Australian Government
Department of Agriculture

Ref: CI2012/00010

Anna Harmer
Assistant Secretary, Electronic Surveillance Policy Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Department of Agriculture seeking 'Enforcement Agency' Status

Dear Assistant Secretary Harmer

I am writing in response to an email dated 27 May 2015 advising changes to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), which are likely to affect the ability of the (Commonwealth) Department of Agriculture (the department) to access historical telecommunications data. The Guidance Note (the note) attached to that email states *'From 13 October 2015 any agencies wanting ongoing access to historical telecommunications data must be listed as an 'enforcement agency', unless already listed as a 'criminal law enforcement agency' in section 110A of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.'*

The department is not a *'criminal law-enforcement agency'* under section 110A of the Data Retention Act. The department is defined as a *'law enforcement agency'* under to section 5(1) of the *Law Enforcement Integrity Commissioner Act 2006 (LEIC Act).*

The department has a clear operational need to maintain effective law enforcement functions under portfolio legislation with respect to investigating possible breaches of portfolio legislation. Section 176A of the Data Retention Act provides that the Attorney-General may declare a body or authority to be an enforcement agency.

I therefore request that the department be declared as an 'enforcement agency', in accordance with the provisions contained under Section 176A of the Data Retention Act.

The department's Enforcement Section is responsible for the investigative and enforcement actions associated with the department's portfolio legislation. In support of Enforcement Section's role, the department gathers intelligence about crime to support the investigative and prosecution functions. The department's Fraud and Security Section is responsible for conducting investigations into fraudulent and corrupt behaviour of departmental staff, and regularly conducts activities jointly with the Australian Commission for Law Enforcement Integrity (ACLEI) and the Australian Federal Police.

The subsections that follow list considerations the Attorney-General must have regard to.

Subsection 176A(3B): The departmental functions include enforcement of criminal law

In response to paragraphs 7 and 12(a) of the note, the department is responsible for administering a variety of Commonwealth legislation relating to the biosecurity of Australia and the agricultural industry as a whole. The department's portfolio legislation includes: *Quarantine Act 1908, Imported Food Control Act 1992, Export Control Act 1982, Australian Meat and Live-stock Industry Act 1997* and the *Illegal Logging Prohibition Act 2012* and subordinate legislation. At times it is applicable to use other Commonwealth legislation including the *Criminal Code Act 1995.*

The legislation, regulations and proclamations made under these Acts contain serious indictable offences and contain a range of criminal penalty provisions, as well as administrative sanctions. Provisions available to the courts range from small fines to significant fines of up to 10,000 penalty units, as well as imprisonment of up to 10 years. Each of the Acts administered by the department has one or more offences that attract imprisonment terms in excess of two years, and so are by definition serious offences.

Prescribed departmental staff members are subject to the LEIC Act. The department's inclusion within ACLEI's jurisdiction has seen an increase in the complexity of criminal investigations undertaken by the department or jointly with ACLEI. The fraud and corruption related offences investigated by the Fraud and Security Section are contained in either the *Criminal Code Act 1995* or the *Crimes Act 1914.* Penalty provisions available to the courts include terms of imprisonment of more than three years and so are by definition serious Commonwealth offences.

Subsection 176A(4)(b): Authorisation would be reasonably likely to assist the authority in performing those functions

In response to paragraph 8(a) of the note, the historical use by the department of telecommunications data obtained under Section 178 of the TIA Act has included s 22 irrelevant

On average, the department receives around 700 reports per year relating to non-compliance with portfolio legislation. Of these, an average of 85 investigations are open at any time.

These requests are undertaken in response to major cases where all other investigative options have been exhausted. Since January 2011, the department has made 318 requests in relation to 76 investigations. Of these, ten significant investigations account for 64 percent of all requests. These cases range from large illegal importation investigations through to high profile live animal export investigations. Information obtained under the TIA Act allowed the department to identify individuals suspected of committing offences and individuals that may have assisted in the offences.

In response to paragraph 12(c) of the note, an example in which telecommunications data has been used is during Operation s 22 irrelevant. This action

constituted the offence of basic illegal importation under section 67(1) of the *Quarantine Act 1908*. This offence is punishable by 10 years imprisonment and/or a fine of 2000 penalty units. s 22 Irrelevant Without the use of this IMEI association and location data, this offender would likely not have been identified.

Another example is Operation s 22 Irrelevant Without the availability of this data obtained under the TIA Act, this investigation would have been unable to support the prosecution of this transnational smuggling syndicate through other investigative means.

In a separate matter, telecommunications data was used to identified and prosecute a company and director involved in a widespread smuggling network operating within the s 22 Irrelevant This led to the successful prosecution of the company and director resulting in a $55000 fine for the company and a two and half year custodial sentence for the director. This also supported the prosecutions of a number of other entities identified during this operation and helped the department counter a significant threat to the biosecurity of Australia.

In response to paragraph 12(b) of the note, the department would have been unable to obtain the information used in the above examples without access to historical telecommunications data. No other data holdings or repositories held the relevant data to identify and prove the communication of suspected criminal entities. Without this information, the enforcement activities would not have been successful and through evidence obtained and supported by telecommunications data, the criminal behaviours would have continued.

The increasing complexity and seriousness of criminal investigations undertaken by the Fraud and Security Section is likely to warrant the department requiring access to historical telecommunications data.

Subsection 176A(4)(c): compliance with the Australian Privacy Principles

In response to paragraphs 8(b) and 31 of the note, as an Australian Government agency, the department is required to adhere to the Australian Privacy Principles when dealing with information obtained under the TIA Act. In accordance with the Australian Privacy Principles, any request for disclosure of information under the TIA Act is subject to a rigorous approval process to ensure that it is reasonably necessary for the enforcement of criminal law. The request for disclosure must only be made in relation to a current investigation into a serious offence, and other avenues must have been exhausted. Approval is required from two employees at the Director level before I, as one of two delegates, approve the request for disclosure.

Information currently held by the department is limited to officers of the Enforcement Section, Compliance Division. The information is stored in an encrypted, access controlled and logged case management system, which is subject to auditing. All members of the Enforcement Section have a minimum baseline security clearance, and are made aware of their obligations in relation to the *Privacy Act 1988* and the Australian Privacy Principles through mandatory training.

Subsection 176A (4)(d): processes and practices to ensure compliance with obligations
In response to paragraphs 8(b) and 31 of the note, the department has in place processes and practices that ensure its compliance to the obligations of an enforcement agency under Chapter 4 of the TIA Act. This includes quarterly audits by the department's Fraud and Security Section as well as quarterly audit activity by the Attorney-General's Department.

Subsection 176A (4)(e): Public Interest
In response to paragraphs 36 and 37 of the note, the department's Enforcement Section is responsible for the investigative and enforcement actions associated with the department's portfolio legislation. The failure to effectively fulfil this role would have significant consequences for the Australian economy, the environment and public health. The *Quarantine Act 1908* in particular seeks to prevent the introduction of exotic diseases and pests into Australia. Without access to historical telecommunications data, the delay in enforcement activities undertaken by the department would be unreasonable and unjustifiable to the public and would impose unnecessary resource constraints on other agencies.

A failure of the Australian biosecurity system could have a significant impact on the economic interests of the country. It is estimated that an outbreak of foot and mouth disease, for example, would cost Australia up to $52 billion over a decade in lost revenue due to lost trade, particularly in the export environment. An historical example was the suspected illegal importation of live pigeons or pigeon eggs, which led to an outbreak of avian paramyxovirus, and subsequent disruptions to trade in the Australian poultry industry.

In response to paragraph 12(d) of the note, this department's nominated contact officer is myself.

Yours sincerely

s 22 irrelevant

Wayne Terpstra
Assistant Secretary
Targeting and Enforcement Branch
Compliance Division

5 June 2015

Australian Government
Department of Agriculture
and Water Resources

Your Ref: 15/5524

Ms Katherine Jones
Deputy Secretary – National Security and Criminal Justice
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Department of Agriculture and Water Resources – *'Enforcement agency'* status under the *Telecommunications (Interception and Access) Act 1979*

Dear Ms Jones,

Thank you for your letter dated 16 March 2016 concerning recent changes to the 'enforcement agency' status of the Department of Agriculture and Water Resources (department). These changes provide that the department no longer has access to telecommunications information and in your letter you suggest we seek access through other agencies.

I am writing to you to seek reconsideration of your decision given a recent report of the Parliamentary Joint Committee which recommends that the department be declared an enforcement agency.

The department was an *enforcement agency* under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) until 13 October 2015, when amendments to the law pursuant to the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, concerning agencies access to historical telecommunications data (metadata), took effect.

The department is not a *criminal law-enforcement agency* under section 110A of the TIA Act, and has petitioned the Attorney-General's Department since June 2015 seeking *enforcement agency* status under the TIA Act. The department's advice to the Attorney-General's Department of 5 June 2015 (copy attached), in support of seeking *enforcement agency* designation, sets out in detail the department's clear operational need to access metadata.

On advice from the Attorney-General's Department, the department has considered other methods of obtaining metadata using statutory coercive powers under portfolio legislation and by engaging the Australian Federal Police (AFP) to obtain metadata. The department has received preliminary legal advice as to the merits of using coercive powers, which suggests that the approach is problematic due to the construction of portfolio legislation. Advice received from the AFP indicates that it does not have the resourcing, compliance or risk considerations to obtain metadata on behalf of other agencies, including the department.

Australian Commission for Law Enforcement Integrity (ACLEI)

The department is defined as a *law enforcement agency* under section 5(1) of the *Law Enforcement Integrity Commissioner Act 2006* (LEIC Act), and since 2013, certain aspects of the department's border-related operations have been subject to ACLEI's jurisdiction. The Parliamentary Joint Committee's report on ACLEI of 5 May 2016 (copy attached) states that

'under current arrangements, the Law Enforcement Integrity Commissioner Regulations provide for the inclusion of certain departmental staff, all of whom are connected to certain functions relating to the cargo control systems'.

ACLEI has supported the inclusion of the entire department within its jurisdiction. The Integrity Commissioner argued that while the department is identified primarily as a policy and program delivery agency, there has been a significant strategic shift in risks within the department's operating environment. Serious organised criminal interest places the department's working profile much more into the law enforcement space. Its biosecurity functions make it vulnerable to law enforcement corruption risks across the entire agency.

The committee's report states the committee acknowledged that at face value, unlike Commonwealth bodies such as the AFP and the Australian Crime Commission, the department 'is not a typical law enforcement agency'. The department has 'some very important law enforcement functions that contribute to the security of Australia's borders. These include its screening for biosecurity risks and cargo management responsibilities at Australia's international airports and seaports. It was as a result of these important responsibilities that in mid-2013 the department's portfolio was partially included within ACLEI's jurisdiction'.

The report continues 'the committee is persuaded that it is preferable to have the entire Department of Agriculture and Water Resources included within ACLEI's jurisdiction'. Accordingly, in its report, the committee recommended the government amend the LEIC Act, to include the entire department within ACLEI's jurisdiction.

Further to this ACLEI has also recommended to the department that it s 22 irrelevant

In light of the committee's statements and formal recommendation to incorporate the department within ACLEI's jurisdiction, I request that the Attorney-General's Department reconsider its previous position and declare the department an *enforcement agency*, in accordance with the provisions contained under section 176A of the TIA Act.

Yours sincerely

s 22 irrelevant

Lyn O'Connell
Deputy Secretary
Department of Agriculture and Water Resources

10 June 2016

Attachments

1. Letter to Attorney General's Department, 5 June 2015
2. Parliamentary Joint Committee's report on ACLEI

Attachments: 2015-07-02 Portfolio Legislation and Offence Provision Overview.docx
2015-07-02 Offence provisions under the Biosecurity Act 2015.docx
2015-07-02 Prosecution Outcomes.docx
2015-07-02 Section 186A - Obligation to keep records.docx
2015-07-02 OGC Consolidated offence provisions table.xlsx

From: Terpstra, Wayne
Sent: Thursday, 2 July 2015 5:37 PM
To: s 22 irrelevant
Cc: s 22 irrelevant ; s 22 irrelevant ; Vivian, Raelene; Luscombe, Kerrie-Anne
Subject: FW: Applications for ongoing access to telecommunications data - Department of Agriculture ~~[DLM=For Official Use Only]~~

Dear s 22 irrelevant

Thank you for email of 1 July 2015 requesting further information from the Department of Agriculture (department) in support of the department's application to obtain ongoing access to telecommunications data.

You requested further information in relation to specific sections and penalties imposed by the department's legislation. Please see attached document *Portfolio Legislation and Offence Provision Overview* which outlines common offences and penalties (and how they may be applied) under the department's portfolio and associated Commonwealth legislation. Also attached is a document *Prosecution Outcomes* showing successful prosecution outcomes prosecuted under department's portfolio legislation. On 16 June 2015, the *Biosecurity Act 2015* and supporting legislation received royal assent. The new legislation will commence on 16 June 2016. Within the new legislation there are approximately 88 identified offences relating to criminal and civil matters. Please see attached *Offence Provisions under the Biosecurity Act 2015*.

Examples of some of the penalties relating to these offences are:

- Section 185 (5) – Fault based offence involving harm to the environment or economic consequences – Penalty: 10 years imprisonment or 600 penalty units, or both
- Section 186 (2) – Basic fault-based offence – Penalty: 5 years imprisonment or 300 penalty units, or both
- Section 186 (3) – Civil penalty provision – 120 penalty units
- Section 186 (4) - Fault based offence involving obtaining commercial advantage – Penalty: 10 years imprisonment or 2,000 penalty units, or both

You also requested further details in relation to whether the department has alternative methods to progress investigations instead of accessing telecommunications data. The department seeks to safeguard Australia's animal and plant health status to maintain overseas markets and protect the economy and environment from the impact of exotic pests and diseases, through risk assessment, inspection and certification and the implementation of emergency response arrangements for Australian agricultural, food and fibre industries. To achieve the department's mission, Enforcement Section undertakes investigative and

enforcement actions associated with the department's portfolio legislation.

Without access to historical telecommunications data, the delay in enforcement activities undertaken by the department may impact the department's ability to fulfil its obligation to safeguard Australia's animal, plant and human health status. The inability to efficiently undertake these responsibilities may be seriously detrimental to the public and the broader Australian economy. Apart from investigations into alleged criminal activity the department also has monitoring warrant powers under various portfolio legislation. The department uses these powers to determine if (for example) quarantine risk is present and to determine if quarantine requirements have been satisfied. Monitoring warrant powers are a fundamental tool used by the department to avoid and manage risk. As an example, research by the Australian Bureau of Agricultural and Resource Economics and Sciences (ABARES), indicates the cost of an FMD outbreak in Australia would be more than $52 billion to our economy over the course of 10 years.

There have been occasions where the department has required urgent telecommunication data to support an application for a monitoring warrant. Similarly there have been occasions where the department has required urgent telecommunication data to support investigations into alleged serious criminal activity and applications for evidentiary search warrants. To seek assistance from another 'Law Enforcement' agency (e.g. Australian Federal Police) to request telecommunication data on our behalf would have an impact on urgent investigations and search warrant activity, undermining the criticality of the information available to the departments enforcement officers and this would impose additional resource constraints on those other agencies.

On 2 July 2015, the department contacted the AFP AOCC – Client Liaison Team to enquire about the process of requesting telecommunications data on its behalf should it be unable to maintain ongoing access. Although the AFP indicated some ability and a general willingness to assist, they would require further consultation with their legal team in order to be able to provide detail about the conditions of releasing the information to the department. The department holds grave concerns about its ability to gain access to required data in emergency situations if it were obliged to seek it through a third party agency with its own priorities and a lack of timely understanding around the departments import mission and priorities.

Finally, you asked the department to observe that if the department obtains ongoing access to telecommunications data, it will be subject to additional record-keeping and oversight requirements. Notwithstanding that the department already has in place rigid guidelines and procedures that detail how requests and records are approved, processed, retained and reported upon and that the department conducts quarterly audits designed to ensure the integrity of the process, the department acknowledges that it is aware of and undertakes to adhere to the ***Obligation to keep records*** requirements set out under Section 186A of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.*

Please contact me again should you require any additional information.

Regards,

Wayne

Wayne Terpstra
Assistant Secretary | Targeting & Enforcement | Compliance Division

s 22 Irrelevant

Department of Agriculture
18 Marcus Clarke Street, Canberra ACT 2601 Australia
GPO Box 858 Canberra ACT 2601 Australia

Australian Government
Department of Agriculture

From: s 22 Irrelevant
Sent: Wednesday, 1 July 2015 3:28 PM
To: Terpstra, Wayne
Subject: Applications for ongoing access to telecommunications data - Department of Agriculture ~~[DLM=For Official Use Only]~~

~~For Official Use Only~~

Dear Wayne

As discussed, AGD is currently assessing the application from the Department of Agriculture (the Department) to obtain ongoing access to telecommunications data.

I would be grateful if you would provide responses to the questions below so AGD can progress the application.

I understand that the Department administers offences under the Quarantine Act 1908, Imported Food Control Act 1992, Export Control Act 1982, Australian Meat and Livestock Industry Act 1997, Illegal Logging Prohibition Act 2012 and the Criminal Code 1995. Grateful if you would provide further details in relation to:

- specific sections and penalties imposed by the legislation, and
- whether the Department has alternative methods to progress the investigation instead of accessing telecommunications data

If the Department obtains ongoing access to telecommunications data, it will be subject to additional record-keeping and oversight requirements. Further information about these requirements can be found here. Please provide an undertaking that the Department is aware of these requirements and intends to comply with them. We ask that such an undertaking be made by an individual who has the authority to bind the Department.

Thank you for your assistance in this matter, I would appreciate if you would provide your response by **COB Thursday 2 July 2015.** Do not hesitate to contact me if you wish to discuss your application further.

Kind regards

s 22 irrelevant **Legal Officer**
Electronic Surveillance Policy Branch
Attorney-General's Department |3-5 National Circuit |Barton ACT 2600
✉ s 22 irrelevant

Australian Government
Attorney-General's Department
