19 February 2021

QANTAS GROUP SUBMISSION ON THE REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFASTRUCTURE) BILL 2020

The Qantas Group (**the Group**) welcomes the opportunity to provide a Submission to the Review by the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) on the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (**the Bill**).

The Group supports the Australian Government's objective of uplifting the security and resilience of critical infrastructure in Australia through changes to the *Security of Critical Infrastructure Act 2018* (**the SOCI Act**). The security of our physical, personnel, supply chain and cyber environments are important to the Group as they directly impact our operations, employees, service providers and the 55 million customers we fly each year (prior to COVID-19). Across our diverse operations – which includes Qantas Domestic, Qantas International, Jetstar Australia, Jetstar Asia, Jetstar Japan, Qantas Loyalty and Qantas Freight – the Group's total contribution to the Australian economy in 2018-19 was $12.8 billion.

Overall, the Group believes it is currently well-positioned to respond to a wide variety of security threats, as we continue to operate under a highly-developed Group Management System and a mature risk management framework. The principles and approach of our own framework already closely aligns with the objectives that Government is seeking to achieve across the nation's critical infrastructure sectors. This enables us to deliver our commercial imperatives, while continuing to meet our obligations across a range of regulatory frameworks. The Group also supports the Government's objectives in this Bill – as well as through *Australia's Cyber Security Strategy 2020* – to help protect Australia's most critical entities against cyber-attacks. Since the *2016 Cyber Security Strategy*, we have completed a cyber transformation program which has significantly uplifted the Group's ability to protect and respond to the dynamic threat environment. Even so, we support a broader uplift in security and resilience across all critical infrastructure sectors and believe this will be ultimately beneficial for the Group, due to the interdependency of systems, services and operating networks.

In our Submission to the PJCIS, the Group would like to comment on four matters regarding the Bill: applicability; potential for duplication; financial implications; and timelines.

Applicability

The Group notes that while the Bill provides definitions around categories of assets and sectors, there remains some uncertainty for companies about precisely which assets may be subject to the new framework proposed by the Bill. This is particularly the case for companies that operate assets in a variety of categories, and therefore may be subject to multiple requirements.

Moreover, companies are not yet aware of whether any of their assets will be prescribed as a system of national significance (**SoNS**). We understand that this prescription will be determined in due course by the Minister for Home Affairs; however, it remains unclear whether the Group – or other entities – will be involved in this process. Given the definition of a SoNS relates to interdependencies across sectors and cascading consequences of disruption, we submit that industry be given the opportunity to articulate their systems of value and operating environment to assist this process. We believe this will assist Government and industry to develop a shared understanding of this environment.

Without knowing which assets or categories will apply, it has been difficult for companies to comment on how the Bill may impact their operations; to calculate the potential financial implications of any security uplift; or to assess the unintended consequences that may result from the introduction of the Bill.

Potential for duplication

The Group is supportive of the Department of Home Affairs' (**DHA**) goal of cross-referencing and complementing existing regulations through this Bill and other proposed legislative changes. However, the Group believes that the proposed regulatory framework has not been established with a view to a single organisation undertaking all (or multiple) functions, but rather as individual organisations undertaking discrete functions. This could result in duplication in documentation and administration for both the Group and Government.

The Group suggests that Government conducts an exercise to map the dependencies between regulators and the relevant laws in order to articulate the impost on industry and identify where efficiencies or regulatory offsets may be realised. The Group suggests that an exemptions model should be considered, which allows entities to obtain exemptions from obligations that are not relevant to their particular infrastructure or business.

The Group also seeks clarification around how the additional cyber responsibilities will be regulated. We understand that while the Australian Cyber Security Centre (**ACSC**) is likely to retain the technical expertise and cyber intelligence function, should cyber-related obligations be regulated by another agencies, this may raise issues with cross-agency coordination. Given the highly technical, sensitive and time-critical nature of the cyber environment, having critical infrastructure-related cyber responsibilities spread among different agencies could undermine the ability for multiple Government and industry stakeholders to manage this shared responsibility.

Financial implications

To meet the additional regulations and requirements under the Bill, it is vital for the Group to strike a balance between investing additional financial resources, with the need to remain viable and sustainable as a business in this challenging time. The Group suggests that without Government funding support, this new framework may not achieve its objective of materially improving critical infrastructure security and resilience, due to economic pressures Australian businesses are currently under due to the COVID-19 pandemic.

Timelines

The Group remains concerned about the short timeframes provided to industry during the consultation phases of this new framework, as this may result in potential unintended consequences. We recommend that Government assess the impact of the legislation from multiple perspectives including supply chain, industry, asset and information technology – at a minimum – to ensure inclusion of the applicable industries, assets and thresholds. We also strongly recommend a more exhaustive and lengthy consultation period on the sector-specific Positive Security Obligations (**PSOs**). Without this – particularly during this period of financial pressure and uncertainty for Australian businesses – there is a risk of industry being ill-equipped and ill-prepared to implement the changes desired by Government.

While the Group believes the proposed new framework will ultimately support the goal of improving the security of the nation's critical infrastructure, we reiterate our recommendations that the collaboration and implementation processes be slowed down significantly in order to ensure due consideration by both industry and relevant government agencies on how to create the most efficient, effective and practical system.