Australian Government
Australian Customs and Border Protection Service

SUBMISSION BY THE

AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE

TO THE

REVIEW OF THE FREEDOM OF INFORMATION ACT 1982

AND THE

AUSTRALIAN INFORMATION COMMISSIONER ACT 2010.

INTRODUCTION

This submission is provided by the Australian Customs and Border Protection Service (hereafter 'Customs and Border Protection') in relation to the *Review of the Freedom of Information Act 1982 and the Australian Information Commissioner Act 2010* being conducted by Dr. Allan Hawke AC from October 2012 and which is subject to a report to the Commonwealth Attorney General by 30 April 2013.

Customs and Border Protection welcomes the opportunity to make a submission to the review and will primarily focus on the following term of reference:

> *(d) the reformulation of the exemptions in the FOI Act, including the application of the new public interest, taking into account:*
>
> > *(i) the requirement to ensure the legitimate protection of sensitive government documents including Cabinet documents; and*
> >
> > *(ii) the necessity for the government to continue to obtain frank and fearless advice from agencies and from third parties who deal with government;*

EXECUTIVE SUMMARY

The current exemptions within *the Freedom of Information Act 1982* (FOI Act) relied upon by law enforcement agencies (particularly ss. 37, 38, 45) do not specifically provide a framework which recognises the present and emerging developments in the collection, analysis, use and disclosure of intelligence material which provides a foundation of risk based intelligence activities by law enforcement.

Fiscal responsibility and limited resources increasingly require that law enforcement agencies use intelligence based systems to ensure that resources are efficiently applied in the detection and prevention of unlawful activity as well as in the investigation and prosecution of offenders. Operating within such an environment also requires a strategy of employing sophisticated analytical techniques and having access to information and intelligence from a variety of sources.

There is a need to recognise intelligence related activities within the law enforcement exemptions to strengthen the protection of truly sensitive information that if released, would undermine these activities. In addition, in order to clarify the sensitivities surrounding particular intelligence information and the possible implications of its release, a specific framework for providing adequate time to consult other Commonwealth law enforcement agencies should to be included within the FOI Act.

Based on the above, Customs and Border Protection recommends for consideration:

Recommendation 1:

The s.37 exemption should be extended to include the following:

> *A document is an exempt document if its disclosure under this Act would, or could reasonably be expected to:*
>
> (ab) *prejudice the conduct of surveillance activities, intelligence gathering activities and intelligence analysis for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law or the proper administration of the law.*

Recommendation 2:

A provision for an extension of time be inserted in the legislation to allow for interagency consultation, perhaps similar to the extension that could be used under s. 26A for consulting State and Territory agencies.

***

INTELLIGENCE RELATED ACTIVITIES

Customs and Border Protection operates similarly to the Australian Federal Police and Australian Crime Commission as a law enforcement agency making extensive use of information and intelligence that it gathers itself or sources from other domestic and foreign agencies and the community and employs sophisticated analytical techniques to identify persons of interest and breaches of the law.

Given the significant and increasing dependency on intelligence and information based systems for effective law enforcement and regulatory action, it is extremely important that the practical application of the FOI Act limits the ability of criminal elements to access surveillance or monitoring information, intelligence gathered or analytical products developed and so allow the avoidance of detection or law enforcement action.

There is also a need to ensure that in obtaining information and intelligence from a range of foreign law enforcement agencies, that the latter can have confidence that any material supplied will be protected from potential release under the FOI Act. To a certain degree that information can be protected on the basis that it is supplied on a confidential basis (s. 45) or disclosure could damage international relations (s.33 (1)(a)). However, given that further intelligence collection or analysis or other action may be taken domestically following receipt of material provided from overseas, it is desirable to remember foreign sourced material when considering the protection of intelligence material generally.

Customs and Border Protection considers that although certain exemptions exist within the FOI Act which can be applied by law enforcement agencies in particular circumstances, those exemptions have their limitations in practice and there may be a need to consider appropriate solutions.

Recently, the amendments in relation to the privacy legislation highlighted aspects of law enforcement activities that may need to be recognised within the current law enforcement exemption under the FOI Act (section 37). This will ensure that the two regimes are consistent in their approach and adequately protect the integrity of law enforcement activities and the collection and analysis of intelligence information.

Please note that:

- The Privacy Amendment (Enhanced Privacy Protection) Bill 2012 which passed both Houses of the Commonwealth Parliament on 29 November 2012 will, following Royal Assent, progressively amend the *Privacy Act 1988*. This includes the proposed Australian Privacy Principles (APP) which will come into effect 15 months after Royal Assent.

- The APPs will address a range of circumstances in which the public interest in maintaining individual privacy is balanced against other public interests, including that of law enforcement agencies to safeguard the community and to investigate and prosecute offenders. The legislation explicitly recognises law enforcement concerns through two strands, the first being the identification of particular agencies within the

definition of "enforcement bodies" (Note: Customs and Border Protection is listed as such a body in the legislation along with the Australian Federal Police, Australian Crime Commission and certain other agencies) and the second is ensuring that an "APP entity" (defined as an agency or organisation – see Schedule 1 Item 6) could use and disclose personal information for "enforcement related activities" (See Schedule 1, Item 20).

Under APP 6.2(e) an APP entity can use or disclose personal information in the following circumstance:

> *(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.*

The legislation defines "enforcement related activity" as:

> *(a) the prevention, detection, investigation, prosecution or punishment of:*
> *(i) criminal offences; or*
> *(ii) breaches of a law imposing a penalty or sanction; or*
> *(b) the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or*
> *(c) the conduct of protective or custodial activities; or*
> *(d) the enforcement of laws relating to the confiscation of the proceeds of crime; or*
> *(e) the protection of the public revenue; or*
> *(f) the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or*
> *(g) the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.*

On becoming law, APP 6.2(e) will ensure that law enforcement bodies (as defined in the Privacy Act) will continue to receive personal information for their functions from organisations and Government agencies in the community. The key to the provision is that there must be a basis of reasonableness before the information can be used or disclosed for the relevant enforcement related activities.

The "enforcement related activities" as defined in the amending legislation identify a core of law enforcement activities most of which may arguably be regarded as covered by existing exemptions under the FOI Act. The one exception is paragraph (b) "*the conduct of surveillance activities, intelligence gathering activities or monitoring activities"* which depending on the circumstances, may or may not fall within the exemption at s. 37 of the FOI Act that concerns 'documents affecting enforcement of law and public safety'.

The closest exemptions arising in that context include:

s. 37(1)(a) –

> *A document is an exempt document if its disclosure under this Act would, or could reasonably be expected to:*

(a) prejudice the conduct of an investigation of a breach, or possible breach, of the law, or a failure, or possible failure, to comply with a law relating to taxation or prejudice the enforcement or proper administration of the law in a particular instance;

s.37 (2) (b) -

A document is an exempt document if its disclosure under this Act would, or could reasonably be expected to:

(b) disclose lawful methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those methods or procedures;

s. 47E(d) -

A document is conditionally exempt if its disclosure under this Act would, or could reasonably be expected to, do any of the following:

(d) have a substantial adverse effect on the proper and efficient conduct of the operations of an agency.

While the methodologies used by Customs and Border Protection in surveillance, intelligence gathering or analysis may be appropriately addressed under the existing s. 37(2)(b), it is arguable that documents generated or created as a consequence of those activities especially where an investigation has not yet commenced may not fall within s.37(1)(a).

Surveillance and monitoring activities may arise within the context of a formal investigation in which there are suspected offenders and identified offences, but it may also occur in situations involving the detection or prevention of an offence being committed where the information available might not support a formal investigation at that stage or before a clear identification of offenders or offences. Further, information or intelligence that is available to law enforcement may require comprehensive analysis before offending behaviour is capable of being detected. In those circumstances, it seems likely that an exemption under s. 37(1) (a) would not be available to safeguard surveillance or monitoring records or intelligence material more generally.

The conditional exemption at s. 47E(d) may be available in certain circumstances where it can be shown that a disclosure would or could have a *substantial adverse effect* on operations, but this may not reach to every situation involving sensitive intelligence material or analytical product. Where particular methodologies could also be revealed and that is undesirable, then this exemption might be used in combination with s. 37(2)(b), but there is no certainty for law enforcement as to whether intelligence material or analytical product can necessarily be exempted.

Given the increasing reliance of law enforcement on the development of sophisticated intelligence gathering and analytical capabilities as well as the requirement for interagency

information sharing (including the obtaining of information or intelligence from foreign agencies) it is essential that this be recognised through a robust exemption in the context of s. 37. If agencies, especially those of foreign countries, came to the conclusion that particular intelligence information was likely to be accessible through an FOI application, this would have a chilling effect on information sharing arrangements. Such arrangements are based on trusting that information will be secure and not widely disclosed.

Another related area of concern is that Customs and Border Protection often receive FOI requests from journalists after a major maritime search and rescue incident. This is despite any media releases that may be made that provide information on the incident. At the time of considering the FOI requests (even some weeks later) it may not fully be known whether the circumstances will result in criminal investigations or coronial inquiries and in these circumstances the s. 37 exemption may be difficult to apply notwithstanding the importance of not releasing certain information to the public at that time.

It is recommended that the s.37 exemptions be extended to include a new exemption:

> *A document is an exempt document if its disclosure under this Act would, or could reasonably be expected to:*
>
> (ab) *prejudice the conduct of surveillance activities, intelligence gathering activities and intelligence analysis for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law or the proper administration of the law.*

If such an exemption is made available, it is considered that surveillance and monitoring activity preliminary to a decision to investigate could be included within its terms without further amendment. An exemption would also provide some needed certainty in relation to intelligence material and analytical product which may have been collected in the past and become dated, but which could still have relevance to present or future operations. The obligation on an agency of demonstrating the relevant prejudice would be a safeguard in ensuring that there are reasonable grounds for seeking to withhold particular documents.

A framework for consultation

Under s. 25 of the FOI Act, an agency may in certain circumstances give a "*notice in writing to the applicant that the agency or the Minister, as the case may be, neither confirms nor denies the existence, as a document of the agency or an official document of the Minister, of such a document but that, assuming the existence of such a document, it would be an exempt document under section 33 or subsection 37(1)…*". In practice, a tension exists in applying this provision in that an applicant may be able to discern whether or not a document exists by making multiple applications for the same document from different agencies and analysing their separate responses or otherwise by being aware that it is likely that if the document existed this would be confirmed by an exemption being claimed.

While a complete solution to this problem may be difficult to achieve, ensuring appropriate inter-agency consultation goes some way to ensuring there is an understanding of the possible effect of disclosure, to ensure consistent responses and to identify whether other agencies' functions or activities (such as ongoing investigations or the identification of an intelligence interest) could be prejudiced by a particular response to an FOI application. Consultation may

also be important to identify whether particular information which may at first appear innocuous has significance to organised criminal elements, for example, the timing of when the agency became aware of certain information or whether release of a document could potentially point to the source of information.

Inter-agency consultations are time consuming for those involved and significantly increase workloads, but it is a necessary part of ensuring the security of law enforcement information and intelligence and the appropriate processing of FOI requests. Unfortunately, given the significant volume of documents held by law enforcement agencies for which an FOI request may be made, most if not all of the 30 days processing time may be used with reduced opportunity for adequate consultation.

At present, there appears to be no framework for an extension of time beyond the statutory 30 days processing period to ensure that potentially affected agencies are properly consulted.

It is recommended that a provision for an extension of time to allow for interagency consultation, perhaps similar to the extension that could be used under s. 26A for consulting State and Territory agencies, be included in the legislation.

The significance of law enforcement activities in the public interest would justify such an extension being available to those agencies that may need to apply s. 33 or 37 exemptions. It would also assist in providing a more consistent approach in neither confirming nor denying the existence of a document under s.25.

Conclusion

In making these recommendations Customs and Border Protection does not intend to disturb the existing exemptions or mechanisms under the FOI Act, but simply to improve the practical application of the current legislation.

The future development of intelligence systems within law enforcement is heavily dependent on the legislative structures that concern freedom of information and privacy. The recommendations made in this submission recognise the need for transparency and accountability, while seeking to ensure that there is continuing protection for intelligence related activities which are so essential for the security of the community and the enforcement of the law.

* * *

AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE

JANUARY 2013