Australian Government
Department of Immigration and Border Protection

4 August 2017

In reply please quote:
FOI Request FA 16/11/00189-R1
File Number ADF2016/65920

Mr Ben Fairless
Sent via email: foi+request-2550-0b3ef691@righttoknow.org.au

Dear Mr Fairless

Freedom of Information request – decision on internal review

This letter refers to your application for an internal review under section 54 of the *Freedom of Information Act 1982* (FOI Act) received by the Department of Immigration and Border Protection (the Department) on 11 December 2016.

On 2 December 2016, Mr [redacted] of the FOI Section, decided to refuse access to documents in accordance with section 47E(d) [Substantial adverse effect on the proper and efficient conduct of the operations of an agency] of the FOI Act. The decision you received related to your request for access to:

> *'1) A copy of the most current configuration settings for janusSEAL. This is an off the shelf product being used by DIBP to classify emails. janusSEAL allows the department to correctly classify emails in line with the Australian Government security classification system.* **[Item 1]**
>
> *2) A copy of any correspondence in the last 3 years sent to all DIBP staff in relation to janusSEAL. This may not reference the product by name, but may be a notification sent across the agency or training piece on how to correctly classify emails, or, for example, what will happen if you try to send an email classified as FOUO, PROTECTED or SECRET to a non .gov.au email address.'* **[Item 2]**

In your internal review application, you provided the following contentions:

> *'…The above information would provide the details of how the software is configured and contain parameters on how end-users interact with the software.*
>
> *… if the information would be harmful to the Department, perhaps they should seek advice from the manufacturer of the product, or from their in-house technical expertise.*
>
> *On the Public Interest Test, I contend that there is significant public interest in understanding how multiple members in the Department have caused classified emails to be sent outside of the agency.'*

Background
I note your internal review decision was due on 10 January 2017, and on 13 January 2017 I contacted you by email to inform you that your decision had been delayed to allow the relevant internal business areas to provide additional advice in relation to your review application. I appreciate your patience in this matter.

Scope of internal review
As you did not raise any contentions in relation to **Item 2** of your request, I have limited the scope of the internal review decision to **Item 1**, **Document 3**, [the document] of your FOI request.

Information considered
In reaching my decision, I have considered the following:

- the terms of your original request and your contentions raised in your internal review
- the *Freedom of Information Act 1982;*
- the Australian Information Commissioner's guidelines; and
- consultation with the relevant business areas.

Decision
I am an officer authorised under section 23 of the FOI Act to make internal review decisions in respect of requests to access documents or to amend or annotate Departmental records.

In relation to Item 2 of your request, I have decided to vary the original decision and to release additional material contained within the **Document 3**. I consider the remaining material is exempt in accordance with the following sections of the FOI Act:

- 47E(d) [Substantial adverse effect on the proper and efficient conduct of the operations of an agency].

Section 22(1)(a)(ii) – Access to edited copies with irrelevant matter deleted
Section 22(1)(a)(ii) allows an agency to delete irrelevant material from a document which is only partially relevant to an applicant's FOI request. I find that some information contained within **Document 3** is material which is irrelevant to your FOI request. I have withheld or deleted that material accordingly. I provide an edited copy of the document to you in accordance with section 22(2) of the FOI Act.

Section 47E(d) –Operations of the agency
Section 47E(d) provides that documents are conditionally exempt if disclosure would, or could, reasonably be expected to have a substantial adverse effect on the proper and efficient conduct of the operations of an agency.

I have considered whether the information contained in **Document 3** is conditionally exempt on the basis that disclosure could result in a substantial adverse effect on the proper and efficient conduct on the security operations of the Department's information technology (IT) systems under section 47E(d) of the FOI Act.

As part of the internal review, I consulted with the relevant business areas within the Department in relation to the configuration summary listed as highlighted in **Document 3** [the document].

Advice received from officers from the Information Communications Technology Division and the Integrity, Security and Assurance Division confirms that **Document 3** contains technical data describing the production environment registry settings which are security controls specific to the Department.

The business area's advice is that the broader policy settings for the JanusSeal product are standard settings required for an Australian Government Department where systems are rated to a 'Protected' security classification. IE: These settings do not apply to material which is unclassified. Further information about the policy definitions as they relate to the broader Australian Government Security Classification System can be found at: https://www.protectivesecurity.gov.au/informationsecurity/Pages/AustralianGovernmentSecurityClassificationSystem.aspx

Consultation responses from the Security and Assurance Division provided additional background information in connection with the document; being:

> *'…Detailed device configurations not only provide information regarding the operating parameters of specific devices, they also give clues as to the architecture and operation of associated systems. For this reason* the Department does not *release specific device configurations unless they have undergone a level of sanitisation and de identification…'*

I note that whilst this document, in isolation, is seemingly innocuous, this information together with other information about the Department's IT systems, may lead to an ability to infiltrate the Department's IT systems now or in the future.

Further advice obtained from the business area notes:

> *'…the release of the configuration details in itself may not cause significant harm, however, releasing this information to the public could cause considerable harm if used with other information about the department's systems…'*

Mosaic theory
In evaluating potential harmful effects of disclosing the configuration summary information, and the information in the document that would affect the security of the Department's internal operations, I have considered the intelligence technique known as the 'mosaic theory'. This theory holds that individual pieces of information, when combined with other pieces, can generate a harmful composite, - a mosaic, that can damage the operations of an agency.

It is important to note that when assessing the potential harm in releasing a document, a decision maker will consider the content of the document in question. However when evaluating the potential harmful effects of disclosing documents that affect the Commonwealth, decision makers may also take into account the 'mosaic theory'.

As such, I consider that to release further information in **Document 3**, would allow a malicious third party to gather further information on the Department's network configuration, which is not publicly available. This would facilitate an attempt to bypass existing security controls, compromising the Department's data.

Further, the configuration summary contained within the document is specific and sensitive information which is strictly limited to certain people authorised to access it. The Department has an obligation to keep such information confidential, not only to protect its own information, but the information and records that the Department retains on behalf of individuals, businesses, other government agencies and international governments.
I considered these factors relevant in forming my decision to exempt the remaining material in accordance with section 47E(d) of the FOI Act.

In summary, disclosure of the exempt material could reasonably lead to the adverse effect on the security controls of the Department's IT systems. I find this adverse effect to be serious and not insubstantial. I find that these documents are conditionally exempt in part under section 47E(d) of the FOI Act. Nonetheless I must give access to the documents *unless*, in the circumstances, access at this time would on balance, be contrary to the public interest.

Public interest
Conditionally exempt matter must be released unless, in the circumstances, access to that document at this time would, on balance, be contrary to the public interest (section 11A(5) of the FOI Act). I have considered the factors favouring access and factors that are irrelevant in subsections 11B(3) and (4).

Factors in favour of disclosure
In balancing the public interest in this case, I have considered the following factors in favour of disclosure:

- disclosure would promote the objects of the FOI Act

Factors against disclosure
I have considered the following factors against disclosure:

- the need to preserve reasonably held expectations of confidentiality
- does not allow a person access to his or her own personal information

Finding on the public interest
I have considered your contentions in relation to the public interest, specifically you raised:

> *'…On the Public Interest Test, I contend that there is significant public interest in understanding how multiple members in the Department have caused classified emails to be sent outside of the agency.'*

I have also noted your comments and contentions in relation to allegations of an unauthorised release of emails. I consider that release of the configuration settings of JanusSeal is not in the public interest as release would not inform public debate. Further, the security configuration settings provide additional defence that; in- depth disclosure would weaken the Department's security posture.

I acknowledge that there is a public interest in ensuring the Department undertakes its functions in a transparent and proper manner, and that there is also a public interest in maintaining confidentiality of some material contained in the document. In this case, I have formed the view that the disclosure of the configuration summary information will make a negligible contribution to the factor in favour of disclosure. While I accept that may be some public interest relating to an allegation of disclosure of Departmental emails, which I note do not form part of the scope of my internal review decision, in contrast there is minimal public interest in the disclosure of the JanusSeal product configuration information.

I have considered the Department's Protective Security Policy Framework (PSPF), which includes information security management policies. The PSPF ensures that:

- all official information is safeguarded to ensure its confidentiality, integrity, and availability by applying safeguards so that:
  - only authorised people, using approved processes, access information
  - information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
  - information is classified and labelled as required.

- all information created, stored, processed, or transmitted in or over government information and communication technology (ICT) systems is properly managed and protected throughout all phases of a system's life cycle, in accordance with the protocols and guidelines set out in the PSPF, which includes the Australian Government Information Security Manual, produced by the Australian Signals Directorate.

In addition I have considered the material in the Information Security Manual (ISM) for the Commonwealth.

The ISM notes, if information of the nature related to the configuration settings of the JanusSeal were to be released into the public arena, such unscrupulous individuals could use these configurations to craft targeted cyber intrusions, or even facilitate access into potentially more valuable commercial systems.

The incentives for, and capability to conduct, malicious activity in cyberspace will be enhanced by a combination of observed trends; in this day of online activity, motivation is increasing. Australia's increasing reliance on the Internet is leading to more high–value information being stored and communicated on Australian government and commercial networks. This is boosting the incentive to undertake cyber-crime or exploitation for direct monetary profit or indirect economic and political advantage. As such, capability is easier to acquire.

Acquiring a cyber capability is becoming easier with increasingly sophisticated tools, information, and guidance readily available online. New technologies will generate new vulnerabilities. The proliferation of new technologies will increase the number of potential vulnerabilities. The spectrum of malicious activities is increasing, and the ease of acquiring a cyber capability coupled with the potential high gains—whether financial, economic, diplomatic or political—is enticing more activity into malicious cyber activity.

I therefore consider and note, it is important for the Department to be able to successfully protect our networks from an increasingly sophisticated and persistent cyber threat. As such, I consider that in relation to this exemption, I have taken into account the same factors in favour and against disclosure, and accordingly, based on the above findings, I have concluded that disclosure of the material would, on balance, be contrary to the public interest and that parts of the document are exempt under section 47E(d) of the FOI Act.

Review rights
You may apply directly to the Office of the Australian Information Commissioner (OAIC) for a review of my decision. You must apply in writing within 60 days of this notice. For further information about your review rights and how to submit a review request to the OAIC, please see FOI fact sheet 12 '*Freedom of information – Your review right*s', available online at www.oaic.gov.au .

How to make a complaint about the handling of your FOI request
You may complain to the Australian Information Commissioner if you have concerns about how the Department has handled your request under the FOI Act. Information about how to submit a complaint is available at www.oaic.gov.au .

Contacting the FOI Section
If you wish to discuss this matter, I can be contacted using the details provided below.

Legislation
A copy of the FOI Act is available at https://www.legislation.gov.au/Series/C2004A02562. If you are unable to access the legislation through this website, please contact our office for a copy.

Yours sincerely

[redacted]

Karen Tulloch
Assistant Director FOI
Authorised decision maker
Freedom of Information Section
Department of Immigration and Border Protection
Email foi.reviews@border.gov.au

Attachments
- ✓ Attachment A - **Document 3**