27 November 2020

Secretariat
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

via email: ci.reforms@homeaffairs.gov.au.

Dear Secretariat

Submission in response to the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and associated regulations

We appreciate the opportunity to comment on the exposure draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill) and associated regulations.

Sydney Airport understands the need to constantly evolve security settings in order to protect critical infrastructure. However, changes always need to be proportionate having appropriately weighed the costs against the risk and reward of action, especially in the context of COVID-19 when company balance sheets are under considerable strain. Our comments on the Bill as proposed relate to:

- the proposed government assistance provisions;
- harmonisation with other requirements; and
- cost considerations associated with any new requirements.

Aligning the use case of the government assistance provisions with industry

Part 3 of the *Security of Critical Infrastructure Act* (SOCI) currently provides the Minister for Home Affairs with the power to issue a direction to a reporting entity or operator to require them to take action to mitigate risks that are prejudicial to security. Sydney Airport is currently subject to similar provisions through the 'Special Security Directions' under the ATSA, which has previously been exercised.

The government assistance provisions in the Bill as proposed provides, as a last resort, the ability for the Minister to intervene through direction powers to protect assets during or following a significant cyberattack against a critical asset. While noting the criticality of these provisions under the circumstances where they would be used, transparency and collaboration here is vital. Policies and procedures should be co-designed with industry, including extensive scenario planning exploring how and when it is likely the government assistance provisions would be used. Any policies and procedures developed as a result of this process should also include a notification requirement on Government to the entity detailing the threat or risk that led to the direction, including providing detail on the nature of the direct action taken on the entity's systems.

Working together to ensure harmonisation between new and existing requirements

Sydney Airport is currently subject to a range of requirements stipulated under the ATSA, the *Aviation Transport Security (Incident Reporting) Instrument 2018*, and Australian Signal Directorate's Essential 8 Requirements. It is critical that there is harmonisation between all legislative and regulatory underpinnings in efficiently managing security requirements.

Sydney Airport has a long track record of engaging with the Aviation and Maritime Security division of Home Affairs and with the Australian Federal Police given their on-airport presence. These relationships should continue to be leveraged in the specific application of the Bill as proposed and any future regulatory requirements imposed on Sydney Airport.

We note that consequential reforms to the ATSA and associated regulations will be progressed next year to give effect to an 'all hazards' approach from the current more limited 'unlawful interference' approach. This process will in large part formalise obligations to undertake entity risk assessment processes which underpin existing transport security programs. It also needs to give due consideration to expanded information sharing

arrangements between industry and government given the move to the more holistic 'all hazards approach,' which will now capture things such as extreme weather events.

Sydney Airport is supportive of these requirements being co-designed with industry on sectoral basis. This will be critical to ensure that the objectives of the reforms are met while adhering to some key principles including:

- not duplicating existing regulatory approaches across sectors
- are principles-based and proportionate to the risk profile of the particular sector or subsector; and
- impose the least regulatory burden necessary to achieve the security outcomes.

Further, Sydney Airport notes the Department of Home Affairs is currently assessing the categorisation of aviation and air cargo entities against key criteria to establish what constitutes a system of national significance. This process will dictate to what extent entities have new or amended requirements imposed upon them under the enhanced cyber security obligations. When this assessment is done, it should be stress tested with industry to ensure that only critical systems are captured and are consistent with the principles set out above.

Properly considering cost imposition on industry in the context of COVID-19

The entire aviation sector has been severely impacted by COVID-19. Since April, passenger numbers have declined by approximately 97% at Sydney Airport, which has had a very significant impact on revenue streams for the airport.

Given this, the capacity of Sydney Airport to absorb upfront capital and ongoing compliance costs is negligible. In short, Sydney Airport remains concerned the increased security requirements will add significant cost to the business at a time when it can least be afforded.

To manage against this, the sectoral co-design and Regulatory Impact Statement process should properly weigh the costs against the risks and rewards of any action taken. This should include examination of every additional requirement imposed, which systems are deemed to be of national significance, and negotiations on appropriate lead times required for implementation of any changes to appropriately manage additional cost impacts as a result of the increased regulatory burden.

Due to the international travel restrictions, the fluid and evolving nature of domestic travel restrictions, and lower future demand (as evidenced by airline fleet reductions), the path to recovery for the aviation sector remains uncertain. In this context, given the overriding public interest served by the reforms in the proposed Bill, serious consideration should be given to the use of Government funding where significant costs would otherwise be levied on the aviation sector. This is especially important while the path to recovery remains uncertain.

Conclusion

Thank you for the opportunity to provide input on the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and associated regulations. If you require any further information, please do not hesitate to contact Sydney Airport's Manager Public Affairs on [redacted] or at [redacted].

Yours sincerely

[redacted]

Sidone Thomas
General Manager Technology, Data & Digital

[redacted]

Matt Duffy
General Manager Operations