Australian Government

Department of Finance

Reference: MC25-001837
Contact: Jessica Wilson
Telephone: 02 6215 2120
e-mail: Jessica.Wilson@finance.gov.au

Ms Lizzie O'Shea
Chair
Digital Rights Watch
PO Box 1426
Fitzroy Nth VIC 3068

Via email: Lizzie@digitalrightswatch.org.au

Dear Ms O'Shea

Thank you for your correspondence of 19 June 2025 to Senator the Hon Katy Gallagher regarding the concerns about Palantir Technologies (Palantir)'s presence in Australia. My area is responsible for the Commonwealth procurement framework, and as such, I am responding on behalf of the Minister. Please note, that in responding to your letter we have consulted with relevant entities within the Commonwealth, in relation to their areas of responsibility.

From an overarching perspective, the *Privacy Act 1988* (Cth) regulates the handling of personal information about Australians through 13 Australian Privacy Principles (APPs) that apply to most Australian government agencies, and private sector organisations with an annual turnover of more than $3 million. The Privacy Act gives effect to Australia's agreement to implement the Organisation for Economic Co-operation and Development's global minimum standards for information privacy and obligations under Article 17 of the International Covenant on Civil and Political Rights.

The Australian Government is committed to ensuring accountability and transparency in its procurement activities. The Department of Finance (Finance), as policy steward of the procurement framework, has been implementing robust measures to safeguard these principles through the Commonwealth Procurement Rules and the introduction of the Commonwealth Supplier Code of Conduct.

Below is more detail in response to your specific queries.

1. Complete list of contracts held by Palantir with Australian Government entities

AusTender, the Australian Government's procurement information system, is a centralised web-based facility that publishes a range of information, including key details of contracts awarded. Information about contracts awarded to Palantir by relevant Commonwealth

entities can be found on the Contract Notices page of the AusTender website[1], including the parties, the value, and the nature of the services. You are able to search either current or closed contracts.

There are currently two active contracts that Palantir Technologies has with the Australian Government:

- CN3942923[2] - Australian Transaction Reports and Analysis Centre (AUSTRAC)
- CN4104368[3] - Department of Defence (Defence).

The Commonwealth procurement framework is devolved, with each entity responsible for its own procurement and contract management processes and decisions, commensurate with the scale, scope and risk of each procurement. Should you seek detailed information on the two current contracts, AUSTRAC and Defence are best placed to respond via their contact details available on the AusTender website.

2. What safeguards have been put in place to protect human rights, including privacy, in the context of Palantir's operations in Australia?

The Australian Government has developed Privacy and Notifiable Data Breaches clauses[4] which are mandatory to be included in any contract where the supplier is providing services under a 'Commonwealth contract' as defined under the Privacy Act. These clauses ensure that suppliers to the Australian Government do not act or practice in such a way that would breach an APP. The Privacy Act also requires that the contract contain provisions that such acts or practices are not authorised by a subcontract.

The APPs require a regulated entity to have a clearly expressed privacy policy that outlines its practices and systems relating to the management of personal information (APP 1). In particular, an entity is not to collect personal information unless the information is reasonably necessary for, or directly related to, an entity's functions or activities (APP 3), and an entity must take reasonable steps to notify an individual of the collection of personal information (APP 5). An entity must not disclose personal information for a secondary purpose unless they obtain the individual's consent or an exception applies (APP 6), and an entity must take reasonable steps to protect personal information that it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11).

On 10 December 2024, the *Privacy and Other Legislation Amendment Act 2024* (Cth) came into effect, representing the first stage in the Government's privacy reform agenda. Among other matters, the Amendment Act provides the Office of the Australian Information Commissioner with access to a broader range of enforcement options, as well as new functions and capabilities, to better protect the privacy and personal information of Australians.

3. What steps has the Government taken to ensure transparency and accountability in dealings with Palantir?

The Commonwealth expects its suppliers to conduct themselves with high standards of ethics such that they consistently act with integrity and accountability. The

---

[1] https://www.tenders.gov.au/cn/search
[2] https://www.tenders.gov.au/Cn/Show/28d54641-8a0b-4d2c-8a4b-59177e9c7646
[3] https://www.tenders.gov.au/Cn/Show/abce7d48-265e-4b3c-aa77-7fbc197e84f2
[4] https://www.finance.gov.au/government/procurement/clausebank/privacy-and-notifiable-data-breaches

Commonwealth Supplier Code of Conduct (Code)[5] came into effect on 1 July 2024 and must be incorporated into all Commonwealth forms of contract by all relevant entities. The Code requires that suppliers must develop and maintain appropriate processes to manage the risks associated with their operations. These include, but are not limited to, risks relating to labour and human rights and cyber security.

Further, to support transparency, Australian Government entities subject to the Commonwealth Procurement Rules must report contracts on AusTender within 42 days of entering into a contract when it is valued at or above the reporting threshold.

The Protective Security Policy Framework (PSPF), administered by the Department of Home Affairs, requires Australian Government non-corporate Commonwealth entities (NCEs) to:

- be accountable for the management of security risks arising from procuring goods and services,
- consider the security risks of vendors operating under foreign ownership, control or influence (FOCI), and
- include proportionate security terms and conditions in procurement, contacts, and third-party outsourced arrangements to ensure that service providers, contractors and subcontractors comply with relevant PSPF Requirements.

The PSPF recommends that NCEs choose vendors that have demonstrated a commitment to security and transparency for all elements of the supply chain relating to their products and services, to ensure accountability and aiding NCEs in meeting their obligations under the PSPF.

In addition, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* applies to all agencies subject to the Privacy Act, helping to build a consistent, high standard of personal information management across all Government agencies. It requires agencies to undertake a written Privacy Impact Assessment for all 'high privacy risk' projects, including initiatives that involve new or changed ways of handling personal information that are 'likely to have a significant impact on the privacy of individuals'. A Privacy Impact Assessment is a systematic assessment of a project, which can assist in identifying potential impacts that a project may have on individuals, and sets out recommendations for managing, minimising or eliminating those impacts.

4. What protections have been applied to safeguard Australian data from access by foreign governments and entities?

In 2024, the Department of Home Affairs issued a Direction to all NCEs through the PSPF, requiring entities to identify indicators of FOCI risk related to the procurement and maintenance of technology assets and appropriately manage and report those risks. This Direction has been incorporated into PSPF Release 2025, which mandates that NCEs consider security risks before engaging providers operating under FOCI for all procurement and contract decisions. Substantial guidance is provided in the PSPF Guidelines on identifying, assessing, treating and reporting FOCI risks in procurement.

The PSPF requires security classified information and data to be securely hosted using a Cloud Service Provider and Data Centre Provider that has been certified against the Australian Government Hosting Certification Framework (HCF), which ensures that data

[5] https://www.finance.gov.au/government/procurement/ethical-conduct-suppliers/commonwealth-supplier-code-conduct-overview

sovereignty, ownership structure, liability, supply chain and transparency arrangement risks are appropriately managed.

Providers of software and data processing services to the Australian Government may also be subject to the *Security of Critical Infrastructure Act 2018* (SOCI Act). The SOCI Act creates a framework to ensure that entities protect data where its security is critical to the social or economic stability of Australia or its people, or to its defence and national security. In particular, the SOCI Act requires entities responsible for critical data storage or processing assets to adopt, maintain, and comply with a critical infrastructure risk management program (CIRMP) specific to their assets – which can include data.

The SOCI Act further requires all responsible entities to include within the considerations of their relevant CIRMPs any business critical data and the storage systems they may have in connection with these. Parts 3 and 3A of the SOCI Act also provide Government last resort powers to respond to security risks and incidents affecting critical infrastructure.

The Australian Government is also progressing a number of initiatives under the *2023-2030 Australian Cyber Security Strategy*[6] (Cyber Security Strategy) aimed at uplifting Australia's data security settings. Two out of the four initiatives that may be of interest include:

- A review of Australia's data brokerage ecosystem, which looks at the risk of malicious actors purchasing and exploiting Australian data through legal markets, as well as options to mitigate these risks, complementing proposed Privacy Act reforms; and
- A review to identify sensitive and critical data categories that may not be adequately protected under existing regulation, and explore options to protect such data once identified.

Both Reviews are due to conclude by the end of 2025 as part of Horizon 1 of the Cyber Security Strategy.

Furthermore, the Privacy Act applies to organisations that are incorporated within Australia, as well as overseas organisations that carry on a business in Australia. The Privacy Act creates a framework for the cross-border disclosure of personal information through the operation of APP 8 and section 16C. The framework generally requires regulated entities to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs and makes the entity accountable if the overseas recipient mishandles the information.

I appreciate your vigilance in advocating for digital rights and privacy. The Australian Government remains committed to addressing these concerns and ensuring that the privacy and security of all Australian's data are upheld.

Yours sincerely

Jessica Wilson
A/g Assistant Secretary
Procurement Policy and Systems Branch

2 October 2025

[6] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf