Dear [Name],

1. I refer to your email, dated 27 July, 2011, in which you requested access, under the Freedom of Information Act 1982 (FOI Act), to documents relating to cyber security incidents. By email, dated 10 August 2011, you were provided with a statement regarding cyber security incidents, outside of the FOI Act. On 9 September 2011, you advised that you wished to proceed with your FOI request.

2. After consultation between our office and you, by email, dated 27 September 2011, you advised that you wished to proceed with the following revised scope:

"A digital copy of the spreadsheet from the ADFCIRT Incident Report Database showing all entries for Cyber Security Incidents, excluding policy violations, from 1 July 2010 to 27 September 2011."

3. The purpose of this letter is to provide you with the decision relating to the document that is the subject of your request.

FOI decision maker

4. Air Commodore N. Barneveld, Commander Defence Strategic Communications is the authorised decision maker, under the FOI Act, in relation to your request.

Documents identified

5. Air Commodore Barneveld identified one document, being an excel spreadsheet produced from the Australian Defence Force Cyber Incident Response Team (ADFCIRT) database, which matches the scope of your request.
Decision

6. Air Commodore Barneveld has decided to release the identified document with deletions, in accordance with section 22 [access to edited copies with exempt or irrelevant matter deleted] of the FOI Act, as the deleted material is considered exempt under section 33(a)(i) [documents affecting national security of the Commonwealth] of the FOI Act.

7. Copies of relevant sections of the FOI Act are at Enclosure 1.

Material taken into account

8. In coming to his decision, Air Commodore Barneveld had regard to:
   - the content of the document in issue
   - relevant provisions in the FOI Act
   - the guidelines published by the Office of the Australian Information Commissioner under section 93A of the FOI Act (the guidelines)

Exemptions claims – Section 33 of the FOI Act

9. Air Commodore Barneveld found that the identified document contained information on how a cyber security incident was detected, when it was detected, and what actions were taken to ensure the Defence Information Environment (DIE) remains secure. Air Commodore Barneveld considers that the information contained in the database, if disclosed, could provide key information on how to compromise the DIE.

10. Air Commodore Barneveld noted that he is mindful that most of the information entered into the database is classified and that the identified document is classified at the ‘SECRET’ level. However, he has also taken into account the guidelines, in particular paragraph 5.23 which states that the classification markings on a document (such as ‘secret’ or ‘confidential’) are not of themselves conclusive of whether the exemption applies...

11. Air Commodore Barneveld considered that the columns titled ‘date/time created’ and ‘incident name’ on the identified document, if disclosed, could reasonably be expected to cause damage to the security of the Commonwealth. The guidelines state there must be ‘real’ and ‘substantial’ grounds for expecting the damage to occur which can be supported by evidence or reasoning. The ADFCIRT provides regular statistics from this database for the purpose of senate estimates, ministerial briefings and media enquiries which he considers broadly informs the general public on this matter. However, to provide details of such events/incidents could lessen the effectiveness of Defence systems as it would enable individuals to cross reference details of this database against malicious activity they may have conducted, which would enable them to determine how attacks were being detected and if any of their respective attacks were detected or not. Air Commodore Barneveld considers that this demonstrates the damage which could occur from disclosure.

12. Further, Air Commodore Barneveld has taken into consideration that the guidelines, at paragraph 5.26(b) state that the term ‘security’ refers to the security of any communications system or cryptographic system of any country used for defence or the conduct of the Commonwealth’s international relations.
13. In light of the above, Air Commodore Barneveld considered that the columns titled ‘date/time created’ and ‘incident name’ on the identified document are exempt under section 33 of the FOI Act. He has decided to de-classify the document and release it with the exempt material removed.

Payment of Charges

14. In our letter dated 30 September 2011, the department estimated the cost associated with processing your request to be [REDACTED]. You agreed to pay charges for the administration of your request and paid the estimated charge in full on 13 October 2011.

15. Upon completion of your request, the actual amount for processing your request was calculated to be [REDACTED]. However, as explained in our above mentioned letter the amount payable can only be more than the preliminary assessment if the decision is to release all of the documents requested in full.

16. Taking the above into consideration, you are not required to pay any further processing charges in relation to this request.

17. A copy of the document in the form approved for release is at Enclosure 2.

Rights of review


Further advice

19. Should you have any questions in regard to this matter please contact me directly on (07) 3332 6359. Alternatively, the FOI team can be contacted on the details at the top of this letter.

Yours sincerely,

Theresa Stinson
Assistant Director – Media Case Management
Freedom of Information

10 November 2011

Enclosures:
1. Relevant sections of the FOI Act
2. Document in form approved for release