusual in integrity or other investigations.

Details of the three Authorisations are outlined below and summarised in the Secretary's Opening Statement and letter to the FPA Committee provided at **Attachment B**.

Authorisation one: 21 June 2024

On 21 June 2024, a DPS Assistant Secretary requested the then CIO to conduct a data search for records relating to the ITR payment to the former DPS Deputy Secretary, which included search terms, for an independent DPS investigation. On receiving the request, the then CIO requested an Authorisation from the Secretary to search the department's internal record keeping facility Content Manager (CM). The Secretary provided the Authorisation for a search of CM on 21 June 2024, and a copy of this Authorisation is at **Attachment C.**

CM is a system used by DPS, that meets the record keeping requirements of the National Archives of Australia. Parliamentarians do not have access to, nor store their information, in this system.

Despite the Secretary's explicit authorisation to conduct a CM search, and a request from the DPS Assistant Secretary to undertake a 'DPS system wide search', officers of ISD used the search terms provided to search across all exchange locations, including the accounts of Parliamentarians and their staff.

The department acknowledges that it is not acceptable that the internal data searches included searches across all exchange locations on the PCN. The internal management by some ISD staff of this matter has been subject to independent investigation and is canvassed later in this submission. Data obtained by ISD was internally filtered and reviewed prior to being provided to TPL (concerns raised about this filtering is canvassed later in this submission).

Completion of the return of the DPS employee data requested by the Assistant Secretary in Authorisation One took 24 days to complete and resulted in a data return of 299.7MB.

Following consultation between ISD and TPL, the transfer of DPS employee data to TPL occurred through a DPS password protected Microsoft Azure storage container, where information would subsequently be made available to HWLE through the TPL proprietary system (Relativity). No concerns were raised by ISD staff about transferring DPS employee data in this manner. No Parliamentarian or Parliamentary data was provided to HWLE Lawyers as part of this search.

Authorisation two: 22 August 2024

In August 2024, concerns were relayed from Dr Roughley to the Secretary that potentially relevant material had been excluded during the first data extraction process. Further, the Secretary was advised that the extraction process also appeared to have impacted the metadata of tranches of the DPS data, significantly limiting the effectiveness of forensic tools that could potentially be deployed.

In light of the concerns raised, the Secretary provided a further Authorisation to the then CIO to provide data extractions of DPS employee data, relating to eight DPS employees, within specific parameters, to ensure that all relevant material was collected. A copy of this Authorisation is at **Attachment D.**

Before the data was extracted in accordance with the Authorisation, and despite the earlier provision of data to TPL by ISD, the then CIO raised concerns about bulk data being extracted. The Secretary agreed to the then CIO's request for a meeting to discuss their concerns and a meeting was scheduled for 5 September 2024.

Prior to this meeting a draft cybersecurity risk assessment was emailed to the Secretary by the then CIO on 4 September 2024. A copy of the draft risk assessment is provided at **Attachment E** and DPS' responses to questions on notice about the risk assessment is provided at **Attachment F.**

When reviewing the draft risk assessment, the Secretary observed that there was insufficient consideration of established control measures and the reduced risk resulting from the implementation of supplementary treatments and assurances.

The Secretary's view was based on the following:

- The data extraction occurring on the APH unclassified network only. Therefore, as national security and/or other classified information (as noted in the assessment) is not permitted on the APH network, it would not be included in the searches.
- That too much emphasis was placed on information being held or hosted on or by networks operated by HWLE, when it had been made clear to representatives of ISD that data would be held/managed on Australian-based secure servers operated by TPL.
- That the consequence rating of the "total loss/corruption of critical information" was an impossible consequence as only copies of relevant DPS staff data was being extracted.
- That the likelihood ratings were not 'LIKELY', but 'POSSIBLE' (before the application of treatments); and that
- The draft risk assessment did not reflect the processes which had been put in place to protect any material that might contain parliamentary privilege from being provided to Dr Roughley.

The Secretary discussed the draft risk assessment with the then CIO in their meeting of 5 September 2024. In that discussion, the Secretary and the then CIO agreed to amend the requested searches by splitting it into two parts:

- The data in relation to two DPS employees to be extracted in bulk (by ISD) for it to then be searched outside of the system using TPL's forensic tools; and
- That ISD staff would conduct searches on the data of the other six identified DPS employees, review for material that may be sensitive or include correspondence from or to parliamentarians and/or their staff, with relevant data then provided to TPL.

Following the discussion on 5 September 2024 between the Secretary and the then CIO the original draft risk assessment rating was, in the Secretary's view, lowered. This view was confirmed in the mind of the Secretary by the fact that ISD provided TPL with the bulk extracted data for two DPS employees on 9 September 2024 and data sets for the remaining six DPS employees on 12 and 13 September 2024. Further, the draft risk assessment was not provided in final form or raised again with the Secretary.

The Authorisation provided by the Secretary to the then CIO and the discussion between the Secretary and the then CIO on 5 September 2024 clearly related only to the mailboxes and Microsoft 365 logs belonging to eight DPS employees. Despite this, officers of ISD searched across all exchange locations on the PCN which included the accounts of Parliamentarians and their staff.

The department again acknowledges that it is not acceptable that the internal data searches conducted by ISD included searches all exchange locations on the PCN. The internal management by some ISD staff of this matter has been subject to independent investigation and is canvassed later in this submission.

The data search conducted under Authorisation two resulted in a data return of 32.63GB of data comprising emails and Microsoft Teams messages and took 22 days to complete. No Parliamentarian or Parliamentary data was provided to HWLE Lawyers as part of this search.

Engagement between technical teams

DPS representatives from ISD (including the then CIO) and the Corporate Services Division collaborated with TPL on several occasions (collectively and/or individually) throughout the progression of Authorisation one and Authorisation two.

This included by email, meetings, teleconferences, videoconferences, on-site collaboration and supervision during the data extraction process. Collaboration also included the establishment of a standing arrangement for ISD to directly contact technical experts at TPL at any point during the investigation to confirm any questions, send data volumes and/or for DPS to send security questions for TPL to answer. There is no record of further engagement between ISD and TPL regarding concerns.

Collaboration dates included, but may not be limited to - 5 July 2024, 15 July 2024, 16 July 2024,1 August 2024, 22 August 2024, 30 October 2024, 31 October 2024 and 1 November 2024.

Authorisation three: 30 October 2024.

In correspondence dated 28 October 2024, Dr Roughley wrote to the Secretary raising serious concerns about the information provided:

> "*...that the data provided to me has not been nearly as complete as I would have expected and there were surprising gaps in the documentary material that has been made available...".*

Dr Roughley also noted:

> "*I continue to hold concerns that relevant material may not have been provided. I also have concerns with production of some relevant material in a way that does not provide the metadata and may obscure relevant information such as recipient details and the broader context in which an email was sent or received*".

As a result, in her correspondence, Dr Roughley recommended that the department:

> *"...consider engaging an independent external expert to undertake further data extraction. That expert should be asked to confirm at the conclusion of the process that the data has been extracted in full and without interference. I make this recommendation to ensure that all potentially relevant material is provided, and that the forensic integrity of such material is maintained".*

On 30 October 2024, the Secretary provided a verbal authorisation for a TPL data forensic expert to extract the following material to assist in Dr Roughley's investigation:

> In relation to eight named DPS employees:
> - all emails and Microsoft 365 logs
> - for the period between 1 February 2023 and 30 November 2023

The extracted material was then scanned by TPL using specialised digital search software with key word based 'search strings' to identify information relevant to the investigation. The data returned via the searches was transferred into a secure digital review program (Relativity) hosted by TPL with access given to HWLE.

HWLE then reviewed the data returned from the forensic search to create a subset of material to be provided to Dr Roughley. This included a review for any material to which parliamentary privilege might apply.

The subset of material was provided to Dr Roughley via the secure digital review program hosted by TPL (Relativity).

The Secretary conveyed her authorisation for the TPL data forensic expert to conduct the extract to the then CIO in a discussion on 30 October 2024, which was followed by an email containing a direction on the support to be given to TPL to undertake the extraction, including:

- *"Provide TPL with full system administrator access to DPS systems, servers and data*
- *Instruct the relevant DPS staff member with working knowledge of the DPS systems, servers and data to assist TPL in the extraction*
- *Not impede the work of TPL; and*
- *To follow all lawful and reasonable directions given to him by TPL"*.

A copy of this direction is provided at **Attachment G**.

The then CIO confirmed receipt of the direction and advised that he had put in place the following treatments and assurances to deal with any potential risks:

- *"the department's Chief Enterprise Architect will personally support the extraction of data"*
- *"The Director, Cyber Security Operations Centre, will also observe the extraction of data as an independent witness to provide assurance that data extraction is within the scope of the investigation and doesn't otherwise compromise the effective operation of parliament"*.
- *"appropriate action will be taken in the very unlikely event that actions pose a significant Cyber Security or operational risk to the effective operation of Parliament. I expect this will be unnecessary, but I think it's prudent to have a clear plan of action in place"*.

TPL attended APH on 31 October and 1 November 2024 and completed the authorised data extractions. The material extracted related to eight DPS employees for the date range of 1 February to 30 November 2023.

The data return was 136.95GB and took two days to complete.

The NACC was informed that a third party would undertake this further data extraction, following concerns about previous data extraction processes undertaken by officers of ISD.

Return of employee information to APH

On 4 November 2025 the Presiding Officers requested the data held by TPL be returned to APH. A process of return was agreed by the Clerk of the Senate and the Clerk of the House of Representatives **(Attachment H).**

The data was returned to APH in accordance with this procedure on 27 November 2025. The data is now securely stored on an encrypted external hard drive held in a Security Construction and Equipment Committee (SCEC) accredited Class C container within APH. Access to the safe is only available to the Secretary and Deputy Secretary. All other actions associated with the data return procedure have been completed and advised to the Presiding Officers.

Dr Roughley's report – key findings and recommendations

Dr Roughley provided her final report to DPS on 12 March 2025.

Public interest continued in relation to the ITR payment and Dr Roughley's report. In order not to prejudice the NACC's ongoing investigation, but to ensure transparency and accountability, a summary report was prepared and agreed with the NACC.

On 16 October 2025, the summary of Dr Roughley's report was provided to the FPA Committee and published on the APH website (**Attachment I**).

Key findings of Dr Roughley's report were:

- There were conflicts of interest, and conflicted persons, within DPS, involved in the decision-making process.
- There were multiple procedural failures by DPS, or informed by DPS, in relation to the calculation of the ITR payment.
- The payment deviated from the Australian Public Service Commission (APSC) guidance material in its calculation, which resulted in an increase in the quantum of the payment made.

Additional concerns expressed by Dr Roughley relating to aspects of the process included:

- Errors identified in the calculation of the payment,
- The exclusion and/or lack of involvement and/or disregard for the advice of specialist DPS Payroll staff, and
- Excessive pressure applied on the timing of the payment.

Dr Roughley's report contained seven recommendations regarding the management of conflicts of interest and DPS process for ITR payments. All recommendations were directed only to DPS.

Dr Roughley's recommendations were that:

- Guidelines should be promulgated about how a decision to make an ITR payment offer will generally be made, including indicative factors that may be relevant to that decision and to the quantification of the amount to be paid.
- Offers of ITR payments should usually only be made in a specified amount or where any variables still to be calculated could only reasonably reduce rather than increase the amount to be paid.
- The reasons for making an offer of an ITR payment in a particular amount should be documented.
- The Payroll Team should be involved in giving advice to the decision-maker on calculating the possible ITR payment.
- Conflicts of interest should be clearly disclosed to those involved in the ITR process and documented.
- A conflicted decision-maker should be quarantined from the decision-making process, and
- Significant ITR payments should not be calculated, decided and/or processed at a time when key individuals involved in the process are on leave with others acting in the relevant roles.

What did DPS do following the receipt of Dr Roughley's Report?

DPS has acted on Dr Roughley's recommendations.

Key internal policies were reviewed and updated, including the *Conflict of Interest Policy* and the *DPS Retirement and Redundancy Incentives Policy*. The Secretary wrote to the FPA Committee Chair to provide copies of these policies on 15 September and 16 October 2025 respectively (**Attachment J**).

Following the concerns raised by Dr Roughley about the substantial deficiencies in the data provided by ISD, internal code of conduct investigations commenced in March 2025 (canvassed later in this submission).

In addition, further internal code of conduct investigations considering other issues identified in Dr Roughley's report formally commenced in August 2025. These matters remain ongoing and in order not to prejudice their completion it is not appropriate that they be discussed at this time.

While the subject of the review was an ITR payment, the findings and Dr Roughley's report have led to further concerns being raised about the culture, behaviours and leadership within parts of the department which are being progressively addressed.

Concerns Regarding Security Clearances for TPL staff member

DPS acknowledges that concerns have been raised about the absence of a security clearance for the TPL forensic expert that undertook the authorised data extraction. These concerns have been raised in the context of handling sensitive material that might contain parliamentary privileged material, as well as the extraction and management of departmental data from the PCN.

As outlined in the correction letter from Ms Nicola Hinder PSM, Deputy Secretary, of 26 November 2025 to the FPA Committee (**Attachment K**), the department was advised by HWLE that the TPL employee retained an AGSVA Negative Vetting Level 1 (NV1) clearance. An email providing this assurance from HWLE to DPS is at **Attachment L**. This assurance was based on advice provided by TPL to HWLE that its officer retained the reported clearance. A verbal assurance, from the TPL data forensic expert that he held a NV1 clearance, was also provided to DPS.

Notwithstanding these assurances, the department was formally advised by HWLE on 26 November 2025 that TPL had confirmed that its employee only held an Organisational Suitability Assessment for another Commonwealth agency and that an AGSVA issued NV1 clearance was not held. Advice received from HWLE and DPS' response is provided at **Attachments M and N**.

DPS acknowledges that it was provided with incorrect advice regarding the security clearance held by the TPL data forensic expert. The department would like to assure the Committee that irrespective of this, effective control measures were put in place by the department as outlined in this submission. DPS confirms that the TPL data forensic expert was supervised by various DPS officers that held AGSVA Security Clearances (Negative Vetting Level 2). These measures served to mitigate the risk of access by the TPL data forensic expert who, unknown to DPS, did not hold a security clearance.

Providing supervised access to the APH network to a person without a security clearance, as occurred in this case, is permissible under the Australian Signals Directorate's Information Security Manual (ISM) (published 1 December 2023) which provides:

> ***Temporary access to systems***
>
> *Under strict circumstances, temporary access to systems, applications or data repositories may be granted to personnel who lack an appropriate security clearance or briefing. In such circumstances, personnel should have their access controlled in such a way that they only have access to data required for them to undertake their duties.*
>
> ***Control: ISM-0441; Revision: 8; Updated: Jun-22; Applicability: All; Essential Eight: N/A***
>
> *When personnel are granted temporary access to a system, effective controls are put in place to restrict their access to only data required for them to undertake their duties.*

Code of conduct investigations

The department does not, as a matter of practice, comment on matters which may be personal or private to its officers and employees, including whether Parliamentary Service Code of Conduct (the Code) investigations have been undertaken, and any outcomes of the same. This is aligned with standard practice across the APS. However, given that some of these matters have been formally investigated, have completed but continue to attract interest, it is reasonable to provide some clarity for the understanding of the Committee.

In response to the concerns raised by Dr Roughley in her letter of 28 October 2024, the Secretary agreed to an audit being conducted of the searches undertaken by ISD. The TPL data forensic expert attended APH on 23 December 2024 and conducted an audit log extraction and reporting (from the APH Microsoft 365 platform) focused on searches undertaken by ISD relevant to Authorisations one and two. An audit log review on the Microsoft platform is the process of examining a detailed, chronological record of user and administrative activities to ensure security, compliance, and operational efficiency – it does not involve searching employee (or other) accounts or the extraction of employee data.

The audit logs extracted by TPL were reviewed independently of DPS (by an independent ICT service provider Terrace Services) and examined in detail to establish all data extraction activities carried out, and sequenced to attempt to determine why the ISD search results were materially different (both in content qualities produced and elapsed time to undertake) from the results returned from the TPL conducted authorised data extraction (Authorisation three).

The independent review of the audit log findings verified Dr Roughley's concerns relating to the data extractions undertaken by ISD. It further identified that data searches were conducted by ISD occurred across all exchange locations on the PCN, not just of DPS employee data. The review also identified restrictions applied by ISD officers that had the effect of reducing the amount of relevant DPS staff data provided to Dr Roughley.

As a result, formal code of conduct investigations into three ISD officers commenced in March 2025. These investigations into breaches of the Code related to the searches conducted in June 2024 and August 2024 (Authorisations one and two).

The three officers were placed on miscellaneous leave with pay while the independent investigation into the conduct was completed. Completion of all steps in the independent investigation (investigation, breach decision and sanction) occurred between March 2025 and November 2025, with different timeframes applying to each officer.

Each Code investigation was undertaken by an external investigator appropriately appointed and delegated by the department. In each of the three Code investigation processes, the independent investigator determined that breaches of the Code had occurred. The three officers were informed of this decision and afforded procedural fairness.

After seeking the required agreement of the Parliamentary Service Commissioner, the Secretary appointed an external independent sanction determiner, and delegated that person the power, under section 15 of the PS Act, to impose sanctions on the officers.

Two officers resigned from the department prior to the sanction being applied. The employment of one officer was terminated.

Was Parliamentary Privilege breached?

The department can confirm that the employee data forensic interrogation was undertaken to identify material relevant to the ITR calculation and payment, as it related to DPS officials. There was, and there remains, no focus on Parliamentarians, or other non-DPS officials operating on the PCN.

In determining the protections to put in place to ensure that the immunity attaching to proceedings in Parliament (as defined in section 16(2) of the *Parliamentary Privileges Act 1987 (Cth)* (the Privileges Act)) was not breached, the principal immunity of proceedings from impeachment and question in courts was carefully considered.

In relation to this immunity, Odgers' Australian Senate Practice (14th edition including updates to 30 June 2022), states:

> *'…The immunity of parliamentary proceedings from impeachment and question in the courts is the only immunity of substance possessed by the Houses and their members and committees.*
>
> *There are two aspects of the immunity. First, there is the immunity from civil or criminal action and examination in legal proceedings of members of the Houses and of witnesses and others taking part in proceedings in Parliament. This immunity is usually known as the right of freedom of speech in Parliament. Secondly, there is the immunity of parliamentary proceedings as such from impeachment or question in the courts…'*

This immunity is legislated in section 16 of the Privileges Act. In particular, the immunity of parliamentary proceedings from impeachment or question in the courts is legislated in section 16(3) of the Privileges Act, which provides:

> *(3) In proceedings in any court or tribunal, it is not lawful for evidence to be tendered or received, questions asked or statements, submissions or comments made, concerning proceedings in Parliament, by way of, or for the purpose of:*
>
> *(a) questioning or relying on the truth, motive, intention or good faith of anything forming part of those proceedings in Parliament;*
>
> *(b) otherwise questioning or establishing the credibility, motive, intention or good faith of any person; or*
>
> *(c) drawing, or inviting the drawing of, inferences or conclusions wholly or partly from anything forming part of those proceedings in Parliament.*

The definition of "proceedings of Parliament" for the purposes of section 16 is set out in section 16(2) of the Privileges Act:

> *(2) For the purposes of the provisions of article 9 of the Bill of Rights, 1688 as applying in relation to the Parliament, and for the purposes of this section,* ***proceedings in***

> ***Parliament*** *means all words spoken and acts done in the course of, or for purposes of or incidental to, the transacting of the business of a House or of a committee, and, without limiting the generality of the foregoing, includes:*
>
> *(a) the giving of evidence before a House or a committee, and evidence so given;*
>
> *(b) the presentation or submission of a document to a House or a committee;*
>
> *(c) the preparation of a document for purposes of or incidental to the transacting of any such business; and*
>
> *(d) the formulation, making or publication of a document, including a report, by or pursuant to an order of a House or a committee and the document so formulated, made or published.*

Immunity of proceedings from impeachment and question

While section 16(3) of the Privileges Act is limited to proceedings "in any court or tribunal", it was considered by the Secretary to be best practice to apply that section to the external investigation conducted by Dr Roughley in the same way that it would apply to a court or tribunal. The Secretary considered that this was best practice because this is the premise on which the following two Memoranda of Understanding are based:

- *Memorandum of Understanding between the National Anti-Corruption Commission and the Attorney-General, the President of the Senate and the Speaker of the House of Representatives – Parliamentary Privilege*; and the
- *Memorandum of Understanding on the execution of search warrants and use of covert investigative powers where Parliamentary Privilege may apply between the Attorney-General, the President of the Senate and the Speaker of the House of Representatives*.

The Secretary noted that investigations by both the NACC and the Australian Federal Police (AFP) can result in the NACC or the AFP commencing matters in a court. In contrast, Dr Roughley did not have the power under her terms of reference to commence a matter in a court or tribunal. Instead, Dr Roughley was undertaking a fact-finding investigation, with the report to be provided to the Secretary. However, the Secretary still considered, for the protection of the immunity, that it was best practice to apply section 16(3) of the Privileges Act to Dr Roughley as if her investigation was a court or tribunal.

In order to do so, the Secretary ensured that a process was put in place so that no material which potentially met the definition "proceedings in Parliament" in section 16(2) of the Privileges Act was provided to Dr Roughley.

In addition to controls outlined previously in this submission, the following procedure was put in place to manage the risks:

- The *first phase* involved electronic forensic searches of the DPS employee data using specialised digital search software programmed with bespoke key word or key word based "search-strings" designed to only identify information relevant to the investigation.

The searches were undertaken by TPL using digital search software. TPL did not review the data extracted from DPS or the contents of the data returned from the searches. The data returned via the forensic searches was made available by TPL into a secure digital review program which the limited team of HWLE lawyers (with appropriate AGSVA security clearances) were provided access to via a secure link hosted by TPL (search result 1).

- The *second phase* involved lawyers from HWLE reviewing the data returned from the forensic search to create a subset of material to be provided to Dr Roughley. This material was reviewed by HWLE to ensure that only DPS staff data relevant to the investigation/s was identified and that no Parliamentarian data or data that could meet the definition of section 16(2) of the Privileges Act was provided to the investigator.

In considering this procedure, the Secretary also considered the following factors:

- The investigation related solely to the actions of DPS staff in relation to the payment of an incentive to retire. This is not a matter which, at that time, had any involvement of Parliamentarians or consideration in proceedings of Parliament.
- The searches conducted for the material required for the investigation, should have only identified DPS employee material. However, the Secretary did not consider that this should lead to an assumption that no material concerning proceedings in Parliament might inadvertently be picked up in a search. As a result, a procedure which included a review of the data prior to the provision to Dr Roughley, to ensure that no Parliamentarian data was provided to the Dr Roughley to protect the immunity was put into place.
- The type of material that DPS staff receive in emails or messages from Parliamentarians, are typically to do with the functioning of and/or matters relating to APH or the support services provided by DPS, not matters that relate to proceedings in Parliament. However, the Secretary again did not consider that this should lead to an assumption that no material concerning proceedings in Parliament might be in the DPS employee data extracted, and so a procedure to protect the immunity was put into place.

The Secretary also ensured that the destruction of the data at the end of the investigation would be complete and certified.

In establishing the process, the department attempted to follow the concept of quarantining material from the investigation to review that material for privileged material, as set out in section 27 of the NACC MoU and section 5.2 of the AFP National Guideline.

The Secretary acknowledges that she did not consult with the Clerks of both Houses prior to putting this procedure in place and agrees that it would have been best practice to have done so. The Secretary unreservedly apologises to the Committee for not consulting with the Clerk of the Senate prior to implementing this process. The department recognises that it would have been best practice and would have provided this Committee and Senators with comfort that the Clerk had the opportunity to provide advice to the Secretary on the process being implemented to protect potentially privileged material from being provided to the investigator.

A procedure is now established for dealing with requests for DPS employee data, that may contain Parliamentarian data, that specifically provides for DPS to consult with the Clerks, or appropriate Clerk, and apply the advice provided in relation to mitigation strategies to ensure that any Parliamentarian data is not inadvertently released.

The procedure also requires that the Presiding Officers be advised of the request for DPS employee data and of the outcome/implementation of advice received from the Clerks/Clerk. The new DPS procedure is provided at **Attachment O**.

Response to the Terms of Reference

The department's policies and procedures relating to parliamentary privilege

The department takes its obligations, as a service provider to the Parliament, Parliamentarians and their staff, Parliamentary department colleagues and APH seriously. This includes maintaining the confidentiality of data relevant to the operations of Parliament and of Parliamentarians, and the operations of the Parliamentary departments to which DPS provides supporting services.

The department manages its obligations with respect to parliamentary privilege in consultation with the Department of the Senate, the Department of the House of Representatives and, where relevant, other entities including the NACC and the AFP.

Parliamentary privilege training is available to all DPS staff. In some circumstances this training is mandatory for officers with explicit authorities, and it is also mandatory for all SES officers. Training is conducted by senior officials of the Department of the Senate and the Department of the House of Representatives.

DPS has a range of policies which outline the need to comply with the Privileges Act. These include, but are not limited to, ICT use, Information Management and Record Keeping, and various security policies and procedures.

However, the department also acknowledges that more can be done in relation to the management of information that may contain privileged information.

DPS is reviewing its current ICT policies and procedures. The review will include the development of an ICT Code of Practice to provide a framework over the management, storage, use, release, retention, and destruction of DPS employee information that may contain Parliamentarian or Parliamentary data.

Until the new ICT Code of Practice is developed, the DPS procedure for dealing with requests for DPS employee data that *may* contain Parliamentarian data (discussed earlier in this submission) has been developed and implemented.

The procedure applies to requests for DPS employee data (e.g. emails, Teams messages and/or other Microsoft 365 data), where the scope of the request *may* include Parliamentarian data, for example an email from a Parliamentarian to a DPS staff member.

These types of requests are most likely to occur in DPS initiated investigations involving DPS employees and/or investigations conducted by third parties involving DPS employees. One of the purposes of this procedure is to function as a safeguard against the possibility that requests to access or obtain DPS employee data may be effected in a manner which amounts, or is intended or likely to amount, to an improper interference with the free exercise by a House or Committee of its authority or functions, or with the free performance by a member or the member's duties as a member.

In this regard, this procedure has effect subject to the powers, privileges, and immunities of each House and of the members and the committees of each House.

As well as functioning as a safeguard to ensure that parliamentary privilege is protected and maintained, this procedure is designed to ensure that Parliamentarian data is not inadvertently released as a result of a request to access DPS employee data.

In time, this procedure will be incorporated into the new ICT Code of Practice under development. Internal review of other DPS policies and procedures to reflect issues of parliamentary privilege will also occur.

Finally, DPS notes that parliamentarians corresponding with public officials is not limited to the DPS environment, and that such correspondence may include privileged material. DPS has engaged with APSC and APS colleagues on this risk, to ensure they consider parliamentary privilege, where employee data searches, in support of breaches of the APS Code of Conduct and/or other investigations, are undertaken.

Management of documents, communications and technology

The department acknowledges that its internal guidance on parliamentary privilege, and an understanding of parliamentarian information and data could be further improved.

Additional consideration is being given to:

- Reviewing available training information and, in consultation with the Clerks, the development of online training resources for staff.
- Making parliamentary privilege training compulsory for all staff and not just for SES officers or those with authorised roles.

DPS is also of the view that the Parliamentary ICT environment and its supporting architecture (inclusive of all users including Parliamentarians and their staff, and staff of the Parliamentary Departments being on the same network platform/s) may no longer be fit for purpose and does not provide for appropriate segmentation between users, structurally increasing the risk of a breach.

Further, DPS considers that the currently established arrangements may not support the effective lifecycle management of Parliamentarian data. Broader considerations and discussions are occurring within the department to develop a future work program that reviews and refines the Parliamentary ICT environment to rectify these issues and modernise APH's ICT architecture.

As some of these considerations relate to cybersecurity and associated physical security supporting applications, the department would welcome the opportunity to broadly outline potential options with the Committee in-camera.

Codes of Practice

On behalf of the Parliament, DPS oversees an Electronic Access Control System (EACS) and a Closed-Circuit Television (CCTV) system. The EACS and CCTV are integral elements of a layered security framework contributing to the safety and security of APH. They provide and assist in access control to areas in and around APH and the parliamentary precincts, including for emergency events such as a lockdown.

In accordance with section 6 of the *Parliamentary Precincts Act 1988* (the Precincts Act), the parliamentary precincts are '*under the control and management of the Presiding Officers'*. The EACS and CCTV systems support the Presiding Officers in exercising this responsibility. The EACS and CCTV systems each have a Code of Practice (CoP), approved by the Presiding Officers, governing oversight of the EACS and CCTV capabilities.

The CoPs, for EACS and CCTV, have clear statements about parliamentary privilege and impose strict requirements on officers authorised to access EACS/CCTV data. Authorised Officers, and their delegations and authorities with respect to the EACS and CCTV, are detailed in the CoP.

Each CoP specifies authorised purposes for which EACS and CCTV data and information may be obtained and used. These authorised purposes are contained in the publicly available versions of each CoP available on the APH website at:

- APH_EACS_Code_of_Practice_Guidance.pdf
- APH_CCTV_Code_of_Practice_Guidance.pdf

All Authorised Officers managing and/or accessing the EACS/CCTV are required to sign a Declaration of Compliance with the CoP which includes a statement acknowledging parliamentary privilege. Authorised officers must also undertake formal parliamentary privilege training provided by the Department of the Senate and the Department of the House of Representatives.

One of the purposes of each CoP is to function as a safeguard against the possibility that the EACS/CCTV data may be used in a manner which amounts, or is intended or likely to amount, to an improper interference with the free exercise by a House or committee of its authority or functions, or with the free performance by a parliamentarian or their duties as a parliamentarian.

In this regard, the administration of the EACS and CCTV and the powers given under the CoP, have effect subject to the powers, privileges and immunities of each House and of the members and the committees of each House.

Parliamentary oversight of the management of the EACS and CCTV is achieved through mandated quarterly reporting to the Presiding Officers, through the APH Security Management Board (SMB) which also has a primary role in the oversight of the CoP's. In turn, the President of the Senate, as Presiding Officer, provides EACS and CCTV reporting to the Senate Committee with oversight of parliamentary security (currently the Senate Appropriations, Staffing and Security Committee).

This reporting comprises:

- Quarterly reporting detailing the nature of requests
- An annual report of any alleged breaches or complaints
- A copy of any review of the CoP or compliance with the CoP.

The Presiding Officers' approved CCTV CoP came into effect in 2015 and the EACS CoP in 2020.

Since 2019, four independent biennial compliance reviews have been conducted in accordance with the requirement of the CoPs. The completed compliance reviews have all been reported to the SMB and Presiding Officers. The most recent EACS CoP compliance review, undertaken in November 2024 by an independent external provider, and led by a previous Clerk of the House of Representatives, found:

- The CoP provides a robust framework that balances security objectives with protections for parliamentary privilege.
- Declarations of Compliance were in place for Authorising Officers, with one acceptable variance that did not present an ongoing compliance issue.
- Simplifying the wording and structure of the CoP will improve usability and clarity.
- Automation of certain manual processes can help reduce administrative risk over time.

Since 2021, DPS has submitted four annual reports of alleged breaches and complaints identifying six breach matters under the CCTV and EACS CoPs (four for CCTV and two for EACS). Of these, three were confirmed actual breaches and three were assessed as suspected breaches. All breach matters were formally notified to the Presiding Officers in accordance with the relevant CoP.

DPS maintains a register of Authorised Officers who have access to EACS and CCTV systems, their completion of parliamentary privilege training and their declaration of compliance with the two CoPs. In accordance with the requirement of the CoP, DPS completes reviews of the Authorised Officers. The most recent review was conducted in June 2025 which indicated that all eighty-three Authorised Officers satisfied the requirements.

Comprehensive and specific approval and authorisation procedures govern access, viewing and release of EACS and CCTV data and information. The specific details of these processes and protocols are closely held as they contain sensitive and confidential information. Public disclosure could compromise security; however further information could be provided to the Committee in-camera.

More can be done

Information, Communication and Telecommunication Code of Practice

As noted earlier in this submission, a CoP is currently being developed to establish a clear, consistent and accountable framework for the handling of Parliamentarian data and information stored or managed on department-owned, department-managed systems.

The CoP will clarify what constitutes Commonwealth records versus non-Commonwealth records, address parliamentary privilege considerations, provide clear authorising officers for various activities in relation to department managed systems and align record-keeping practices with legal and policy requirements.

The CoP will be developed based on the following guiding principles:

- **Privilege first**: Material that may attract parliamentary privilege must not be accessed or disclosed without Presiding Officer or Clerk authorisation.
- **Shared responsibility:** The department will provide secure systems and controls that protect privilege while enabling operational support.
- **Transparency:** Access to Parliamentarian data must be authorised, logged and auditable.
- **Lifecycle assurance:** Records must be managed from creation to disposal/transfer at the end of a Parliamentarian's term.

DPS will consult with the Clerks through the development of the CoP prior to seeking the agreement of the Presiding Officers.

Arrangement, agreements or memorandum of understanding with a third party, agency or department

As custodians of APH, and service providers of ICT to parliamentarians, their staff and parliamentary departments, the department observes three Memorandum of Understandings.

National Anti-Corruption Commission (2024)

The MoU between the NACC and the Attorney-General, President of the Senate and the Speaker of the House of Representatives was signed in November 2024. This MoU is publicly available on the APH website at: NACC MoU 27 November 2024

The purpose of the MoU is to establish agreed processes for the exercise of the NACC's powers in circumstances where issues of parliamentary privilege could arise, in order to ensure that parliamentary privilege is respected while permissible action by the NACC to detect and investigate corrupt conduct is not inhibited.

Part 7 of the MoU covers matters related to third parties, where the department, and its processes are captured.

The MoU provides for the quarantining of potentially privileged material under clauses 11, 16, 19, 20, 24, 28 and 31. Part 8 of the MoU provides guidance for the resolution of such material. These matters are directly dealt with by the NACC and the relevant Clerk.

Australian Federal Police (2024)

The MoU records the understanding between the Attorney-General, President of the Senate and the Speaker of the House of Representatives on the process to be followed where the AFP execute search warrant/s or use covert investigative powers under the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* where parliamentary privilege may apply.

The MoU was signed in May 2024 and includes as an attachment the AFP National Guideline on investigations where parliamentary privilege may be involved. This MoU is publicly available on the APH website at: AFP_MOU_and_National_Guideline

The guideline outlines the obligations of AFP appointees involved in law enforcement investigations and is designed to ensure that investigations are conducted in a way that respects parliamentary privilege and that any privileged material is managed appropriately.

Part 6.7 of the guideline provides guidance for AFP appointees related to information held by a third party. In these circumstances, the executing officer (in consultation with the Deputy Commissioner of National Security) will notify the relevant Presiding Officer or Clerk.

Independent Parliamentary Expenses Authority

The MoU relates to the process for information-gathering powers under the *Independent Parliamentary Expenses Authority 2017* and claims for parliamentary privilege. The MoU was signed in November 2024 and includes specific guidance (paragraphs F, 3 and 5) about when DPS will become involved with the provision of any information or data. This MoU is publicly available on the APH website at: MOU_with_IPEA_on_Parliamentary_Privilege.pdf

ICT Service Providers

The department is primarily in-sourced for ICT services. However, DPS does engage a range of ICT service providers under contractual arrangements to support the secure and effective operations of parliamentary systems. These providers may, in the course of their work, access, manage, or transmit data and metadata of current or former parliamentarian.

All ICT service providers are required to acknowledge and comply with contractual arrangements which stipulate that no data, metadata, or information relating to parliamentarians may be disclosed to third parties, including law enforcement or other authorities, without the express written permission of DPS.

In circumstances where a third party seeks access to information held by the ICT service provider relating to a parliamentarian under coercive powers, such as a search warrant, the relevant parliamentarian must be consulted and given the opportunity to consider any claim for parliamentary privilege before any material is released. This approach ensures that the rights of the parliamentarian are protected and that DPS remains compliant with its obligations as custodian of parliamentary information.

Should any ICT service provider have concerns regarding the ownership of material or suspect that requested information may relate to the operation of Parliament, they are required to contact DPS immediately. This enables DPS to work collaboratively with the provider and the requesting authority to ensure that all necessary permissions are obtained and that parliamentary privilege is appropriately considered.

These requirements are formalised through assurance letters and contractual terms, and providers are asked to acknowledge their understanding in writing. An example copy of the assurance letter is provided at **Attachment P.**

Other contractual terms

The arrangements with ICT providers detailed above complement standard terms and conditions in in Commonwealth contracts used by DPS including the requirements to comply with relevant law and policy and the *Privacy Act 1988 (Cth),* and to protect confidential information. Going forward, DPS will look to, where appropriate, insert clauses relating to parliamentary privilege into contracts and work orders under Deeds of Standing Offer.

Conclusion

While we are confident that parliamentary privilege was not breached in the course of Dr Roughley's investigation, the department acknowledges that it has more to do.

This work will continue in the years ahead to enhance our organisational effectiveness and service delivery to support Parliamentarians, the functioning of the Parliament, APH and the community.

The Secretary and the department's Executive will continue to be transparent, accountable and will assist the Committee in this inquiry.

Annex – Summary of key events

Date / Range	Event / Reference
13 October 2023	Incentive to Retire (ITR) payment made to a former Deputy Secretary.
Early 2024	Media reporting and parliamentary scrutiny begin regarding the ITR payment made by DPS.
3 June 2024	Concerns about the ITR payment are formally raised with the Secretary, leading to the Secretary deciding to seek an external investigator to undertake a fact-finding investigation in relation to DPS' actions in relation to the ITR payment.
21 June 2024	Assistant Secretary requests the then CIO to conduct data search for in records relation to the ITR payment which included search terms for an independent DPS investigation. The then CIO requested an authorisation from the Secretary to search Content Manager. Secretary authorised search of Content Manager.
5 July 2024	Meeting held where TPL provides assurances about the treatment and hosting of departmental data on secure, Australia-based, servers.
11 July 2024	Dr Fiona Roughley SC is engaged as an independent external investigator into the ITR payment.
15 July 2024	Initial data provided by ISD to TPL.
24 July 2024	Secretary writes to the Commissioner of the NACC to inform him of the Dr Roughley investigation.
1 August 2024	Further data provided by ISD to TPL.
5 August 2024	NACC Commissioner writes to the Secretary to inform her that he is considering issuing a stop direction in relation to Dr Roughley's investigation or considering a joint investigation. A period of consultation was then undertaken in relation to a joint investigation between the NACC and DPS.
Mid-August 2024	Concerns raised with DPS on behalf of Dr Roughley about potentially excluded material during the data extraction process.
22 August 2024	Secretary provides instructions to the then CIO to undertake bulk data extractions in relation to 8 DPS employees with specific parameters.

Date / Range	Event / Reference
4 September 2024	Draft risk assessment provided to the Secretary.
5 September 2024	Secretary and CIO discuss the draft risk assessment and way forward. Agreed to amend the request as follows: - The data in relation to two DPS employees to be extracted in bulk (by ISD) for it to then be searched outside of the system using TPL's forensic tools. - ISD staff conduct searches on the data of the other six identified DPS employees and review for material that may be sensitive or include correspondence from or to parliamentarians and/or their staff and then provide to TPL.
6 September 2024	Joint investigation into the ITR payment commenced between the NACC and DPS.
9 September 2024	Bulk extract in relation to two DPS employees provided by ISD officers to TPL.
12 and 13 September 2024	Employee data (in relation to six DPS employees) is provided by ISD officers to TPL.
2 October 2024	NACC Commissioner writes to the Secretary (dated 1 October 2024) to advise of the expansion of the NACC's investigation and the termination of the joint investigation.
3 October 2024	NACC execute warrants on DPS.
28 October 2024	Dr Roughley writes to the department, expressing concerns about the completeness of data and recommends engaging an independent external expert for further extraction.
30 October 2024	Secretary authorises TPL to undertake a bulk extract of material in relation to eight DPS employees.
31 October – 1 November 2024	TPL extract of material in relation to eight DPS employees is undertaken. The extraction was supervised by DPS staff with the data transferred on encrypted USBs, in a secure case, to TPL forensic labs in Sydney.
17 December 2024	President of the Senate and Speaker of the House terminate the appointment of the former Secretary Mr Rob Stefanic due to loss of trust and confidence.

Date / Range	Event / Reference
23 December 2024	TPL conducts audit log reporting at APH to enable a review to be conducted by a third party of the ISD searches conducted, confirming deficiencies in the data provided.
11 March 2025	Ms Jaala Hinchcliffe appointed as Secretary
12 March 2025	Dr Roughley provides her report to DPS.
March 2025	Formal Code of Conduct investigations commence in response to concerns about data handling and search deficiencies.
August 2025	Additional Code of Conduct investigations commence from issues identified in Dr Roughley's report.
16 October 2025	Secretary provides a summary of Dr Roughley's report to the Senate Standing Committee on Finance and Public Administration.
November 2025	Three Code of Conduct processes are finalised – two staff resigned ahead of sanctions and one officer's employment was terminated.
26 November 2025	Correction letter from Deputy Secretary Ms Nicola Hinder PSM clarifies that the TPL staff member did not hold an NV1 clearance, but an Organisational Suitability Assessment.
27 November 2025	Data is securely returned to Australian Parliament House by SCEC-accredited safe hand service; access is restricted to the Secretary and Deputy Secretary.
2 January 2026	New DPS Procedure for dealing with requests for DPS employee data that may contain Parliamentarian data implemented.