QON No. 23

Legislative Assembly for the Australian Capital Territory
elect Committee on Estimates 2026–2027

Inquiry into Appropriation Bill 2026–2027 and Appropriation (Office of the Legislative Assembly) Bill 2026–2027

Answer to question on notice

Asked by: Ms Fiona Carrick MLA

Addressed to: Minister for the Public Service

Reference: ACT Digital Strategy

Hearing: 21 July 2026
In relation to: Risk Management
Question received: 28 July 2026
Answer Due: 5 August 2026

1. What mitigation strategies does the ACT Government have in place to address the risk of a foreign government directing technology providers to remove or restrict access to critical services used by the ACT Government?

2. Is the ACT Government considering increasing the use of open-source software solutions as part of its risk mitigation strategies, including the use of open-source large language models?

Rachel Stephen-Smith MLA: The answer to the Member's question is as follows:

1. The ACT Government mitigates the risk of foreign governments directing technology providers to remove or restrict access to critical services through a combination of protective security policy, procurement controls, Foreign Ownership, Control and Influence (FOCI) risk management requirements, targeted security directions, and enhanced due diligence processes for high-risk technology procurements. These measures are designed to identify, assess, and manage risks associated with suppliers that may be subject to FOCI, and to support informed decisions regarding the use of technologies that underpin critical government services.

   The ACT Protective Security Framework (PSF) sets out the government's approach to protecting people, information, and assets. To strategically mitigate FOCI risks, the ACT PSF Core Practices Standards were updated in 2025 to incorporate FOCI risks management requirements. Under GOVSEC 6 – Security governance for contracted goods and service providers, entities are required to identify and manage security risks relevant to the procurement, including FOCI risks.

   In 2025, the Attorney-General issued two ACT PSF Directions to accountable authorities to manage the relevant protective security risks within the ACT Government.

   a. ACT PSF Direction 001-2025 DeepSeek Products, Applications and Web Services

   b. ACT PSF Direction 002-2025 Kaspersky Lab, Inc. Products and Web Services

2. The ACT Government has a range of risk mitigation strategies in place to ensure the safety of its technology systems. The Cyber Security Policy (ACT Government Cyber Security Policy - ACT Government Transparency Portal) and ACT Protective Security Framework (ACT-PSF-Core-Practice-Standards.pdf) sets out the requirements for ACT Government systems to undergo cybersecurity risk assessment.

   The ACT Government's AI Policy and Assurance Framework (ACT Government Artificial Intelligence Policy - ACT Government Transparency Portal), sets out the parameters for safe, secure and ethical use of AI across the ACT public service. When a business area is considering an AI tool that may meet their specific business needs, including open-source LLMs, they are required to undertake an AI risk assessment, which is reviewed by the ACT's AI Advisory Group. The subject matter experts in the Group provide advice to initiative owners on risks across Australia's eight AI ethics domains, which are outlined in the ACT Government's AI Policy.

Approved for circulation to the Select Committee on Estimates 2026–2027

Signature:  Date: 6/8/26

By the Minister for the Public Service, Rachel Stephen-Smith MLA