Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Daryl Quinlivan
Secretary
Department of Agriculture and Water Resources
18 Marcus Clarke Street
CANBERRA CITY ACT 2600

Dear Mr Quinlivan

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Chris Moraitis
Secretary
Attorney General's Department
3-5 National Circuit
BARTON ACT 2600

Dear Mr Moraitis

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Mike Mrdak
Secretary
Department of Communications and the Arts
2 Phillip Law Street
CANBERRA ACT 2601

Dear Mr Mrdak

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Greg Moriarty
Secretary
Department of Defence
Russell Offices, R1-5-Sec's Suite
CANBERRA ACT 2600

Dear Mr Moriarty

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Dr Michele Bruniges
Secretary
Department of Education and Training
Level 11 Executive, 50 Marcus Clarke Street
CANBERRA ACT 2600

Dear Dr Bruniges

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Ms Kerri Hartland
Secretary
Department of Employment
Level 3, 12 Mort Street
CANBERRA ACT 2601

Dear Ms Hartland

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Finn Pratt
Secretary
Department of the Environment and Energy
John Gorton Building, King Edward Terrace
PARKES ACT 2600

Dear Mr Pratt

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Ms Rosemary Huxtable
Secretary
Department of Finance
1 Canberra Avenue
FORREST ACT 2603

Dear Ms Huxtable

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Ms Frances Adamson
Secretary
Department of Foreign Affairs and Trade
R G Casey Building, John McEwen Crescent
BARTON ACT 2600

Dear Ms Adamson

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Ms Glenys Beauchamp
Secretary
Department of Health
Scarborough House, Atlantic Street
WODEN ACT 2606

Dear Ms Beauchamp

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Ms Renee Leon
Secretary
Department of Human Services
Doris Blackburn Building, 18 Canberra Avenue
FORREST ACT 2603

Dear Ms Leon

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Michael Pezzullo
Secretary
Department of Immigration and Border Protection
6 Chan Street
BELCONNEN ACT 2617

Dear Mr Pezzullo

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Dr Heather Smith
Secretary
Department of Industry, Innovation and Science
Level 13, Industry House
10 Binara Street
CANBERRA CITY ACT 2601

Dear Dr Smith

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Dr Steven Kennedy
Secretary
Department of Infrastructure
111 Alinga Street
CANBERRA ACT 2600

Dear Dr Kennedy

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Ms Kathryn Campbell
Secretary
Department of Social Services
Athlon Drive
TUGGERANONG ACT 2903

Dear Ms Campbell

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr John Fraser
Secretary
Department of the Treasury
Langton Crescent
PARKES ACT 2600

Dear Mr Fraser

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr Simon Lewis
Secretary
Department of Veterans Affairs
Gnabra Building, 21 Genge Street
CANBERRA CITY ACT 2601

Dear Mr Lewis

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017

Australian Government

Department of the Prime Minister and Cabinet

**SECRETARY**

**DR MARTIN PARKINSON AC PSM**

Mr John Lloyd
Australian Public Service Commissioner
B Block, Treasury Building
Parkes Place West
PARKES ACT 2600

Dear Mr Lloyd

You may be aware that the United States Government has recently banned the use of Kaspersky Labs software in its federal agencies. Last weekend, the Head of the United Kingdom's National Cyber Security Centre issued interim advice to permanent Secretaries, highlighting the risks of using foreign anti-virus products in their networks.

The Head of the Australian Cyber Security Centre (ACSC) and National Cyber Security Adviser, Alastair MacGibbon, has asked that I write to you regarding this issue.

These concerns from two of our closest allies, coupled with our understanding of the threat posed by foreign interference, mean we need to evaluate ICT supply chain risk in the Australian context.

For an anti-virus product to be effective, it must be highly intrusive within a network so it can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction. It is obvious why this matters in terms of our national information and systems security.

The general cyber security advice has not changed: it is the responsibility of each department and agency to ensure they are **constantly evaluating the risks** to the information they hold. This remains true for anti-virus software, network providers, hardware or any other ICT system.

Postal Address: PO BOX 6500, CANBERRA ACT 2600
Telephone: +61 2 6271 5200 Fax: +61 2 6271 5935 www.pmc.gov.au ABN: 18 108 001 191

However, in light of these recent announcements, I ask that you undertake an immediate risk assessment of the ICT products used in **your department and also your portfolio agencies**. I ask that this be done for all software and vendors, but with initial focus on anti-virus products and any vendors outside of our Five-Eyes partners.

In determining if a product is fit for purpose, I ask that departments and agencies simply consider whether or not they would be comfortable with the vendor's host country possibly having access to the information they hold. If the answer is no, then the product is not fit for purpose.

The Australian Security Intelligence Organisation and the Digital Transformation Agency are both aware of this request.

In light of the importance of this issue, I ask that you report back to me by **22 December 2017** detailing actions undertaken to mitigate the risk of foreign owned vendors in your systems.

If you require assistance, the National Cyber Security Adviser has established a small team within the ACSC, which can be contacted via s 22(1)(a)(ii) @pmc.gov.au

Yours sincerely

s 22(1)(a)(ii)

11 December 2017