

1 February 2022

Mr Hamish Hansford
Group Manager
Head - Cyber & Infrastructure Security Centre
Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Dear Hamish,

Transport Security Amendment (Critical Infrastructure) Bill 2022

Thank you for the opportunity to provide comment on the above referenced proposed amendment. Adelaide Airport Limited (AAL) is pleased to provide its response for consideration by the Cyber & Infrastructure Security Centre, Department of Home Affairs.

AAL welcomes the approach by Government to avoid unnecessary duplication through enacting the required changes through amendment of the Aviation Transport Security Act 2004 (ATSA). We also thank you for the opportunity afforded to industry to participate in the regulatory co-design process. This is an important step to ensure that the future legislation and associated regulatory obligations meet Government requirements to uplift the security and resilience of Australia's critical infrastructure, whilst not conferring overly burdensome reporting requirements on critical infrastructure operators.

AAL recommends that the determination of critical industry participants is risk based, aligning with the Airport Categorisation Model. It would be helpful for Government to share further detail on the establishment of Systems of National Significance (SoNS) and how they might apply within the aviation industry. In parallel, we would welcome clarification on how SoNS within the other identified critical infrastructure sectors, which have interdependencies with aviation, will be managed. In support of the management of risk across all Australian critical infrastructure, there should be a consistent reporting framework which facilitates Government's ability to draw meaningful comparison across sectors. This could be via the adoption of existing established risk management frameworks, such as the National Institute of Standards & Technology Cyber Security or the Australian Cyber Security Centre's Essential Eight frameworks.

AAL requests that determination is given to the 'relevant impact' triggers required for mandatory cyber security incident reporting. It is imperative that a balance is found to manage contemporary threat and risk whilst affording operators the latitude to ensure on-going business continuity. We look forward to receiving further details on the mechanism to be deployed to streamline mandatory reporting, which we note is intended to be provided to both the Department of Home Affairs and the Australian Signals Directorate.

AAL notes the intent of the changes are to ensure an 'all hazards' approach to risk management. Further consultation on defining required changes to Transport Security Programs (TSP) is encouraged, specifically the level of detail on our processes to manage unlawful and operational interference through adoption of the 'all hazards' approach. We strongly recommend that the agreed inclusions in the TSP do not confer an unnecessary administrative burden on both industry participants and CISC, brought about by a requirement to make frequent amendments, noting AAL has a well-established risk management program with frequent comprehensive risk reviews undertaken across all aspect of its business.



Adelaide Airport Limited
1 James Schofield Drive
Adelaide Airport
South Australia 5950

T +61 8 8308 9211
F +61 8 8308 9311
adelaideairport.com.au
ABN 78 075 176 653

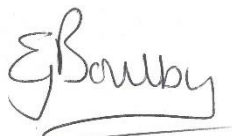
Furthermore, we recommend that industry participants should be able to leverage their existing enterprise risk management programs and reporting protocols, rather than being required to replicate within the TSP. We favour a model which considers assurance attestations by industry, aligned to the 'all hazards' approach. Such an attestation might be a statement of alignment to AS31000 and that all identified risks and vulnerabilities have been considered. This would provide Government with assurance that there is robust risk management framework in place, whilst giving appropriate oversight of material cyber and security risks.

We note the additional powers to be conferred on Transport Security Inspectors. AAL requests that any additional powers to access data, systems and equipment of the critical infrastructure operator be done in consultation with the operator and with its oversight. This will assist TSIs in ensuring appropriate and timely access to specific information deemed to be required in the course of investigations. We also suggest that consideration is given by Government to the use of independent auditors as well as the stated model of a specialist support person working with the TSI, particularly with regard to cyber security oversight, noting its complexity and pace of threat evolution.

AAL would welcome additional information on the format of periodic reporting required to demonstrate compliance with these regulatory reforms, which we note will be required from AAL on an annual basis. Insight on the proposed regulatory and compliance oversight of the 'all hazards' approach to managing critical infrastructure risks will assist us to ensure we are best placed to meet our new regulatory obligations.

We look forward to continued engagement with Government through the regulatory co-design process. If you would like to discuss any of the issues considered in this response, please contact me at [REDACTED] or [REDACTED].

Yours sincerely



Emma Boulby
Executive General Manager Airport Operations
Adelaide Airport Limited