Australian Airline Pilots' Association
Member of IFALPA

Suite 6.01, Level 6
243-249 Coward Street
Mascot NSW 2010

T. +61 2 8307 7777
F. +61 2 8307 7799
E. office@ausalpa.org.au

By Email

12 December 2022

Mr Jim Anderson
Assistant Secretary, AusCheck
Cyber and Infrastructure Security Centre
Department of Home Affairs
PO Box 25
BELCONNEN, ACT 2616

Email: IBReformProject@homeaffairs.gov.au

Dear Jim,

AusALPA SUBMISSION ON THE AUSCHECK DISCUSSION PAPER: *IMPLEMENTING A SINGLE ISSUING BODY REFORM FOR AVIATION AND MARITIME SECURITY IDENTIFICATION CARDS (ASICS AND MSICS)*

Who are we?

The Australian Airline Pilots' Association (AusALPA) is the Member Association for Australia and a key member of the International Federation of Airline Pilot Associations (IFALPA) which represents over 100,000 pilots in 100 countries. IFALPA was formed in 1948, formally recognised by the International Civil Aviation Organisation (ICAO) in 1952 and enjoys permanent observer status in recognition of its continuing contribution to international aviation standards.

AusALPA is a non-industrial collaboration between the safety and technical resources of the Australian Federation of Air Pilots (AFAP) and the Australian International Pilots association (AIPA), representing more than 7,500 professional pilots within Australia. Our membership places a very strong expectation of rational, risk and evidence-based safety and security behaviour on our government agencies and processes. We regard our participation in the safety and security-related work of the Australia's government agencies as essential to ensuring that our policy makers get the best of independent safety and technical advice.

As a key stakeholder in Australia's aviation industry and representative of ASIC holders operating in the highest risk environment, AusALPA welcomes the opportunity to contribute to the AusCheck Single Issuing Body reform proposal.

AusCheck's vision

AusALPA completely supports the vision outlined in the Discussion Paper (DP):

> Our vision is for a cyber-secure, streamlined, user focused and transparent system for security identification services which will support the best available identity verification methods appropriate to each of the schemes AusCheck administers under the *AusCheck Act 2007*.

However, we are hesitant about this assertion:

> For the ASIC and MSIC schemes, the single issuing body in AusCheck will support the needs of all users: individuals, employers and infrastructure facility operators.

In particular, the key issue will be the benchmark set for AusCheck to measure the required level of "support" before it considers the single issuing body (SIB) strategy as successfully redressing the previous system failures. It is yet to be seen whether the service standards set out on page 17 of the DP are sufficient to maintain or enhance current efficiency levels. Furthermore, it is not clear what independent review process AusCheck will be subject to in order to assess the stakeholders' view of the level of support provided in comparison to their stated needs.

Systemic failures

The systemic failures outlined in the Regulation Impact Statement referred to on page 8 of the DP are not entirely unexpected in such a widely distributed system as the ASIC/MSIC IB system grew to become. AusALPA understood that the genesis of today's multiple IB scheme was that the Office of Transport Security (OTS), however now known, for a variety of machinery of government reasons could not possibly support the needs of industry stakeholders in terms of scale, flexibility or efficiency for the provision of these critical identification documents. More importantly, the most obvious failure to be seen was the inability or unwillingness of OTS to adequately and rigorously supervise the IBs as their numbers proliferated.

While we acknowledge that the cyber threat level has changed significantly and that securing a single database is preferable to trying to secure many, vulnerabilities will continue to exist where commercial and industry partners are involved, particularly at the critical entry point of identity verification. We recognise that AusCheck is well aware of that problem, but balancing the efficiency needs of stakeholders with the security benefits of data control by a monolithic DHA bureaucracy seems likely to result in degraded responsiveness.

It is noteworthy that, following the Wheeler Report[1], the Australian Parliament's Joint Committee of Public Accounts and Audit issued a report in December 2006[2] that included the following:

> **Recommendation 4**
>
> 3.45 As well as being responsible for the assessment of criminal and security background checks for applicants of Aviation Security Identification Cards (ASICs), that the new Australian Background Checking Service, AusCheck, be charged with responsibility for the issue of these cards, and that appropriate standards for the issue of ASICs be determined in consultation with industry.

We are left to wonder whether the much more recent exposure of cyber risks across government and business in Australia has more to do with this reform than any lingering concerns about the utility of ASICs and MSICs as effective access control mechanisms.

While government agencies often point to the COVID-19 pandemic responses as justification for inaction, the reality is that while the vast majority of our members were stood down, many without income, the vast majority of the staff of the Australian Public Service continued to be employed with no income reductions. In other words, rather

---

1 Rt Hon Sir John Wheeler, *An Independent Review of Airport Security and Policing for the Government of Australia*, September 2005

2 JCPAA Report 409 "Developments in Aviation Security since the Committee's June 2004 *Report 400: Review of Aviation Security in Australia*"

than being a hindrance, in many ways the pandemic provided an opportunity for accelerating policy making and implementation.

Despite the long history of this issue, rather than taking an holistic view the AusCheck DP still takes a 'one step at a time approach' to secure personal identification and access controls. AusALPA considers government's management of the continuing security weaknesses in the current ASIC/MSIC regime to be the biggest systemic failure since the system began, a legacy that must be rectified during the transition to a SIB.

Previous engagement

We have been engaged in the aviation security space for a considerable time and remain frustrated at the glacial pace of reform.

In the particular case of ASIC reform, the last significant engagement was in 2015 – firstly, through the Senate Regional Affairs and Transport References Committee Inquiry into Airport and Aviation Security and, secondly, through the then Department of Infrastructure and Regional Development (DIRD) Options Discussion Paper *Scope of Aviation Security Identification Cards (ASICs)*. Before then, going back to at least 2010, we were engaged with OTS on making the ASIC more useful as a barrier to access to secure areas by bad actors.

ASICs/MSICs for entry control

From the Cyber and Infrastructure Security Centre (CISC) perspective, the ASIC/MSIC serves solely as a visual indication of a person's authority to be present in certain security-controlled areas. The ability of a facility operator to encode the authorised person's ASIC/MSIC card stock with facility access control is a secondary CISC consideration but a primary one for the facility operator if the vulnerabilities of separate unlinked cards are to be avoided. From a pilot's perspective, they are largely inseparable considerations since operating efficiency is severely impacted if a pilot is authorised to be somewhere but unable to gain access.

The DP is focused on the issue of data integrity for an 'authority to be present'. It does not address the anti-counterfeit strategy that AusALPA considers essential for the integrity of a visual authority check. We are aware anecdotally of people copying or constructing fake cards and we are also aware of people swapping or lending valid ASICs to unauthorised persons, in each case with the intention of exploiting the porosity of airside access controls and lack of scrutiny.

On the specifics of access control, the DP states:

> Access control remains an industry responsibility; not that of the Government. The single issuing body will produce security identification cards. We will provide an applicant with an ASIC/MSIC printed on an encodable card stock if/as requested by the employer.

To be blunt, access control is merely delegated to the industry – the government remains responsible for the security outcomes. This approach underpins the failure of OTS to properly regulate the multiple IB scheme and hints at a continuing attitudinal failure with the CISC that needs to be urgently addressed.

Part of our anti-counterfeit strategy is to go beyond the CISC proposition to merely provide encoding capability by instead requiring that access to security-controlled areas may only be gained through an encoded ASIC/MSIC. Visitor Identification Cards (VICs) and Temporary Aircrew Cards (TACs) should not be access-enabled to avoid short-cutting the proper vetting processes.

Another part of our anti-counterfeit strategy is to link ASICs/MSICs to biometric data, in much the same way as employed in Parliamentary passes and e-Passports. In addition to mitigating security vulnerabilities, biometric links underpin our long-term advocacy for expedited entry to our workplaces. The current arrangements are highly inefficient and we believe unnecessarily contributing to congestion at public security screening points.

In a 2016 submission to Senate Regional Affairs and Transport References Committee Inquiry into Airport and Aviation Security[3] with which AFAP agreed, AIPA stated:

> In making these observations, AIPA is not indicating any lack of support for security screening per se. We are strongly supportive of risk-based screening and also of advanced technology solutions that are designed to detect those who act to avoid detection and the things they seek to bring into the secure areas or onto the aircraft.
>
> However, we wish to be crystal clear that repetitive screening of flight crew and the repetitive mini-power-plays by screeners serves absolutely no useful security or safety purpose. It is an entirely remote risk that a flight crew member carrying a pair of nail clippers, a Leatherman or even a pair of knitting needles is going to unlawfully interfere with the aircraft using those things in preference to the full range of control options available in the cockpit. The original decision (confirmed by OTS) to force flight crew through normal screening was solely for the purposes of public display and nothing else. It is noteworthy that this Australian stance is considerably stricter than that applied to flight crew in the US, despite the US previously having a significantly greater aviation security risk.
>
> Apart from a complete lack of leadership to undo that decision, no one has actually costed the efficiency deficit that attends every decision that adds time and distance to preflight preparation and there is little responsibility taken by any decision-makers within the system for the additional stress placed on flight crew when screening incidents occur unnecessarily – both of which AIPA considers as potential sources of human error incidents.
>
> One other concern that we have is in regard to the creation of a choke point in passenger movement at the screening points. While we have no doubt that the risk planners in OTS, the AFP and in ASIO will have carefully considered the changes in people density throughout terminal areas, It seems to us in AIPA that many check-in areas and security screening queues regularly create largely stagnant masses of people who are held close to the open front side of terminals with little freedom of movement. This is particularly the case in older terminals where the designs were formulated for vastly different movement patterns and occupation densities.

Currently, being in possession of a valid ASIC means nothing in this ludicrous public relations screening parody. Instituting 'front of the queue' or flight crew priority lanes is a Band-Aid enhancement that is not always well received by members of the public who at best are entirely uninterested in whether the flight crew are subjected to the same screening processes.

AusALPA believes that Australia's aviation security arrangements have consistently failed to properly distinguish the risk profile and role that flight crew play in the aviation security space.

The security risk profile of pilots

Our members are the users of ASICs who, along with cabin crew, are the primary bearers of aviation security risk on a daily basis. We obviously share the risks with ground-based airport workers in between flights, but then take the risks into the air. While our

---

3 Submission 6, Senate Regional Affairs and Transport References Committee Inquiry into *Airport and Aviation Security*

passengers are exposed to similar hazards, their occasional rather than daily exposure greater reduces the risk.

Importantly, we are not random or casual users of the aviation system – we are the most frequent users as well as the most scrutinised and peer monitored group of people within the system. We are operationally risk-averse and highly security conscious – as the President of our US equivalent, the Airline Pilots Association, International (ALPA-I), recently reminded the Administrator of Transport Security Agency (TSA):

> As the Pilot in Command, we are the final arbiter of safety and security and we bring invaluable resources and expertise to the agency…

Currently, our risk profile and policy expertise is ignored by CISC in two significant ways: first, we are security-screened in exactly the same way as unknown members of the general public, and second, we are invited to participate in public exposure of policy discussions such as the current DP as if we are merely members of the general public.

AusALPA is strongly of the view that we are an important stakeholder in aviation security matters and need to be included in the policy design and implementation arrangements by CISC. Airlines generally do not speak for their pilots – they speak primarily for their shareholders – and AusALPA has a well-established track record of providing government with well-researched non-partisan policy advice.

If CISC wishes to be fully informed in terms of the practicality of policy design and implementation, AusALPA must be included in their development, not only as part of the "co-design" workshops but more generally.

Had we been so, perhaps much more efficient and practical outcomes could be achieved other than forcing flight crew through public security screening.

ASIC-dependent expedited crew access

Australia's flight crews are not the same risk as unknown members of the general public. Unlike cabin crew, pilots need not ordinarily access the aircraft via the normal passenger access routes – in multi-level terminals, the most efficient access is via the ground handling access points. At most of our major airports, the current public security display process adds significant time and distance to flight access, resulting in significant lost time in fatigue-limited windows for operating flights.

A robust secure database that allows secure facility access to be tied to verified identity cards with biometric links will provide the opportunity to revamp the system into one that reflects the known risk profiles of ASIC holders and permits, with safeguards, an expedited crew access (ECA) system that relies on enhanced crew processing.

There is considerable experience with ECA systems in the US, where the Known Crewmember (KCM) system was established as a partnership between the TSA, ALPA-I and the airlines. The KCM system is currently subject to review in response to a very small number of rule breaches for criminal purposes, but has no known breaches of security. AusALPA sees that KCM experience as the sound basis for us to design and implement a better system here in Australia that meets safety, security and policing requirements.

In terms of allocating scarce resources to the security task, greater ASIC integrity reinforces the opportunity to reduce the security effort unnecessarily consumed in providing secure access for flight crew and reducing the added time and distance currently wasted in accessing their place of work.

Our position

AusALPA fully supports strengthening the integrity of ASICs/MSICs.

Access to security-controlled areas should only be permitted by using a suitably encoded ASIC/MSIC. The card ideally should incorporate biometric data.

AusALPA should be included by CISC as a competent stakeholder in policy design and implementation forums, including but not limited to the "co-design" workshops.

CISC should as a matter of urgency introduce an ECA system and abandon the current farce of treating flightcrew members as if they represent the same risk as unknown members of the general public.

We look forward to further engagement with CISC in aviation security.

Yours sincerely,

Captain Louise Pole
President AusALPA
President AFAP

Captain Tony Lucas
Vice President AusALPA
President AIPA

Tel: 61 – 2 – 8307 7777
Fax: 61 – 2 – 8307 7799

Email: office@ausalpa.org.au
government.regulatory@aipa.org.au
technical@afap.org.au