Australian Government

Department of Infrastructure and Regional Development

SUBMISSION FROM

THE DEPARTMENT OF INFRASTRUCTURE AND REGIONAL DEVELOPMENT

TO THE

PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

INQUIRY INTO THE INTEGRITY OF AUSTRALIA'S BORDER ARRANGEMENTS

May 2015

Transport security and border integrity

1. The Department regulates the security of the Australian maritime and aviation transport industries through its administration of the *Aviation Transport Security Act 2004* (the ATSA) and associated Aviation Transport Security Regulations 2005 (the ATSR), and the *Maritime Transport and Offshore Facilities Security Act 2003* (the MTOFSA) and associated Maritime Transport and Offshore Facilities Security Regulations 2003 (the MTOFSR).

2. The purpose of this legislation is to establish a regulatory framework to safeguard against unlawful interference with civil aviation, maritime transport or offshore facilities, and meet Australia's associated international obligations.[1] Broadly this can be interpreted as maintaining and improving transport security in accordance with international standards and practices. While it provides for the regulation of Australia's major maritime and aviation border ports, the focus of the legislation is on preventing activities which threaten the safety or security of an aircraft/vessel and/or its passengers; or put the safe operation of a port, or the safety or security of any person at a port at risk. The legislation does not address criminality.

3. The ATSA and MTOFSA provide the framework for preventive security in the aviation and maritime transport industries, and the associated regulations set out the mandated minimum standards for industry to meet in their operations. Consequently, the Department is responsible for administering the legislation while regulated aviation and maritime transport operators (such as airport and airline operators and offshore facility and ship operators) are responsible for delivering security on a day-to-day basis. This recognises the aviation and maritime industries have specialist capability and expertise to effectively manage key infrastructure securely, which is not available within the Government. As a result, industry and the Department are responsible for ensuring that staff and contractors are appropriately trained and authorised to undertake any specific security roles and responsibilities as needed under the ATSA and MTOFSA.

4. In practice, this means that many of the physical security measures that are obvious to a traveller departing Australia's borders, such as security screening and access controls to secure areas, are managed by the relevant regulated industry participant. The Department does not have a permanent presence at any international port; instead, the Department oversees compliance through a regular programme of inspections, audits and other activities.

5. Where non-compliance is identified there are a range of responses that the Department can take, proportionate to the particular non-compliance or pattern of non-compliance. These range from administrative tools, such as the issuing of non-compliance notices, to fines and criminal prosecutions. Depending on the nature of the non-compliance, these may be applied to individuals or organisations.

6. The transport security framework recognises the important role that Commonwealth officers undertake to safeguard Australia's international seaports and airports. The ATSA and MTOFSA both provide police officers on duty at ports, and certain Customs officers, with special authority to:

    *   stop and search people, vehicles, aircraft and vessels in maritime security zones or at security controlled airports, and people on security regulated vessels and aircraft;

    *   remove people from ships, aircraft, maritime security zones or airports if they do not leave when requested to do so; and

    *   remove vehicles and vessels from airports and maritime security zones if an officer is unable to have the vehicles or vessels removed by persons in control of them.

---

[1] Set out in the Convention on International Civil Aviation (the Chicago Convention) and the International Convention for the Safety of Life at Sea (the SOLAS Convention).

Security identification cards and background checks

7. In addition to physical security measures and screening, the integrity of secure zones is supported by the Aviation and Maritime Security Identification Card (ASIC and MSIC) schemes. The schemes are designed to ensure people who regularly access secure areas of Australia's security controlled airports and seaports undergo background checks. Access control is the responsibility of the airport or seaport operator. The cards demonstrate the holder has passed a background check.

8. To be eligible for an ASIC or an MSIC a person must have an operational need to access a secure area or work in a security sensitive position (e.g. screening officers, airport security guards, check-in staff, baggage handlers and eligible Customs Officers) and successfully pass background checks every two years. The checks include a national security assessment by ASIO, criminal history check by Crimtrac, and, for foreign nationals, an immigration check.

9. These checks are useful in countering the threat to security systems posed by 'trusted insiders' – employees in a position to exploit a security system to conduct or enable an act of unlawful interference. This might include a radicalised employee acting directly; or an employee providing access or information for a range of reasons that enables others to bypass security measures.

10. A network of regulated issuing bodies (private and public sector) is responsible for confirming an applicant's identity and operational need, and applying for a background check − coordinated by AusCheck, a division of the Attorney-General's Department. The establishment of an applicant's identity at this stage is critical to ensuring persons with intent to interfere with aviation or maritime transport do not acquire a false identity by fraudulent means.

11. The cards themselves include a photograph of the holder, the name of the holder, expiry date, a unique identifier number, and a security feature in the form of a tamper-evident Kinegram® Hot Stamped Patch Optically Variable Device.

Strengthening the ASIC and MSIC schemes

12. The Government is committed to reducing criminal influence at airports and sea ports and has agreed to a forward plan to strengthen the ASIC and MSIC schemes. This includes:

   - tightening the eligibility criteria to ensure people who have committed serious criminal offences do not obtain an ASIC or MSIC;

   - ensuring AFP and Customs officers have adequate powers to enforce the appropriate use of ASICs and MSICs; and

   - examining the potential to use biometric technology to strengthen identity verification.

13. This work is being undertaken in conjunction with the Attorney-General's Department, and in close consultation with law enforcement and border security agencies.

14. To mitigate risks associated with the current issuing body arrangements, and to align ID-proofing processes with best practice, the Department is currently developing regulatory amendments to ensure that ASIC and MSIC documentation requirements comply with the National Identity Proofing Guidelines issued by the Attorney-General's Department in late 2014. This will include amendments to require:

   - All ASIC and MSIC applicants to present in-person to an issuing body; and

   - identification documents to be sighted by the issuing body for each application.

An efficient, safe and secure transport sector

15. An efficient, safe and secure international transport system is integral to Australia's social and economic well-being. The Department takes an active and forward looking approach to transport security regulation, constantly reflecting on what Government knows about security threats to ensure that Australia's transport security system is fit for purpose and security measures are targeted towards the areas of highest risk.

16. No system can be completely fail-safe, particularly where elements of it rely on human judgment and skill. It is also not practical to try to future-proof the maritime and aviation transport sectors by seeking to mitigate all known vulnerabilities, regardless of how negligible a risk they pose. Were the Government to do this, it would make international trade and travel uneconomic. Furthermore, it is likely that even with an over-investment in security those with the intent and capability could still potentially identify and exploit vulnerabilities.

17. The Department will continue to work closely with the international community, other government agencies and industry to ensure that Australia's system remains responsive to new and emerging threats at Australia's borders, and can continue to cope with the expected growth in both the international aviation and international maritime transport sectors.