AUSTRALIAN AIRPORTS ASSOCIATION

22 September 2020

Critical Infrastructure Centre
Department of Home Affairs
3-5 National Circuit
BARTON ACT 2600

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

To whom it may concern,

Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

On behalf of its members, the Australian Airports Association (AAA) welcomes the opportunity to comment on the *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper (the Paper). The AAA's submission supports those provided by airport operators, such as Sydney Airport and contains advice provided by other major airports.

Australia's aviation industry has been heavily affected by COVID-19, with airports among the first to be affected, particularly after the Australian Government's decision to close the international borders in March 2020. The decline in air traffic between March and May 2020 saw passenger numbers at Australian airports fall by 97% below the same time in 2019. International and local forecasts for recovery means airports will also be among the last to emerge from the aviation industry's crisis once the pandemic comes to an end.

Airports are net consumers rather than producers of critical infrastructure (CI) systems, sourced from a range of private sector suppliers. These include electronic payment systems used by airport retailers, voice and data telecommunications systems and other systems used by airports such as environmental control, building management and business systems. Airports also use CI systems provided by government, such as safety-critical Air Traffic Control systems provided by Airservices and security systems for border control and biosecurity operated by Border Force and Department of Agriculture respectively. The AAA recommends Department of Home Affairs (DHA) explores fully the interdependencies between private sector and government systems in CI entities.

Security of Australia's airport sector is already heavily regulated, with the nine major 'designated' airports defined in the *Aviation Transport Security Act 2004* and most other airports operating within an existing raft of physical, personnel and cyber security obligations. At a high level, the AAA is concerned at the potential for confusion and overlap between these different security obligations. Airports have also stated the current security environment appears disjointed from an end user perspective, particularly between cyber security and personnel and physical security domains How the Government proposes to deal with this perception that an already complicated system will increase in complexity is a matter that should be resolved as part of any CI Strategy.

Airports have expressed to the AAA their concerns that any new CI regulatory framework is extremely likely to duplicate existing security measures and systems, potentially creating a conflicting regulatory regime for airports between physical, personnel and cyber security. For

Level 1, 55 Blackall Street
Barton ACT 2600
T +61 2 6230 1110 | F +61 2 6230 1367 | E info@airports.asn.au
www.airports.asn.au ABN 89 008 647 336

airports, the physical security regime outlined in the Paper (p. 19) is currently being extended to an increasing number of regional airports due to the Australian Government's decision to strengthen aviation security systems, announced in May 2018. Similarly, airports are already engaged with many of the personnel security elements of the Paper (p. 20) through the Aviation Security Identification Card (ASIC) process, either as ASIC issuers or through the ASIC vetting process.

In other domains of aviation security, the question of who funds new or upgraded government-manded security measures has become an issue. Revenues in Australia's airport sector were already slashed by $1.57 billion in the first half of 2020, with the full year total of lost revenue expected to reach $3.5 billion. The AAA strongly recommends that questions of who will fund and who will pay for the costs of complying with an upgraded CI security environment is fully explored in any subsequent iteration of a CI Strategy and in the Regulatory Impact Analysis process.

The pandemic has exposed the difficulty of funding increased security measures for airports through either 'user pays' or 'beneficiary pays' methods. The collapse in air traffic has shrunk the ability to offset the increased costs of complying with new or upgraded mandatory aviation security requirements through long-term trend growth in passenger numbers.

The effect on the 'user pays' model in aviation security is highlighted by the recent announcement from Melbourne Airport that international security screening charges would rise by 450% from $6.22 to $29.76 per passenger from October 2020. It is likely that other airports will follow suit with increases in per passenger charges for both international and domestic security screening. Costs are recovered by airlines on behalf of airports from passengers through a ticketing surcharge.

The 'beneficiary pays' model is used by the Australian Government to achieve compliance in the rollout of enhanced security screening infrastructure. As airports benefit through having upgraded security screening infrastructure and facilities compliant with international standards, it was expected that airports would fund procurement of their own screening equipment and upgraded facilities. While some airports could meet this cost through their own means, others were unable to fund these upgrades, requiring Government-led grant funding initiatives to achieve compliance.

These examples highlight the potential difficulties in funding the rollout of a CI Strategy through a 'user pays' or 'beneficiary pays' system in the current aviation environment, which is not expected to return to pre-pandemic activity levels until 2024. A finalised CI Strategy should account for the uneven capabilities of CI-identified sectors such as airports to self-fund upgrades and a role for Government-led solutions such as grant funding in assisting airports to meet CI compliance goals.

In regard to the consultation process for the CI Strategy so far, the AAA is concerned at the speed with which the first stage was conducted, creating a perception at odds with the co-design principles put forward in the Paper. The AAA recommends that future consultation with the airport sector on CI strategy and operations takes place through existing stakeholder engagement processes managed by DHA's Aviation and Maritime Security Division. These are well understood by industry participants and bring together key staff with strong industry-specific knowledge that will be valuable for DHA in co-designing a fit-for-purpose framework to manage CI in aviation.

If you require further information, please contact Mr. Scott Martin, Manager of Policy and Corporate Affairs on [redacted] or at [redacted].

Yours sincerely

[redacted]

James Goodwin
Chief Executive