EXECUTIVE MINUTE

on

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
REPORT No. 447

EPBC Act, Cyber Security, Mail Screening, ABR and Helicopter Program: Review of Auditor-General's Reports Nos. 32 to 54 (2013 - 14)

General comments

The Australian Border Force (formerly Australian Customs and Border Protection Service) undertakes a risk based approach to targeting and screening international mail. Work is currently underway to implement a sampling program to enhance our targeting and screening capabilities in this environment.

Response to the recommendation(s)

Recommendation No.2

The Committee recommends that the Department of Agriculture and Water Resources and the Australian Customs and Border Protection Service review international methods in screening international mail to ensure Australia responds to international best practice and report results of that analysis to the Joint Committee of Public Accounts and Audit.

Response

Countries target different risks in international mail and apply a variety of screening models based on their own operating arrangements and logistical constraints. While international mail is a challenging environment due to the absence of electronic data, the Australian Border Force (ABF) works collaboratively with stakeholders, including other Commonwealth Government Departments and international Customs administrations to develop and enhance risk assessment methodologies. We liaise with our counterparts through a number of networks, such as the World Customs Organisation to exchange information, contribute to new initiatives, and participate in co-ordinated joint enforcement efforts. An example of this is Operation SKY-NET II, commencing in November 2015, which aims to strengthen relationships between international administrations and enhance capability in combating the trafficking of drugs and other contraband products through postal and express courier channels.

In support of this recommendation, the ABF is working closely with the Department of Agriculture and Water Resources to adopt a consistent approach to screening international mail at the border. The ABF is currently implementing a mail sampling program in line with the Department of Agriculture and Water Resources's methodology. This will provide opportunities to streamline risk assessment practices and provide additional data to assist in analysing the effectiveness of our screening processes. Following the completion of a three month trial, it is anticipated that this program will be rolled out nationally.

The Tackling Crime initiative announced by the Government in January 2014 provided additional funding for the ABF to increase screening of international mail. In 2014-15, the ABF inspected approximately 50 million international mail items. The focus on increased screening will continue to be a priority for the ABF in 2015-16. Increased screening has resulted in an increase of detections of illicit drugs, tobacco, firearms (including parts and accessories) and undeclared currency.

The National Tripartite Forum provides a formal mechanism for regular communication between the ABF, DIBP, Department of Agriculture and Water Resources and Australia Post. The forum is a decision making body responsible for ensuring that inbound international mail operations are carried out in accordance with each agency's policy. The forum also acts as a conduit between the three agency's national and regional operations. The function of the forum is to maintain a whole of Government policy approach to processing inbound international mail. The forum is also responsible for consideration of policy making on strategic and operational matters relating to ensure efficiency and national effectiveness.

The Department continues to work closely with our international partners. As part of our engagement with New Zealand Customs Service, the ABF will share international mail screening information on a reciprocal basis to explore opportunities for improvement in this sector.

IBM has been working with the Department and Australia Post to put forward a strategy for improving disruption of illicit goods in the international mail environment. This strategy focuses on:

- Cohesive data collection
- Automation screening and image analytics
- Sampling and targeting

This response has been developed in consultation with the Department of Agriculture and Water Resources.

Recommendation No.3
The Committee recommends that the Australian Customs and Border Protection Service report to the Joint Committee of Public Accounts and Audit no later than six months after the tabling of the report on the:

- existing state of cooperative arrangements with other countries regarding identification of illicit firearms shipments
- what discussions/negotiations are underway with other countries to strengthen existing arrangements

Response
The Department of Immigration and Border Protection seeks to work closely with international partners, including on firearms matters, to detect and respond to reports of illegal activity in the border environment. The Department has well established processes to identify and treat the risk of illegal firearms importations through all streams, including international mail. Among these processes are regular intelligence exchange with international partners and domestic law enforcement stakeholders.

The former Australian Customs and Border Protection Service established a Firearms Intelligence and Targeting Team in 2012 which has evolved to become the Firearms and Weapons Section (FaWS) within the new Department. Where appropriate, intelligence is actioned though joint activity between FaWS and Australian Border Force officers working at international gateways across Australia.

The Department continues to explore new agreements to share relevant detection data with our international partners. As an example, the Department has recently agreed to participate in an intelligence sharing arrangement specifically focused on the sharing of firearms detection data relating to importations from one of the participant's countries. The FaWS is actively engaged with Interpol and Europol over a range of operational and intelligence matters. FaWS consults with Interpol concerning the tracing of detected whole firearms and identifiable frames, receivers, parts and accessories (those with serial numbers) through Interpol's iARMS system. Through the AFP the FaWS regularly engages with Europol on targeting the international trafficking in small arms, particularly in international mail (referred to by Europol as fast parcels).

The Department agrees to this recommendation and will report relevant information that does not compromise operational activity or arrangements with other countries.

On 22 January 2014, the Government announced additional funding as part of the Tackling Crime Measures. The Department received funding to increase screening targets for high risk illicit cargo and international mail including firearms. The funding also provided additional equipment, new technology, and additional ABF officers to undertake screening of cargo, provide tactical analysis support and additional investigations capability. A number of initiatives have been implemented to enhance capability to detect firearms and firearm parts in cargo and international mail, including:

- The introduction of x-ray image analyst testing;
- Extension of the libraries available to image analysts around firearms and firearm parts; and
- And other enhancements of x-ray capability including comprehensive testing and training through organisations such as the United States Bureau of Alcohol, Tobacco Firearms and Explosives.

These initiatives have enhanced the capability of ABF officers to identify firearm markings, parts and components, and the methods that can be used by organised crime to conceal illicit importations of firearms.

The Department engages in a variety of operational activities with B5 partners that address illegal firearms importations and is constantly identifying new opportunities for collaboration.

Recommendation No.8
The Committee recommends that the seven agencies audited by the ANAO achieve full compliance with the top four mitigation strategies and related controls in the Information Security Manual as soon as possible. Further:

- each agency should produce a clear and detailed plan of necessary activities, including a definitive date of compliance
- agencies that do not expect to achieve full compliance before august 2015 should notify the Committee – the Committee may then seek an explanation of why full compliance is not expected to be achieved as well as the mitigation strategies the agency has put in place

Response
Since the last reporting period in August 2014 there has been a consolidation of security functions from both Immigration and Australian Customs and Border Protection Service as part of the establishment of the new Department of Immigration and Border Protection which includes the Australian Border Force. In support of the new Department, a newly created Security Branch has undertaken a number of activities including:

- The establishment of a Portfolio wide Vulnerability Management Board (VMB) which validates, recommends and records strategies to monitor and/or remediate any identified vulnerabilities to assist the Portfolio in its role in maintaining a secure information environment. The membership of the VMB includes all Information Communication Technology (ICT) external service providers, Departmental ICT and Security representatives.
- As part of the Portfolio Reform activities, a New Policy Proposal funded Cyber Integrity programme of work is currently being undertaken to achieve a broad range of capability enhancements for security policy, protective and cyber security, and identity access management functions.
- Establishing dedicated project resources for a top four project which is specifically targeted at compliance across the Department. Early work includes technical and policy enforcement of compliance.

The Cyber Integrity programmed which is funded over the next four years will seek to continuously improve and enhance the Department's security posture. It has an established security programme plan which identifies full compliance through the development of enterprise work processes and technology that will build enduring cyber integrity capability.

The expected milestone for completion of the four mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' is 30 June 2016. This will establish processes to maintain ongoing compliance with application whitelisting which builds on the existing mechanisms and policies that have already delivered compliance with operating system patching, application patching and privileged administration.

Michael Pezzullo
Secretary
Department of Immigration and Border Protection