

Skorupa, Jessica MISS

From: Media
Sent: Thursday, 12 October 2017 10:08 PM
To: s47F
Cc: Media
Subject: RE: Questions on contractor IT breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good evening s47F

Thank you for your enquiry.

Please attribute the below response to a Defence spokesperson rather than a named individual.

Obligations under the United States' International Traffic in Arms Regulations (ITAR) are a matter for the company and whomever it was sub-contracting to.

Defence reviews ITAR compliance on an ongoing basis and is in regular discussion with the United states on ITAR related matters.

All Defence contracts that involve classified material stipulate that the contractor must meet the requirements of Defence Security Policy. A security risk assessment must be undertaken as part of the planning process for all significant procurement activity.

Defence provides security support and advice to contractors through:

- the Defence Industry Security Program (DISP). A business, whether a prime contractor or subcontractor, is required to obtain and maintain membership of the Defence Industry Security Program when it will be accessing, handling or storing information across a spectrum of national security classifications. All Defence Industry Security Program members must comply with the security standards required by the Defence Security Manual, Australian Government Protective Security Policy Framework, and the Australian Government Information Security Manual.
- the Centre for Defence Industry Capability (CDIC); and
- the Australian Cyber Security Centre (ACSC).

In August 2017, the CDIC, Defence and ACSC delivered seven Defence Industry Security and Cyber Awareness Forums across Australia to provide contextual cyber security threats affecting Australia's defence industry. The forums provided information about preventative strategies and resources.

Kind regards,

Defence Media

Department of Defence | Russell Offices | PO Box 7909 Canberra BC ACT 2610
Phone: (02) 6127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

From: s47F
Sent: Thursday, 12 October 2017 12:23 PM
To: Media
Subject: Questions on contractor IT breach

Hi guys,

I have some questions on the data breach by a Defence contractor.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

Has it reviewed how Australian contractors generally maintain their ICT security?

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

Can I get answers by 5pm?

thanks,

--
s47F

Defence & National Security Correspondent

s47F

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: Media
Sent: Thursday, 12 October 2017 9:57 PM
To: Laube, Wade MR 1
Cc: Budd, Henry MR; Geering, John MR; Kelton, Alexandra MS; Fraser, Katherine MRS 1; Media
Subject: FW: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Hi Wade,

Are you happy with the below response?

Kind regards,

Sarah Collins

Public Affairs Officer | Corporate Communication

Ministerial Executive Co-ordination & Communication (MECC) Division

Department of Defence | Russell Offices | PO Box 7909 Canberra BC ACT 2610

Phone: (02) 6127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Geering, John MR
Sent: Thursday, 12 October 2017 9:54 PM
To: Media
Cc: Kelton, Alexandra MS; Fraser, Katherine MRS 1
Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

Sarah this is it, could u fwd to wade to quickly check, my phone isnt accessing the directory for some reason, then if he happy im happy for it to go john

Obligations under the United States' International Traffic in Arms Regulations (ITAR) are a matter for the company and whomever it was sub-contracting to.

Defence reviews ITAR compliance on an ongoing basis and is in regular discussion with the United States on ITAR related matters.

All Defence contracts that involve classified material stipulate that the contractor must meet the requirements of Defence Security Policy. A security risk assessment must be undertaken as part of the planning process for all significant procurement activity.

Defence provides security support and advice to contractors through:

- the Defence Industry Security Program (DISP). A business, whether a prime contractor or subcontractor, is required to obtain and maintain membership of the Defence Industry Security Program when it will be accessing, handling or storing information across a spectrum of national security classifications. All Defence Industry Security Program members must comply with the security standards required by the Defence Security Manual, Australian Government Protective Security Policy Framework, and the Australian Government Information Security Manual.
- the Centre for Defence Industry Capability (CDIC); and
- the Australian Cyber Security Centre (ACSC).

In August 2017, the CDIC, Defence and ACSC delivered seven Defence Industry Security and Cyber Awareness Forums across Australia to provide contextual cyber security threats affecting Australia's defence industry. The forums provided information about preventative strategies and resources.

Sent from my iPhone

On 12 Oct 2017, at 9:25 pm, Media <media@defence.gov.au> wrote:

UNCLASSIFIED

Thank you John

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Geering, John MR
Sent: Thursday, 12 October 2017 9:25 PM
To: Media
Cc: Kelton, Alexandra MS; Fraser, Katherine MRS 1
Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach
[SEC=UNCLASSIFIED]

Sarah ive agreed words with wade so once he clears we can go john

Sent from my iPhone

On 12 Oct 2017, at 8:37 pm, Media <media@defence.gov.au> wrote:

UNCLASSIFIED

Hi John,

OMINDEF have made some changes to the response (See below).

The original proposed response is attached.

Please advise if this is cleared to send.

Kind regards,

Sarah Collins

Public Affairs Officer | Corporate Communication

Ministerial Executive Co-ordination & Communication (MECC) Division

Department of Defence | Russell Offices | PO Box 7909 Canberra BC ACT 2610

Phone: (02) 6127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Laube, Wade MR 1

Sent: Thursday, 12 October 2017 8:33 PM

To: Tyrrell, Lauren MRS 1; Media

Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

The following is cleared by OMINDEF and OMINDP:

Obligations under the United States' International Traffic in Arms Regulations (ITAR) are a matter for the company and whomever it was sub-contracting to.

Defence reviews ITAR compliance on an ongoing basis and is in regular discussion with the United states on ITAR related matters.

All Defence contracts that involve classified material stipulate that the contractor must meet the requirements of Defence Security Policy. A security risk assessment must be undertaken as part of the planning process for all significant procurement activity.

Defence provides security support and advice to contractors through:

- the Defence Industry Security Program (DISP). A business, whether a prime contractor or subcontractor, is required to obtain and maintain membership of the Defence Industry Security Program when it will be accessing, handling or storing classified information. All Defence Industry Security Program members must comply with the security standards required by the Defence Security Manual, Australian Government Protective Security Policy Framework, and the Australian Government Information Security Manual.
- the Centre for Defence Industry Capability (CDIC); and
- the Australian Cyber Security Centre (ACSC).

In August 2017, the CDIC, Defence and ACSC delivered seven Defence Industry Security and Cyber Awareness Forums across Australia to provide contextual cyber security threats affecting Australia's defence industry. The forums provided information about preventative strategies and resources.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

<mime-attachment>

Skorupa, Jessica MISS

From: Media
Sent: Thursday, 12 October 2017 9:26 PM
To: Geering, John MR; Media
Cc: Kelton, Alexandra MS; Fraser, Katherine MRS 1
Subject: RE: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Thank you John

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Geering, John MR
Sent: Thursday, 12 October 2017 9:25 PM
To: Media
Cc: Kelton, Alexandra MS; Fraser, Katherine MRS 1
Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

Sarah ive agreed words with wade so once he clears we can go john

Sent from my iPhone

On 12 Oct 2017, at 8:37 pm, Media <media@defence.gov.au> wrote:

UNCLASSIFIED

Hi John,

OMINDEF have made some changes to the response (See below).

The original proposed response is attached.

Please advise if this is cleared to send.

Kind regards,

Sarah Collins

Public Affairs Officer | Corporate Communication
 Ministerial Executive Co-ordination & Communication (MECC) Division

Department of Defence | Russell Offices | PO Box 7908 Canberra BC ACT 2610
Phone: (02) 8127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Laube, Wade MR 1
Sent: Thursday, 12 October 2017 8:33 PM
To: Tyrrell, Lauren MRS 1; Media
Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

The following is cleared by OMINDEF and OMINDP:

Obligations under the United States' International Traffic in Arms Regulations (ITAR) are a matter for the company and whomever it was sub-contracting to.

Defence reviews ITAR compliance on an ongoing basis and is in regular discussion with the United States on ITAR related matters.

All Defence contracts that involve classified material stipulate that the contractor must meet the requirements of Defence Security Policy. A security risk assessment must be undertaken as part of the planning process for all significant procurement activity.

Defence provides security support and advice to contractors through:

- the Defence Industry Security Program (DISP). A business, whether a prime contractor or subcontractor, is required to obtain and maintain membership of the Defence Industry Security Program when it will be accessing, handling or storing classified information. All Defence Industry Security Program members must comply with the security standards required by the Defence Security Manual, Australian Government Protective Security Policy Framework, and the Australian Government Information Security Manual.
- the Centre for Defence Industry Capability (CDIC); and
- the Australian Cyber Security Centre (ACSC).

In August 2017, the CDIC, Defence and ACSC delivered seven Defence Industry Security and Cyber Awareness Forums across Australia to provide contextual cyber security threats affecting Australia's defence industry. The forums provided information about preventative strategies and resources.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: Zorzi, Adam MR
Sent: Friday, 13 October 2017 8:29 AM
To: Media
Cc: CIOG Media; Morgan, Lindsay MR 1; Masters, Amon MR; Thomas, Emma MS 4
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]
Attachments: CT - 002945 - Contractor IT breach CIOG input.doc

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good morning Defence Media,

Please find attached templated CIOG Response. Clearance below from AS ICTSB.

Kind regards,

Adam Zorzi | CIOG Communications

Commercial & Business Enablement
 Chief Information Officer Group | Department of Defence
 APW-05-062 | Anzac Park West | PO Box 7953 | Canberra BC | ACT 2610
 P: 02 614 44433

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Morgan, Lindsay MR 1
Sent: Friday, 13 October 2017 8:21 AM
To: Zorzi, Adam MR
Cc: Masters, Amon MR; Thomas, Emma MS 4; Keesing, Col MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Adam,

The coordinated responses provided yesterday, cleared by myself and Mr Pete West from DSVS is as below:

Defence provides security support and advice to contractors, primarily through the Defence Industry Security Program (DISP), to assist them meeting their obligations and the security expectations they are required to meet.

Defence provides security advice to contractors and suppliers on a regular basis, including support through the Centre for Defence Industry Capability and the Australian Cyber Security Centre.

Regards,

Lindsay

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Thomas, Emma MS 4
Sent: Friday, 13 October 2017 7:50 AM
To: Morgan, Lindsay MR 1
Cc: Zorzi, Adam MR; Masters, Amon MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Lindsay

Please see below.

Thank you

Kindest regards,

Em

Emma (Em) Thomas

Executive Assistant to, Lindsay Morgan

Assistant Secretary Information Communication Technology Security Branch, ASICTSB

Chief Information Officer Group

P: (02) 6144 4019 | E: emma.thomas4@defence.gov.au

A: APW-3-270, Anzac Park West, Constitution Avenue, Parkes ACT 2600

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Zorzi, Adam MR
Sent: Friday, 13 October 2017 7:47 AM
To: Masters, Amon MR
Cc: Thomas, Emma MS 4
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Amon,

Defence Media has come back requesting your responses be cleared by the appropriate Band 1. Would it be possible to have Lindsay provide clearance this morning?

Kind regards,

Adam Zorzi | CIOG Communications

Commercial & Business Enablement
Chief Information Officer Group | Department of Defence
APW-05-062 | Anzac Park West | PO Box 7953 | Canberra BC | ACT 2610
P: 02 614 44433

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Masters, Amon MR
Sent: Thursday, 12 October 2017 3:41 PM
To: Zorzi, Adam MR
Cc: Thomas, Emma MS 4; Keesing, Col MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Adam,

Steve Scanlan (DS&VS) has already responded to most of these....(see attached).

ICTSB responses below.

Has it reviewed how Australian contractors generally maintain their ICT security?

- Defence has a program in place to ensure industry partners adhere to protective security requirements.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- Defence has a program in place to provide appropriate guidance and support to both internal and external Defence stakeholders when an incident occurs that requires it.

Regards,

Amon Masters

Head of

Commercial & Business Enablement

Chief Information Officer Group | Department of Defence

APW-05-062 | Anzac Park West | PO Box 7953 | Canberra BC | ACT 2610

P: 02 614 44433

s22

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Thomas, Emma MS 4
Sent: Thursday, 12 October 2017 3:17 PM
To: Keesing, Col MR
Cc: Zorzi, Adam MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]
Importance: High

UNCLASSIFIED

Hi Col

In Lindsay's absence can you please answer Adams question IRT contractor IT breach?

Thank you

Kindest regards,

Em

Emma (Em) Thomas

Executive Assistant to, Lindsay Morgan

Assistant Secretary Information Communication Technology Security Branch, ASICTSB

Chief Information Officer Group

P: (02) 6144 4019 / E: emma.thomas4@defence.gov.au

A: APW-3-270, Anzac Park West, Constitution Avenue, Parkes ACT 2600

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Zorzi, Adam MR **On Behalf Of** CIOG Media
Sent: Thursday, 12 October 2017 3:17 PM
To: Thomas, Emma MS 4
Cc: Loane, Annie MS
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]
Importance: High

UNCLASSIFIED

Hi Emma and Annie,

Is this media enquiry one for us?

Kind regards,

Adam Zorzi | CIOG Communications

Commercial & Business Enablement
Chief Information Officer Group | Department of Defence
APW-05-062 | Anzac Park West | PO Box 7853 | Canberra BC | ACT 2610
P: 02 614 44433

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media

Sent: Thursday, 12 October 2017 3:10 PM

To: SP&I-SP-Exec; CIOG Media; [REDACTED] s7

Cc: Media

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon all,

FYSA- please see attached for your urgent attention and response.

DSVS has advised they are not best placed to respond and advise that Export control Branch, ASD, CIOG, ACSC and AG are best placed to provide a response.

The journalist has requested a response by 1700 today, I will manage his expectations.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Scanlan, Steven MR

Sent: Thursday, 12 October 2017 2:58 PM

To: Media; Chifley, Damien MR

Cc: West, Peter MR 2; Keesing, Col MR; [REDACTED] s7 Wong, Sam'; Wong, Sam MR; Wardle, Peter MR; Forth, John MR

Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Media

DS&VS is not best placed to respond to this Media enquiry as it largely relates to export controls. I have provided some guidance to assist in responding to this request including potential POCs. The content below is not cleared for public release.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfil those obligations?

- Export Controls Branch is best placed to answer this question (I understand that these are legal obligations)
- I understand the company in question was part of the Australia Community not the Defence Industry Security Program. DS&VS through Security Operations Branch provide support to this initiative under export controls direction (Peter Wardle and John Forth can advise if required).

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

- Export Control Branch is best placed to answer.

Has it reviewed how Australian contractors generally maintain their ICT security?

- CIOG, ASD or ACSC (and CERT in AGD) are best placed to answer. I would suggest that ACSC report that led to this query is an example of Defence constantly reviewing and providing advice to industry broadly on good cyber security such as the Top 4 and Essential 8.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- DS&VS is not aware of any general directive; however through our outreach and engagement the importance of good information security controls is emphasised in particular applying ASD recommended Essential 8.
- The CDIC play a role here (Sam Wong) – recent CDIC roadshow talking about good cyber security.
- ACSC play a role here s7
- CIOG play a role here (Col Keesing)

Kind regards
Steve

Steven Scanlan

A/g Assistant Secretary
Security Policy and Programs
Defence Security & Vetting Service
Department of Defence
t + 61 2 6266 3638 | e Steven.Scanlan@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Madge, Bronwyn MS
Sent: Thursday, 12 October 2017 1:50 PM
To: Scanlan, Steven MR
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Steve,

One for you.

Cheers,

Bronwyn

Bronwyn Madge | Director Vetting Governance and Review

a CP3-4-099

t 7 0133 e bronwyn.madge@defence.gov.au

HOURS 9.00am - 5.00pm Monday to Friday

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media

Sent: Thursday, 12 October 2017 1:48 PM

To: Madge, Bronwyn MS

Cc: Media

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Bronwyn,

Please see attached for your action, if it could be returned to MECC ASAP it would be greatly appreciated.

SP&I have advised this is best tasked to you for a response (see below).

Kind regards,

Sarah Collins | Public Affairs Officer

Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600

P: +61 2 6127 1999

E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:37 PM
To: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

I have also sent back the OpenText task with the comment below. SP is not the best placed to respond to the questions posed.

Regards,

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence
R1-01-A009 Russell Offices | PO Box 7801 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Chifley, Damien MR
Sent: Thursday, 12 October 2017 13:25
To: Holmback-Piggott, Louanne MS
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Louanne,

I think that this is best responded to by DSVS who run the Defence Industry Security Program and this is all related to things that were the subject of recommendations from the review conducted last year.

I think it was called the Defence Industry Security Review.

The best bet would be Peter West's branch.

Thanks

Damien

Damien Chifley
Director Defence Export Assessments and Regimes
Defence Export Controls Branch

Department of Defence R1-1-A037 PO Box 7910 Canberra BC ACT 2610
phone +61 2 626 51122 | mobile -s22 | email damien.chifley@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:16 PM
To: Chifley, Damien MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

See attached, let me know if you are going to take it on.

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence
R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 13:14
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please find attached the template for the below s47F enquiry.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999

E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:02 PM
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: FW: Questions on contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please see the below from s47F

I will template this up and send through for your action.

David has requested this by COB.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

From: s47F@fairfaxmedia.com.au
Sent: Thursday, 12 October 2017 12:23 PM
To: Media
Subject: Questions on contractor IT breach

Hi guys,

I have some questions on the data breach by a Defence contractor.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?
Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?
Has it reviewed how Australian contractors generally maintain their ICT security?
Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

Can I get answers by 5pm?

thanks,

s47F

Defence & National Security Correspondent

s47F

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Proposed MEDIA Response

Inquiry Number	CT-002945
Subject	Contractor IT breach
Contact Name	s47F [REDACTED]
Phone / Mobile / Email	
Organisation	Fairfax
Due to Defence Media	<p>12/10/2017</p> <p><i>Media queries need to be prioritised as urgent. Please contact Defence Media at least 24 hours prior to the deadline if it is not achievable.</i></p> <p><i>Extensions will only be granted in exceptional circumstances.</i></p>
Questions / Query	<p>I have some questions on the data breach by a Defence contractor.</p> <p>What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?</p> <p>Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?</p> <p>Has it reviewed how Australian contractors generally maintain their ICT security?</p> <p>Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?</p>
Background / Summary	<p><i>Please provide a brief background into the media topic/issue using the below questions as a guide.</i></p> <p><i>Focussing questions (delete upon entry)</i></p> <ul style="list-style-type: none"> ➤ <i>Is this information already in the public domain? If so, where?</i> ➤ <i>Has the media previously asked questions on this topic? If so, what was the response?</i> ➤ <i>Was this mentioned in Parliament or at senate estimates recently?</i> ➤ <i>Was this as a result of a policy decision or legislative change?</i> ➤ <i>Is this in relation to a recent incident that occurred in Australia or overseas?</i>

10/25/2017

	<p>➤ Have any of the groups or services seen this request? If so, what was their instruction?</p>
Proposed Response	<p>Defence provides security support and advice to contractors, primarily through the Defence Industry Security Program (DISP), to assist them meeting their obligations and the security expectations they are required to meet.</p> <p>Defence provides security advice to contractors and suppliers on a regular basis, including support through the Centre for Defence Industry Capability and the Australian Cyber Security Centre.</p>

Clearances

Clearance officers please ensure both date and time are detailed.

Drafted	Name	Appointment	Date and Time
Response Drafted by:	Amon Masters	Director Governance & Assurance	12/10/17 15:41

Clearance	Name	Appointment	Date and Time
Group/Service 1 Star or above	Lindsay Morgan	AS ICTSB	13/10/17 08:20
Strategic Communications Adviser	Adam Zorzi	Communications Advisor	13/10/17 08:25

Minister	Name	Appointment	Date and Time
Ministerial Consultation:: (To be completed by Defence Media)			

Skorupa, Jessica MISS

From: Media
Sent: Thursday, 12 October 2017 4:00 PM
To: Zorzi, Adam MR
Cc: Media
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Thank you Adam,

Could you please provide these answers in a template with appropriate clearances.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Zorzi, Adam MR
Sent: Thursday, 12 October 2017 3:58 PM
To: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Sarah,

Please see below advice from ICT Security Branch wrt to this enquiry.

Kind regards,

Adam Zorzi | CISO Communications

Commercial & Business Enablement

Chief Information Officer Group | Department of Defence
APW-05-052 | Anzac Park West | PO Box 7853 | Canberra BC | ACT 2610
P: 02 614 0443

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Masters, Amon MR
Sent: Thursday, 12 October 2017 3:41 PM
To: Zorzi, Adam MR
Cc: Thomas, Emma MS 4; Keesing, Col MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Adam,

Steve Scanlan (DS&VS) has already responded to most of these.

ICTSB responses below.

Has it reviewed how Australian contractors generally maintain their ICT security?

- Defence has a program in place to ensure industry partners adhere to protective security requirements.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- Defence has a program in place to provide appropriate guidance and support to both internal and external Defence stakeholders when an incident occurs that requires it.

Regards,

Amon Masters

Director

Overseas & Assistance

ICT Security Branch | Chief Information Officer Group | Department of Defence

0000 | APW-05-052 | Anzac Park West | Canberra Avenue | PO Box 7853 | ACT 2610

P: 02 614 0443 | s22 | 00000000000000000000

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Thomas, Emma MS 4
Sent: Thursday, 12 October 2017 3:17 PM
To: Keesing, Col MR
Cc: Zorzi, Adam MR

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]
Importance: High

UNCLASSIFIED

Hi Col

In Lindsay's absence can you please answer Adams question IRT contractor IT breach?

Thank you

Kindest regards,

Em

Emma (Em) Thomas

Executive Assistant to, Lindsay Morgan

Assistant Secretary Information Communication Technology Security Branch, ASICTSB

Chief Information Officer Group

P: (02) 6144 4019 | E: emma.thomas4@defence.gov.au

A: APW-3-270, Anzac Park West, Constitution Avenue, Parkes ACT 2600

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Zorzi, Adam MR **On Behalf Of** CIOG Media

Sent: Thursday, 12 October 2017 3:17 PM

To: Thomas, Emma MS 4

Cc: Loane, Annie MS

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

Importance: High

UNCLASSIFIED

Hi Emma and Annie,

Is this media enquiry one for us?

Kind regards,

Adam Zorzi | CIOG Communications

Commercial & Business Enablement

Chief Information Officer Group | Department of Defence

APW-05-062 | Anzac Park West | PO Box 7853 | Canberra BC | ACT 2610

P: 02 614 44433

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media

Sent: Thursday, 12 October 2017 3:10 PM

To: SP&I-SP-Exec; CIOG Media; s7

Cc: Media

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon all,

FYSA- please see attached for your urgent attention and response.

DSVS has advised they are not best placed to respond and advise that Export control Branch, ASD, CIOG, ACSC and AG are best placed to provide a response.

The journalist has requested a response by 1700 today, I will manage his expectations.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600

P: +61 2 6127 1929

E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Scanlan, Steven MR

Sent: Thursday, 12 October 2017 2:58 PM

To: Media; Chifley, Damien MR

Cc: West, Peter MR 2; Keesing, Col MR; s7 'Wong, Sam'; Wong, Sam MR; Wardle, Peter MR; Forth, John MR

Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Media

DS&VS is not best placed to respond to this Media enquiry as it largely relates to export controls. I have provided some guidance to assist in responding to this request including potential POCs.

The content below is not cleared for public release.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfil those obligations?

- Export Controls Branch is best placed to answer this question (I understand that these are legal obligations)
- I understand the company in question was part of the Australia Community not the Defence Industry Security Program. DS&VS through Security Operations Branch provide support to this initiative under export controls direction (Peter Wardle and John Forth can advise if required)

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

- Export Control Branch is best placed to answer.

Has it reviewed how Australian contractors generally maintain their ICT security?

- CIOG, ASD or ACSC (and CERT in AGD) are best placed to answer. I would suggest that ACSC report that led to this query is an example of Defence constantly reviewing and providing advice to industry broadly on good cyber security such as the Top 4 and Essential 8.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- DSVS is not aware of any general directive; however through our outreach and engagement the importance of good information security controls is emphasised in particular applying ASD recommended Essential 8.
- The CDIC play a role here (Sam Wong) – recent CDIC roadshow talking about good cyber security.
- ACSC play a role here ^{s7}
- CIOG play a role here (Col Keesing)

Kind regards

Steve

Steven Scanlan

A/g Assistant Secretary

Security Policy and Programs

Defence Security & Vetting Service

Department of Defence

t + 61 2 6266 3638 | e Steven.Scanlan@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Madge, Bronwyn MS

Sent: Thursday, 12 October 2017 1:50 PM

To: Scanlan, Steven MR

Cc: Media

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Steve,

One for you.

Cheers,
Bronwyn

Bronwyn Madge | Director Vetting Governance and Review

a CP3-4 099

t 7 0133 e bronwyn.madge@defence.gov.au

HOURS

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:48 PM
To: Madge, Bronwyn MS
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Bronwyn,

Please see attached for your action, if it could be returned to MECC ASAP it would be greatly appreciated.

SP&I have advised this is best tasked to you for a response (see below).

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:37 PM

To: Media

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

I have also sent back the OpenText task with the comment below. SP is not the best placed to respond to the questions posed.

Regards,

Louanne

Louanne Holmback-Piggott | Assistant Director

Strategic Policy Division | Department of Defence

R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610

P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Chifley, Damien MR

Sent: Thursday, 12 October 2017 13:25

To: Holmback-Piggott, Louanne MS

Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Louanne,

I think that this is best responded to by DSVS who run the Defence Industry Security Program and this is all related to things that were the subject of recommendations from the review conducted last year.

I think it was called the Defence Industry Security Review.

The best bet would be Peter West's branch.

Thanks

Damien

Damien Chifley

Director Defence Export Assessments and Regimes

Defence Export Controls Branch

Department of Defence R1-1-A037 PO Box 7910 Canberra BC ACT 2610

phone +61 2 626 51122 | mobile **s22** | email damien.chifley@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:16 PM
To: Chifley, Damien MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

See attached, let me know if you are going to take it on.

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence
R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 13:14
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please find attached the template for the below **s47F** enquiry.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:02 PM
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: FW: Questions on contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please see the below from s47F

I will template this up and send through for your action.

David has requested this by COB.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

From: s47F [mailto:s47F@fairfaxmedia.com.au]
Sent: Thursday, 12 October 2017 12:23 PM
To: Media
Subject: Questions on contractor IT breach

Hi guys,

I have some questions on the data breach by a Defence contractor.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

Has it reviewed how Australian contractors generally maintain their ICT security?

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

Can I get answers by 5pm?

thanks,

S47F

Defence & National Security Correspondent

s47F

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: Media
Sent: Thursday, 12 October 2017 5:39 PM
To: Tyrrell, Lauren MRS 1
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good afternoon Lauren,

FYSA- see below response from CIOG to the questions.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Zorzi, Adam MR
Sent: Thursday, 12 October 2017 3:58 PM
To: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Sarah,

Please see below advice from ICT Security Branch wrt to this enquiry.

Kind regards,

Adam Zorzi | CIO Communications

Commercial & Defence & Government

Chief Information Officer Group | Department of Defence
APW-05-062 | Anzac Park West | PO Box 7953 | Canberra BC | ACT 2610
P: 02 614 44433

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Masters, Amon MR
Sent: Thursday, 12 October 2017 3:41 PM
To: Zorzi, Adam MR
Cc: Thomas, Emma MS 4; Keesing, Col MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Adam,

Steve Scanlan (DS&VS) has already responded to most of these.

ICTSB responses below.

Has it reviewed how Australian contractors generally maintain their ICT security?

- Defence has a program in place to ensure industry partners adhere to protective security requirements.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- Defence has a program in place to provide appropriate guidance and support to both internal and external Defence stakeholders when an incident occurs that requires it.

Regards,

Amon Masters

Director

Chief Information Officer Group

Department of Defence

For more information, please contact the relevant Defence stakeholder.

For more information, please contact the relevant Defence stakeholder.

s22

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Thomas, Emma MS 4
Sent: Thursday, 12 October 2017 3:17 PM
To: Keesing, Col MR
Cc: Zorzi, Adam MR

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]
Importance: High

UNCLASSIFIED

Hi Col

In Lindsay's absence can you please answer Adams question IRT contractor IT breach?

Thank you

Kindest regards,

Em

Emma (Em) Thomas

Executive Assistant to, Lindsay Morgan

Assistant Secretary Information Communication Technology Security Branch, ASICTSB

Chief Information Officer Group

P: (02) 6144 4019 | E: emma.thomas4@defence.gov.au

A: APW-3-270, Anzac Park West, Constitution Avenue, Parkes ACT 2600

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Zorzi, Adam MR **On Behalf Of** CIOG Media

Sent: Thursday, 12 October 2017 3:17 PM

To: Thomas, Emma MS 4

Cc: Loane, Annie MS

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

Importance: High

UNCLASSIFIED

Hi Emma and Annie,

Is this media enquiry one for us?

Kind regards,

Adam Zorzi | CIOG Communications

Commercial & Business Enablement

Chief Information Officer Group | Department of Defence

APW-05-062 | Anzac Park West | PO Box 7953 | Canberra BC | ACT 2610

P: 02 614 44433

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 3:10 PM
To: SP&I-SP-Exec; CIOG Media; s7
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon all,

FYSA- please see attached for your urgent attention and response.

DSVS has advised they are not best placed to respond and advise that Export control Branch, ASD, CIOG, ACSC and AG are best placed to provide a response.

The journalist has requested a response by 1700 today, I will manage his expectations.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Scanlan, Steven MR
Sent: Thursday, 12 October 2017 2:58 PM
To: Media; Chifley, Damien MR
Cc: West, Peter MR 2; Keesing, Col MR; s7; Wong, Sam'; Wong, Sam MR; Wardle, Peter MR; Forth, John MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Media

DS&VS is not best placed to respond to this Media enquiry as it largely relates to export controls. I have provided some guidance to assist in responding to this request including potential POCs.

The content below is not cleared for public release.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfil those obligations?

- Export Controls Branch is best placed to answer this question (I understand that these are legal obligations)
- I understand the company in question was part of the Australia Community not the Defence Industry Security Program. DS&VS through Security Operations Branch provide support to this initiative under export controls direction (Peter Wardle and John Forth can advise if required).

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

- Export Control Branch is best placed to answer.

Has it reviewed how Australian contractors generally maintain their ICT security?

- CIOG, ASD or ACSC (and CERT in AGD) are best placed to answer. I would suggest that ACSC report that led to this query is an example of Defence constantly reviewing and providing advice to industry broadly on good cyber security such as the Top 4 and Essential 8.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- DSVS is not aware of any general directive; however through our outreach and engagement the importance of good information security controls is emphasised in particular applying ASD recommended Essential 8.
- The CDIC play a role here (Sam Wong) – recent CDIC roadshow talking about good cyber security.
- ACSC play a role here S7
- CIOG play a role here (Col Keesing)

Kind regards

Steve

Steven Scanlan

A/g Assistant Secretary
Security Policy and Programs
Defence Security & Vetting Service
Department of Defence
t + 61 2 6266 3638 | e Steven.Scanlan@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Madge, Bronwyn MS
Sent: Thursday, 12 October 2017 1:50 PM
To: Scanlan, Steven MR
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Steve,

One for you.

Cheers,
Bronwyn

Bronwyn Madge | Director Vetting Governance and Review

a CP3-4-099

t: +61 2 6127 0133 e bronwyn.madge@defence.gov.au

HOURS: 9.00am to 5.00pm (AEST) 07/10/17

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:48 PM
To: Madge, Bronwyn MS
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Bronwyn,

Please see attached for your action, if it could be returned to MECC ASAP it would be greatly appreciated.

SP&I have advised this is best tasked to you for a response (see below).

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1899
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:37 PM

To: Media

Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

I have also sent back the OpenText task with the comment below. SP is not the best placed to respond to the questions posed.

Regards,

Louanne

Louanne Holmback-Piggott | Assistant Director

Strategic Policy Division | Department of Defence

R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610

P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Chifley, Damien MR

Sent: Thursday, 12 October 2017 13:25

To: Holmback-Piggott, Louanne MS

Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Louanne,

I think that this is best responded to by DSVS who run the Defence Industry Security Program and this is all related to things that were the subject of recommendations from the review conducted last year.

I think it was called the Defence Industry Security Review.

The best bet would be Peter West's branch.

Thanks

Damien

Damien Chifley

Director Defence Export Assessments and Regimes

Defence Export Controls Branch

Department of Defence R1-1-A037 PO Box 7910 Canberra BC ACT 2610

phone +61 2 626 51122 | mobile **s22** | damien.chifley@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:16 PM
To: Chifley, Damien MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

See attached, let me know if you are going to take it on.

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence
R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 13:14
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please find attached the template for the below s47F enquiry.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:02 PM
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: FW: Questions on contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please see the below from s47F

I will template this up and send through for your action.

David has requested this by COB.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

From: s47F@fairfaxmedia.com.au
Sent: Thursday, 12 October 2017 12:23 PM
To: Media
Subject: Questions on contractor IT breach

Hi guys,

I have some questions on the data breach by a Defence contractor.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?
Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?
Has it reviewed how Australian contractors generally maintain their ICT security?
Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

Can I get answers by 5pm?

thanks,

s47F

Defence & National Security Correspondent

s47F

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: Media
Sent: Wednesday, 11 October 2017 8:52 PM
To: s47F
Cc: Media
Subject: RE: Defence contractor hacking [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good evening s47F

Please attribute the below to a spokesperson from the Australian Cyber Security Centre (ACSC):

"Today, while presenting at a conference in Sydney, an ASD official (who works for the ACSC) disclosed information about the theft of data from an Australian company.

"While the Australian company is a national-security linked contractor and the information disclosed was commercially sensitive, it was unclassified. The Government does not intend to discuss further the details of this cyber incident."

Kind regards,

Defence Media

Department of Defence | Russell Offices | PO Box 7909 Canberra BC ACT 2610
 Phone: (02) 6127 1959 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

From: s47F @aap.com.au]
Sent: Wednesday, 11 October 2017 4:45 PM
To: Media; Media
Subject: Defence contractor hacking

Hi there,
 Seeking comment from the department about the accuracy of the following report?

https://www.defenceconnect.com.au/intel-cyber/1377-f-35-and-naval-vessels-information-stolen-in-cyber-hack?utm_source=DefenceConnect&utm_campaign=11_10_17&utm_medium=email&utm_content=1

Is it true the hackers stole technical info about the F-35s, naval vessels, P-8 Poseidon, C-130 and the Joint Direct Attack Munition (JDAM) guidance kit?

If you could get back to me ASAP that would be grand.

Warm Regards,

s47F

s47F Journalist



Australian Associated Press

AAP Press Gallery, Suite 69, Parliament House, Capital Hill, Canberra ACT 2600, Australia

s47F

s47F www.aap.com.au

This email may contain information that is confidential. If you receive an email in error please delete it immediately.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: Media
Sent: Wednesday, 11 October 2017 8:51 PM
To: s47F
Cc: Media
Subject: RE: Fairfax enquiry [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good evening s47F

Please attribute the below to a spokesperson from the Australian Cyber Security Centre (ACSC):

"Today, while presenting at a conference in Sydney, an ASD official (who works for the ACSC) disclosed information about the theft of data from an Australian company.

"While the Australian company is a national-security linked contractor and the information disclosed was commercially sensitive, it was unclassified. The Government does not intend to discuss further the details of this cyber incident."

Kind regards,

Defence Media

Department of Defence | Russell Offices | PO Box 7900 Canberra BC ACT 2610
Phone: (02) 6127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

From: s47F [mailto:s47F@fairfaxmedia.com.au]
Sent: Wednesday, 11 October 2017 4:38 PM
To: Media
Subject: Fairfax enquiry

Hi guys,
Can I check whether this is accurate please?

https://www.defenceconnect.com.au/intel-cyber/1377-f-35-and-naval-vessels-information-stolen-in-cyber-hack?utm_source=DefenceConnect&utm_campaign=11_10_17&utm_medium=email&utm_content=1

Do you have a copy of Mitchell Clarke's presentation and can I get a copy? Evidently it was a public event. And can I get an answer asap thanks.

thanks,

s47F

Defence & National Security Correspondent

s47F

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: Media
Sent: Wednesday, 11 October 2017 8:47 PM
To: s47F
Cc: Media
Subject: RE: Urgent - transcript [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good evening s47F

Please attribute the below to a spokesperson from the Australian Cyber Security Centre (ACSC):

"Today, while presenting at a conference in Sydney, an ASD official (who works for the ACSC) disclosed information about the theft of data from an Australian company.

"While the Australian company is a national-security linked contractor and the information disclosed was commercially sensitive, it was unclassified. The Government does not intend to discuss further the details of this cyber incident."

Kind regards,

Defence Media

Department of Defence | Russell Offices | PO Box 7809 Canberra BC ACT 2610
Phone: (02) 6127 1989 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: s47F [mailto:s47F@momentummedia.com.au]
Sent: Wednesday, 11 October 2017 2:39 PM
To: Media
Subject: Urgent - transcript

Hi there,

Just called up regarding Mitchell Clarke of ASD speaking at the Australian Information Security Association (AISA), I'm really hoping to get a copy of the transcript of his talk or, alternatively, give him a quick call to confirm some information he may have stated.

Thanks,

s47F

MOMENTUMMEDIA

s47F

Email: s47F@momentummedia.com.au

Web: www.defenceconnect.com.au

Address: Level 13, 132 Arthur Street, North Sydney, NSW, 2060

Skorupa, Jessica MISS

From: Media
Sent: Wednesday, 11 October 2017 8:45 PM
To: s47F
Cc: Media
Subject: RE: URGENT request from Wall Street Journal [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good evening s47F

Please attribute the below to a spokesperson from the Australian Cyber Security Centre (ACSC):

"Today, while presenting at a conference in Sydney, an ASD official (who works for the ACSC) disclosed information about the theft of data from an Australian company.

"While the Australian company is a national-security linked contractor and the information disclosed was commercially sensitive, it was unclassified. The Government does not intend to discuss further the details of this cyber incident."

Kind regards,

Defence Media

Department of Defence | Russell Offices | PO Box 7909 Canberra BC ACT 2610
Phone: (02) 6127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DefenceMedia

From: s47F [mailto:s47F@wsj.com]
Sent: Wednesday, 11 October 2017 2:58 PM
To: Media
Subject: URGENT request from Wall Street Journal

Hi, am following up this report in ZDNet on a speech to a conference in Sydney today by a member of the ASD, Mitchell Clarke. As a matter of urgency, is it possible to get a copy of his speech and confirm these details, or alternatively reach Mr. Clarke himself? This speech has already been public domain ...

BEGINS

In November 2016, the Australian Signals Directorate (ASD) was alerted by a "partner organisation" that an attacker had gained access to the network of a 50-person aerospace engineering firm that subcontracts to the Department of Defence.

Restricted technical information on the F-35 Joint Strike Fighter, the P-8 Poseidon maritime patrol aircraft, the C-130 transport aircraft, the Joint Direct Attack Munition (JDAM) smart bomb kit, and "a few Australian naval vessels" was among the sensitive data stolen from a small Australian defence contractor in 2016.

The secret information was restricted under the International Traffic in Arms Regulations (ITAR), the US system designed to control the export of defence- and military-related technologies, **according to Mitchell Clarke, an incident response manager at the ASD who worked on the case.**

One document was a wireframe diagram of "one of the navy's new ships". A viewer could "zoom in down to the captain's chair and see that it's, you know, 1 metre away from nav chair", Clarke said.

s47F

CORRESPONDENT, AUSTRALIA AND PACIFIC

WSJ

s47F

s47F

@wsj.com

Room 117, Press Gallery
Parliament House
Canberra, ACT, 2600, Australia

WSJ

WSJ40

CELEBRATING
40 YEARS IN ASIA

VISIT WSJ.COM/ASIA40

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

s7



s7



Stewart, Nicholas MR 2

From: Media
Sent: Wednesday, 11 October 2017 5:13 PM
To: Kelton, Alexandra MS
Cc: Media
Subject: Articles [SEC=UNCLASSIFIED]

Categories: UNCLASSIFIED

UNCLASSIFIED

Good afternoon Alex,

Please find links to the published articles:

- <http://www.zdnet.com/article/secret-f-35-p-8-c-130-data-stolen-in-australian-defence-contractor-hack/>
- https://www.defenceconnect.com.au/intel-cyber/1377-f-35-and-naval-vessels-information-stolen-in-cyber-hack?utm_source=DefenceConnect&utm_campaign=11_10_17&utm_medium=email&utm_content=1

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

—IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: s47F [REDACTED]@wsj.com>
Sent: Wednesday, 11 October 2017 4:01 PM
To: Media
Subject: Re: URGENT request from Wall Street Journal [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

Hi Sarah, the deadline is as soon as possible. We are trying also to confirm through the conference team, as well as Minister Tehan's office. Hopefully it won't be too difficult, given it's already public.

Thanks and regards,

s47F [REDACTED]

CORRESPONDENT, AUSTRALIA AND PACIFIC

THE WALL STREET JOURNAL.

s47F [REDACTED]

s47F [REDACTED]@wsj.com
 A Suite 117, Press Gallery
 Parliament House
 Canberra, ACT, 2600, Australia

 **DOW JONES**

WSJ40 CELEBRATING
40 YEARS IN ASIA

VISIT WSJ.COM/ASIA40

On Wed, Oct 11, 2017 at 3:55 PM, Media <media@defence.gov.au> wrote:

UNCLASSIFIED

Good afternoon s47F [REDACTED]

Thank you for your enquiry.

We will endeavour to respond to your questions as soon as possible, did you have a deadline you were working toward? Unfortunately, it will unlikely be today.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999

E: media@defence.gov.au

From: [REDACTED] s47F [REDACTED]@wsj.com]
Sent: Wednesday, 11 October 2017 2:58 PM
To: Media
Subject: URGENT request from Wall Street Journal

Hi, am following up this report in ZDNet on a speech to a conference in Sydney today by a member of the ASD, Mitchell Clarke. As a matter of urgency, is it possible to get a copy of his speech and confirm these details, or alternatively reach Mr. Clarke himself? This speech has already been public domain ...

BEGINS

In November 2016, the Australian Signals Directorate (ASD) was alerted by a "partner organisation" that an attacker had gained access to the network of a 50-person aerospace engineering firm that subcontracts to the Department of Defence.

Restricted technical information on the F-35 Joint Strike Fighter, the P-8 Poseidon maritime patrol aircraft, the C-130 transport aircraft, the Joint Direct Attack Munition (JDAM) smart bomb kit, and "a few Australian naval vessels" was among the sensitive data stolen from a small Australian defence contractor in 2016.

The secret information was restricted under the International Traffic in Arms Regulations (ITAR), the US system designed to control the export of defence- and military-related

s7



Proposed MEDIA Response

Inquiry Number	CT-002940
Subject	Transcript request- Mitchell Clarke
Contact Name	s47F
Phone / Mobile / Email	
Organisation	Wall Street Journal
Due to Defence Media	<p>11/10/2017</p> <p><i>Media queries need to be prioritised as urgent. Please contact Defence Media at least 24 hours prior to the deadline if it is not achievable.</i></p> <p><i>Extensions will only be granted in exceptional circumstances.</i></p>
Questions / Query	<p>Hi, am following up this report in ZDNet on a speech to a conference in Sydney today by a member of the ASD, Mitchell Clarke. As a matter of urgency, is it possible to get a copy of his speech and confirm these details, or alternatively reach Mr. Clarke himself? This speech has already been public domain ...</p> <p>BEGINS</p> <p>In November 2016, the Australian Signals Directorate (ASD) was alerted by a "partner organisation" that an attacker had gained access to the network of a 50-person aerospace engineering firm that subcontracts to the Department of Defence.</p> <p>Restricted technical information on the F-35 Joint Strike Fighter, the P-8 Poseidon maritime patrol aircraft, the C-130 transport aircraft, the Joint Direct Attack Munition (JDAM) smart bomb kit, and "a few Australian naval vessels" was among the sensitive data stolen from a small Australian defence contractor in 2016.</p> <p>The secret information was restricted under the International Traffic in Arms Regulations (ITAR), the US system designed to control the export of defence- and military-related technologies, <u>according to Mitchell Clarke, an incident response manager at the ASD who worked on the case.</u></p> <p>One document was a wireframe diagram of "one of the navy's new ships". A viewer could "zoom in down to the captain's chair and see that it's, you know, 1 metre away from nav chair", Clarke said.</p>

Background / Summary	<p><i>Please provide a brief background into the media topic/issue using the below questions as a guide.</i></p> <p><i>Focussing questions (delete upon entry)</i></p> <ul style="list-style-type: none"> ➤ <i>Is this information already in the public domain? If so, where?</i> ➤ <i>Has the media previously asked questions on this topic? If so, what was the response?</i> ➤ <i>Was this mentioned in Parliament or at senate estimates recently?</i> ➤ <i>Was this as a result of a policy decision or legislative change?</i> ➤ <i>Is this in relation to a recent incident that occurred in Australia or overseas?</i> ➤ <i>Have any of the groups or services seen this request? If so, what was their instruction?</i>
Proposed Response	

Clearances

Clearance officers please ensure both date and time are detailed.

Drafted	Name	Appointment	Date and Time
Response Drafted by:			

Clearance	Name	Appointment	Date and Time
Group/Service 1 Star or above			
Strategic Communications Adviser			

Minister	Name	Appointment	Date and Time
Ministerial Consultation:: (To be completed by Defence Media)			

Skorupa, Jessica MISS

From: Media
Sent: Wednesday, 11 October 2017 3:51 PM
To: s47F
Cc: Media
Subject: RE: Urgent - transcript [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Hi s47F

Thank you for your enquiry.

Could you please advise what questions you would like to ask and we will manage accordingly, could you also please specify the deadline you are working toward?

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: s47F @momentummedia.com.au]
Sent: Wednesday, 11 October 2017 2:39 PM
To: Media
Subject: Urgent - transcript

Hi there,

Just called up regarding Mitchell Clarke of ASD speaking at the Australian Information Security Association (AISA), I'm really hoping to get a copy of the transcript of his talk or, alternatively, give him a quick call to confirm some information he may have stated.

Thanks,

s47F

MOMENTUMMEDIA

Phone: s47F
Mobile: [REDACTED]
Email: s47F@momentummedia.com.au
Web: www.defenceconnect.com.au
Address: Level 13, 132 Arthur Street, North Sydney, NSW, 2060

s7



Proposed MEDIA Response

Inquiry Number	CT-002940
Subject	Transcript request- Mitchell Clarke
Contact Name	s47F [REDACTED] - WSJ s47F [REDACTED] - Momentum Media
Phone / Mobile / Email	
Organisation	Wall Street Journal
Due to Defence Media	11/10/2017 <i>Media queries need to be prioritised as urgent. Please contact Defence Media at least 24 hours prior to the deadline if it is not achievable.</i> <i>Extensions will only be granted in exceptional circumstances.</i>
Questions / Query	s47F [REDACTED] WSJ Hi, am following up this report in ZDNet on a speech to a conference in Sydney today by a member of the ASD, Mitchell Clarke. As a matter of urgency, is it possible to get a copy of his speech and confirm these details, or alternatively reach Mr. Clarke himself? This speech has already been public domain ... s47F [REDACTED] - Momentum Media Just called up regarding Mitchell Clarke of ASD speaking at the Australian Information Security Association (AISA), I'm really hoping to get a copy of the transcript of his talk or, alternatively, give him a quick call to confirm some information he may have stated.
Background / Summary	<i>Please provide a brief background into the media topic/issue using the below questions as a guide.</i> Focussing questions (delete upon entry) ➤ <i>Is this information already in the public domain? If so, where?</i> ➤ <i>Has the media previously asked questions on this topic? If so, what was the response?</i> ➤ <i>Was this mentioned in Parliament or at senate estimates recently?</i>

	<p>➤ <i>Was this as a result of a policy decision or legislative change?</i></p> <p>➤ <i>Is this in relation to a recent incident that occurred in Australia or overseas?</i></p> <p>➤ <i>Have any of the groups or services seen this request? If so, what was their instruction?</i></p>
Proposed Response	

Clearances

Clearance officers please ensure both date and time are detailed.

Drafted	Name	Appointment	Date and Time
Response Drafted by:			

Clearance	Name	Appointment	Date and Time
Group/Service 1 Star or above			
Strategic Communications Adviser			

Minister	Name	Appointment	Date and Time
Ministerial Consultation:: (To be completed by Defence Media)			

Skorupa, Jessica MISS

From: AUS iSentia Transcript <TranscriptAU@isentia.com>
Sent: Thursday, 12 October 2017 2:24 PM
To: Media
Cc: cae@isentia.com
Subject: Transcript - Christopher Pyne - ABC News, Mornings - Cyber security breach - 12October17
Attachments: Christopher Pyne - ABC News Mornings - 12 October 2017.doc
Follow Up Flag: Follow up
Flag Status: Completed
Categories: SC

Please find attached the requested transcript of Christopher Pyne about cyber security breach.

This is an automated message, for assistance please contact your Account Executive team using the details below.

Kind Regards,

Canberra Account Executive Team

t. 061 2 6124 5200
a. 131 Canberra Ave. Griffith, ACT 2603, Australia
e. cae@isentia.com
isentia.com



<http://www.isentia.com/>



THE HON CHRISTOPHER PYNE MP
Minister for Defence Industry
Leader of the House
Federal Member for Sturt

TRANSCRIPT

E&OE TRANSCRIPT

Doorstop Interview

12 October 2017

SUBJECTS: Cyber security

JOE O'BRIEN: Alastair MacGibbon there, and just in the last few minutes, the Minister for Defence Industry, Christopher Pyne, has been speaking about this issue.

[Excerpt]

CHRISTOPHER PYNE: It's a salutary reminder to Australian businesses that they have to get their cyber security right, that they can't be underdone for cyber security. These attempts at hacking are happening all the time. As we speak, they're going on right now. Thousands and thousands of attempts are happening every year at breaking into Australian businesses, for whatever reason. Usually commercial reasons. And in this case, of course, the information that's been stolen is commercial information. It's not classified information, so it's not military information, and fortunately the processes that we have in place have found this breach working with Primes, and it's being attended to, but it's a very important reminder to small and medium enterprises as well as the large contractors that they will not get work in Defence Industry if their cyber security is not up to standard. So actually, while it's disappointing, I'm grateful that it's not as serious as if there were military breaches, but also I'm pleased, in a way, that it reminds Australian business of the dangers that lurk out there, whether from state actors or non-state actors.

QUESTION: So you admit that the government should have been a little more thorough in who they were using?

CHRISTOPHER PYNE: No, not at all. The Government's doing its job. Australian businesses need to be thorough in providing the best cyber security otherwise they won't get contracts with the Government.

QUESTION: [Indistinct] you're quite confident that there's no risk to national security as a result of this.

CHRISTOPHER PYNE: That's my advice from the minister responsible, Dan Tehan. He's the Minister for Cyber Security, and he has all the technical information in his hands and he assures me that's the case.

QUESTION: The securities department, though, the directorate that describes this as intensive and extensive. That must raise concerns, just by your comments, that it's not a military nature?

CHRISTOPHER PYNE: Australian Signals Directorate? Well, the ASD's doing its job and I'm glad it's done its job, and that's what it's there for and so is the Cyber Security Office.

QUESTION: But they took three or four months to get to this point, mate.

CHRISTOPHER PYNE: Well, I'm not going to have a big argument about this because today is actually a great day for Adelaide. This is a terrific day for Adelaide. The story out of this morning is that we have filled in Labor's valley of death with 600 construction jobs and many more to come, and there'll be more ...

QUESTION: [Indistinct question].

CHRISTOPHER PYNE: There'll be more announcements down the track of new jobs here to keep filling in that valley of death.

QUESTION: [Indistinct] have access to this Defence information? How many subcontractors?

CHRISTOPHER PYNE: Look, I've answered all the questions about the cyber breach.

QUESTION: You said this morning on radio that the media don't know all the details in regards to this. What don't we know?

CHRISTOPHER PYNE: Well, the Government has a lot of information at its disposal. Of course it does, that's what the Australian Signals Directorate is for. We don't share...

QUESTION: [Talks over] What are you alluding to, that we don't know all the details?

CHRISTOPHER PYNE: You going to let me finish my point, or do you want to finish my point for me? The Australian Government has a lot of information at its disposal, because that's what the Australian Signals Directorate does. It's a very highly skilled and sophisticated organization of world standard. Now, we don't tell the media everything that we know because for obvious reasons, we don't want hackers, state actors, non-state actors to know what we know about what they're doing. So there's a lot of information that we don't necessarily share with the media, because we are actually trying to defend Australia.

We have a defensive capability in cyber security, we have an offensive capability in cyber security. We've said that in the Defence White Paper, we've provided for the spending on the Australian Signals Directorate and the Cyber Security Offices and the integrated investment plan of this big defence capability build-up, and it's in the Defence Industry policy statement. So we are well across what needs to be done, and we're doing that job.

QUESTION: The fact that we're a target in a time when we're dealing with the hostility between North Korea and the US, isn't that worrying that we're not ...

CHRISTOPHER PYNE: Of course we're a target. We're undertaking the largest submarine project in the world right now. Adelaide is one of the most interesting and hottest spots, as they say, for cyber security and people trying to breach our businesses and our government. And that's why.

QUESTION: Is that why it was so easy to breach?

CHRISTOPHER PYNE: No, not at all, they're hard to breach. But we are spending hundreds of millions of dollars - and across the economy, billions of dollars - on cyber security. Whether it's the government, whether it's the banks, financial institutions, small and medium enterprises. And I guess this breach that's occurred is a great reminder to everybody in Australian business that they need to get their cyber security right, that there are malicious actors out there - whether they are other states, or whether they're non-state actors - who are trying to get that commercial information. And fortunately, on this occasion, the information they have breached is commercial. It's not classified, and it's not dangerous in terms of the military.

QUESTION: So this is when you'll ramp up the kind of protections on information that would endanger our national security?

CHRISTOPHER PYNE: Well, we have processes in place and that's what the ASD is doing. That's what the cyber security office is doing, and that's why Malcolm Turnbull appointed the first cyber security minister in Australia's history, Mr Dan Tehan.

QUESTION: The Adelaide contractor is regulated under the International Traffic and Arms Regulations. Will it face any penalties from the Australian Government or the US Government over this?

CHRISTOPHER PYNE: I think the information that was taken was about how ITAR works. It wasn't actually about any classified information that ITAR is responsible for.

QUESTION: Minister, how concerned are you about ...

CHRISTOPHER PYNE: Let's let Stacey Lee have a go, it's a long way away from the back. Ahead of the pack, I should say.

QUESTION: Peter Dutton has said in an interview that he would one day like to be the leader of the Liberal Party. Do you think he'd make a good leader, and do you think this is him putting in steps in place to replace Malcolm Turnbull?

CHRISTOPHER PYNE: I think if you read the entire quote, you'll see that he said it was the most unlikely thing imaginable. He wouldn't even get to first base, because there is absolutely no question about this issue. He's a great colleague, I have a lot of other great colleagues in the Cabinet and in the party room. We have a fantastic leader in Malcolm Turnbull, he's doing a sensational job, he's vastly more popular than the alternative. And as a consequence, I'm sure, by the 2019 election, when our policies are working as they are now, in terms of reducing power prices, making energy reliable, meeting our international targets for our emissions reductions. When we see those policies working, we'll get credit for it at the election which is at least 20 or more months away. And as a consequence, any other talk to the contrary, is quite frankly ridiculous.

QUESTION: The polls showing Nick Xenophon likely to win [audio skip] hardly, how concerned are you that SA First could relegate the Liberal Party here in SA to another four year term in opposition?

CHRISTOPHER PYNE: Look, if you vote for Nick Xenophon, you will probably get a Labor government for 20 years in this state. That is the danger. Nick Xenophon is a celebrity candidate, his party is a shambles, the polls will always reflect popularity for a celebrity candidate, but he can't manage his own party and therefore he shouldn't be entrusted with the keys of the state. He's lost John Darley, Ann Bressington, Rhys Adams – I mean, the list is getting longer and longer of the shambolic nature of Nick Xenophon's management of both his party and his policies.

So it is the danger to the state. The last thing South Australia needs right now is a shambolic government, and that's what Nick Xenophon is offering. Worse than that, a vote for Nick Xenophon will give 20 years of Labor government in this state, which is the last thing people want. The one very clear message from that poll is hardly anybody wants to vote Labor, and yet if you vote Nick Xenophon, you will get 20 years of Labor government.

[End of excerpt]

JOE O'BRIEN: Okay, we'll leave that there. That was from Adelaide a short time ago, the Defence Industry Minister Christopher Pyne saying this breach of a subcontractors computer system – they were subcontracting the Defence Department – is a good reminder of the importance of strong cyber security.

Media Contacts

Rory Grant: ^{s22} [REDACTED] pynemedia@defence.gov.au

Eleisa Hancock: ^{s22} [REDACTED], pynemedia@defence.gov.au

Defence Media (02) 6127 1999

Skorupa, Jessica MISS

From: Media
Sent: Thursday, 12 October 2017 2:31 PM
To: Laube, Wade MR 1
Cc: Media
Subject: RE: Transcript - Alistair McGibbon/ABC radio [SEC=UNCLASSIFIED]
Attachments: Transcript- ABC- Alistair MacGibbon.docx

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Good afternoon Wade,

Please see attached the requested transcript.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Laube, Wade MR 1
Sent: Thursday, 12 October 2017 11:23 AM
To: Media
Subject: Transcript - Alistair McGibbon/ABC radio [SEC=UNCLASSIFIED]

UNCLASSIFIED

Could we please request a transcript of the above?

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.



THE HON CHRISTOPHER PYNE MP
Minister for Defence Industry
Leader of the House
Federal Member for Sturt

TRANSCRIPT

E&OE TRANSCRIPT

Doorstop Interview

12 October 2017

SUBJECTS: Cyber security

JOE O'BRIEN: Alastair MacGibbon there, and just in the last few minutes, the Minister for Defence Industry, Christopher Pyne, has been speaking about this issue.

[Excerpt]

CHRISTOPHER PYNE: It's a salutary reminder to Australian businesses that they have to get their cyber security right, that they can't be underdone for cyber security. These attempts at hacking are happening all the time. As we speak, they're going on right now. Thousands and thousands of attempts are happening every year at breaking into Australian businesses, for whatever reason. Usually commercial reasons. And in this case, of course, the information that's been stolen is commercial information. It's not classified information, so it's not military information, and fortunately the processes that we have in place have found this breach working with Primes, and it's being attended to, but it's a very important reminder to small and medium enterprises as well as the large contractors that they will not get work in Defence Industry if their cyber security is not up to standard. So actually, while it's disappointing, I'm grateful that it's not as serious as if there were military breaches, but also I'm pleased, in a way, that it reminds Australian business of the dangers that lurk out there, whether from state actors or non-state actors.

QUESTION: So you admit that the government should have been a little more thorough in who they were using?

CHRISTOPHER PYNE: No, not at all. The Government's doing its job. Australian businesses need to be thorough in providing the best cyber security otherwise they won't get contracts with the Government.

QUESTION: [Indistinct] you're quite confident that there's no risk to national security as a result of this.

CHRISTOPHER PYNE: That's my advice from the minister responsible, Dan Tehan. He's the Minister for Cyber Security, and he has all the technical information in his hands and he assures me that's the case.

QUESTION: The securities department, though, the directorate that describes this as intensive and extensive. That must raise concerns, just by your comments, that it's not a military nature?

CHRISTOPHER PYNE: Australian Signals Directorate? Well, the ASD's doing its job and I'm glad it's done its job, and that's what it's there for and so is the Cyber Security Office.

QUESTION: But they took three or four months to get to this point, mate.

CHRISTOPHER PYNE: Well, I'm not going to have a big argument about this because today is actually a great day for Adelaide. This is a terrific day for Adelaide. The story out of this morning is that we have filled in Labor's valley of death with 600 construction jobs and many more to come, and there'll be more ...

QUESTION: [Indistinct question].

CHRISTOPHER PYNE: There'll be more announcements down the track of new jobs here to keep filling in that valley of death.

QUESTION: [Indistinct] have access to this Defence information? How many subcontractors?

CHRISTOPHER PYNE: Look, I've answered all the questions about the cyber breach.

QUESTION: You said this morning on radio that the media don't know all the details in regards to this. What don't we know?

CHRISTOPHER PYNE: Well, the Government has a lot of information at its disposal. Of course it does, that's what the Australian Signals Directorate is for. We don't share...

QUESTION: [Talks over] What are you alluding to, that we don't know all the details?

CHRISTOPHER PYNE: You going to let me finish my point, or do you want to finish my point for me? The Australian Government has a lot of information at its disposal, because that's what the Australian Signals Directorate does. It's a very highly skilled and sophisticated organization of world standard. Now, we don't tell the media everything that we know because for obvious reasons, we don't want hackers, state actors, non-state actors to know what we know about what they're doing. So there's a lot of information that we don't necessarily share with the media, because we are actually trying to defend Australia.

We have a defensive capability in cyber security, we have an offensive capability in cyber security. We've said that in the Defence White Paper, we've provided for the spending on the Australian Signals Directorate and the Cyber Security Offices and the integrated investment plan of this big defence capability build-up, and it's in the Defence Industry policy statement. So we are well across what needs to be done, and we're doing that job.

QUESTION: The fact that we're a target in a time when we're dealing with the hostility between North Korea and the US, isn't that worrying that we're not ...

CHRISTOPHER PYNE: Of course we're a target. We're undertaking the largest submarine project in the world right now. Adelaide is one of the most interesting and hottest spots, as they say, for cyber security and people trying to breach our businesses and our government. And that's why.

QUESTION: Is that why it was so easy to breach?

CHRISTOPHER PYNE: No, not at all, they're hard to breach. But we are spending hundreds of millions of dollars - and across the economy, billions of dollars - on cyber security. Whether it's the government, whether it's the banks, financial institutions, small and medium enterprises. And I guess this breach that's occurred is a great reminder to everybody in Australian business that they need to get their cyber security right, that there are malicious actors out there - whether they are other states, or whether they're non-state actors - who are trying to get that commercial information. And fortunately, on this occasion, the information they have breached is commercial. It's not classified, and it's not dangerous in terms of the military.

QUESTION: So this is when you'll ramp up the kind of protections on information that would endanger our national security?

CHRISTOPHER PYNE: Well, we have processes in place and that's what the ASD is doing. That's what the cyber security office is doing, and that's why Malcolm Turnbull appointed the first cyber security minister in Australia's history, Mr Dan Tehan.

QUESTION: The Adelaide contractor is regulated under the International Traffic and Arms Regulations. Will it face any penalties from the Australian Government or the US Government over this?

CHRISTOPHER PYNE: I think the information that was taken was about how ITAR works. It wasn't actually about any classified information that ITAR is responsible for.

QUESTION: Minister, how concerned are you about ...

CHRISTOPHER PYNE: Let's let Stacey Lee have a go, it's a long way away from the back. Ahead of the pack, I should say.

QUESTION: Peter Dutton has said in an interview that he would one day like to be the leader of the Liberal Party. Do you think he'd make a good leader, and do you think this is him putting in steps in place to replace Malcolm Turnbull?

CHRISTOPHER PYNE: I think if you read the entire quote, you'll see that he said it was the most unlikely thing imaginable. He wouldn't even get to first base, because there is absolutely no question about this issue. He's a great colleague, I have a lot of other great colleagues in the Cabinet and in the party room. We have a fantastic leader in Malcolm Turnbull, he's doing a sensational job, he's vastly more popular than the alternative. And as a consequence, I'm sure, by the 2019 election, when our policies are working as they are now, in terms of reducing power prices, making energy reliable, meeting our international targets for our emissions reductions. When we see those policies working, we'll get credit for it at the election which is at least 20 or more months away. And as a consequence, any other talk to the contrary, is quite frankly ridiculous.

QUESTION: The polls showing Nick Xenophon likely to win [audio skip] hardly, how concerned are you that SA First could relegate the Liberal Party here in SA to another four year term in opposition?

CHRISTOPHER PYNE: Look, if you vote for Nick Xenophon, you will probably get a Labor government for 20 years in this state. That is the danger. Nick Xenophon is a celebrity candidate, his party is a shambles, the polls will always reflect popularity for a celebrity candidate, but he can't manage his own party and therefore he shouldn't be entrusted with the keys of the state. He's lost John Darley, Ann Bressington, Rhys Adams – I mean, the list is getting longer and longer of the shambolic nature of Nick Xenophon's management of both his party and his policies.

So it is the danger to the state. The last thing South Australia needs right now is a shambolic government, and that's what Nick Xenophon is offering. Worse than that, a vote for Nick Xenophon will give 20 years of Labor government in this state, which is the last thing people want. The one very clear message from that poll is hardly anybody wants to vote Labor, and yet if you vote Nick Xenophon, you will get 20 years of Labor government.

[End of excerpt]

JOE O'BRIEN: Okay, we'll leave that there. That was from Adelaide a short time ago, the Defence Industry Minister Christopher Pyne saying this breach of a subcontractors computer system – they were subcontracting the Defence Department – is a good reminder of the importance of strong cyber security.

Media Contacts

Rory Grant: ^{s22} [REDACTED] pynemedia@defence.gov.au

Eleisa Hancock: ^{s22} [REDACTED] pynemedia@defence.gov.au

Defence Media (02) 6127 1999

Stewart, Nicholas MR 2

From: Media
Sent: Thursday, 12 October 2017 11:54 AM
To: Pearse, Sophie MISS
Cc: Media
Subject: RE: Request for transcripts from yesterday cyber attack coverage for JSF Div [SEC=UNCLASSIFIED]
Attachments: Dan Tehan - National Press Club ABC24 - 10 October 2017.doc
Categories: UNCLASSIFIED

UNCLASSIFIED

Good morning Sophie,

Please find attached a transcript of Tehan's Tuesday Press Club address.

We don't have any audio/vision of yesterday's presentation.

Cheers,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Pearse, Sophie MISS
Sent: Thursday, 12 October 2017 11:51 AM
To: Media
Cc: CASG Media
Subject: Request for transcripts from yesterday cyber attack coverage for JSF Div [SEC=UNCLASSIFIED]
Importance: High

UNCLASSIFIED

Hi team,

Do you have a transcript of Minister Dan Tehan's Cyber Security address to the Press club yesterday?

Also, do you know whether anyone recorded old mate from ASD's presentation yesterday? Our JSF Div are seeking information urgently.

Anything you can provide will be greatly appreciated,

Thank you team!

Kind regards,

Sophie.

Sophie Pearce

Acting Senior Media & Communications Advisor
CASG Media and Communications

Department of Defence | Capability Acquisition and Sustainment Group Follow us on Twitter: @Defence_CASG

Russell Offices, R2-5-A138 | PO Box 7904 | CANBERRA BC ACT 2610 T: (02) 6266 7220 | s22

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Kennedy, Emily MS 1

Sent: Thursday, 12 October 2017 11:19 AM

To: Pearce, Sophie MISS

Subject: Transcripts from yesterday cyber attack coverage [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hey Sophie,

Do you have transcripts of Michael Clarke's from ASD presentation to the media yesterday?

Also – Tehan transcripts?

So sorry to bother you.

Em

Emily Kennedy

Principal Communications Advisor
Stakeholder Engagement and Communication
JSF Division

Department of Defence | Capability Acquisition and Sustainment Group
Brindabella Park Offices, BP1-2-022 | PO Box 7904 | CANBERRA BC ACT 2610

T: +61 2 6144 2145 | s22 | emily.kennedy1@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Stewart, Nicholas MR 2

From: Media
Sent: Thursday, 12 October 2017 6:27 PM
To: 'cae@isentia.com'
Cc: Media
Subject: FW: Transcripts [SEC=UNCLASSIFIED]

Categories: UNCLASSIFIED

UNCLASSIFIED

Good evening iSentia,

Could we please order transcripts of the below as well as ETAs please.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P +61 2 6127 1999
E media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Laube, Wade MR 1
Sent: Thursday, 12 October 2017 6:26 PM
To: Media
Cc: Kiploks, Jimmy MR; Carlson, Dean MR; Varjavandi, Faz MR; Budd, Henry MR
Subject: Transcripts [SEC=UNCLASSIFIED]

UNCLASSIFIED

Could we please order transcripts of the following:

- Senator Scullion on ABC Darwin Drive, to be broadcast this evening,
- Alastair MacGibbon on Speers Tonight, on Sky News at 8pm,
- Alastair MacGibbon on The Panel, this evening,
- Minister Tehan on ABC Sydney Drive at 5.05pm and ABC RN Drive at 6.05pm.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

Skorupa, Jessica MISS

From: s47F [REDACTED]@dva.gov.au>
Sent: Thursday, 12 October 2017 7:33 PM
To: Media
Cc: Geering, John MR; Kelton, Alexandra MS; Fraser, Katherine MRS 1; Gillis, Kim MR
Subject: RE: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

Thanks Lauren

If Defence is comfortable with the below it is approved to go to s47F [REDACTED] from a Defence spokesperson:

Obligations under the United States' International Traffic in Arms Regulations (ITAR) are a matter for the company and whomever it was sub-contracting to.

Defence reviews ITAR compliance on an ongoing basis and is in regular discussion with the United states on ITAR related matters.

All Defence contracts that involve classified material stipulate that the contractor must meet the requirements of Defence Security Policy. A security risk assessment must be undertaken as part of the planning process for all significant procurement activity.

Defence provides security support and advice to contractors through:

- the Defence Industry Security Program (DISP). A business, whether a prime contractor or subcontractor, is required to obtain and maintain membership of the Defence Industry Security Program when it will be accessing, handling or storing electronic or hardcopy information classified PROTECTED or above. All Defence Industry Security Program members must comply with the security standards required by the Defence Security Manual, Australian Government Protective Security Policy Framework, and the Australian Government Information Security Manual.
- the Centre for Defence Industry Capability (CDIC); and
- the Australian Cyber Security Centre (ACSC).

In August 2017, the CDIC, Defence and ACSC delivered seven Defence Industry Security and Cyber Awareness Forums across Australia to provide contextual cyber security threats affecting Australia's defence industry. The forums provided information about preventative strategies and resources.

From: Media [mailto:media@defence.gov.au]

Sent: Thursday, 12 October 2017 7:06 PM

To: s47F [REDACTED]@dva.gov.au>

Cc: Media <media@defence.gov.au>; Geering, John MR <john.geering@defence.gov.au>; Kelton, Alexandra MS <alexandra.kelton@defence.gov.au>; Fraser, Katherine MRS 1 <katherine.fraser1@defence.gov.au>; Gillis, Kim MR

<kim.gillis@defence.gov.au>

Subject: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good evening s47F

Seeking your urgent clearance for the attached response to be provided to s47F at the SMH & The Age.

Grateful for your earliest attention to this.

Kind regards,

Lauren Tyrrell

Assistant Director | Corporate Communication
Ministerial Executive Co-ordination & Communication (MECC) Division

Department of Defence | R1-5-A060 Russell Offices | PO Box 7909 Canberra BC ACT 2610
Phone: (02) 6127 1987 Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 77 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT

1. Before opening any attachments, please check for viruses.
2. This e-mail (including any attachments) may contain confidential information for the intended recipient. If you are not the intended recipient, please contact the sender and delete all copies of this email.
3. Any views expressed in this e-mail are those of the sender and are not a statement of Australian Government Policy unless otherwise stated.
4. Electronic addresses published in this email are not conspicuous publications and DVA does not consent to the receipt of commercial electronic messages.
5. To unsubscribe from emails from the Department of Veterans' Affairs (DVA) please go to http://www.dva.gov.au/contact_us/Pages/feedback.aspx, and advise which mailing list you would like to unsubscribe from.
6. Finally, please do not remove this notice.

Skorupa, Jessica MISS

From: Geering, John MR
Sent: Thursday, 12 October 2017 8:45 PM
To: Media
Cc: Kelton, Alexandra MS; Fraser, Katherine MRS 1
Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

This change to the wording is incorrect. Companies are not obliged to join the disp for low level classified info. Only protected high and above (according to peter west) can you call wade?

Sent from my iPhone

On 12 Oct 2017, at 8:37 pm, Media <media@defence.gov.au> wrote:

UNCLASSIFIED

Hi John,

OMINDEF have made some changes to the response (See below).

The original proposed response is attached.

Please advise if this is cleared to send.

Kind regards,

Sarah Collins

Public Affairs Officer | Corporate Communication

Ministerial Executive Co ordination & Communication (MECC) Division

Department of Defence | Russell Offices | PO Box 7909 Canberra BC ACT 2610

Phone: (02) 6127 1999 | Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Laube, Wade MR 1
Sent: Thursday, 12 October 2017 8:33 PM
To: Tyrrell, Lauren MRS 1; Media
Subject: Re: Seeking URGENT OMINDP clearance: CT-002945 Contractor IT Breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

The following is cleared by OMINDEF and OMINDP:

Obligations under the United States' International Traffic in Arms Regulations (ITAR) are a matter for the company and whomever it was sub-contracting to.

Defence reviews ITAR compliance on an ongoing basis and is in regular discussion with the United States on ITAR related matters.

All Defence contracts that involve classified material stipulate that the contractor must meet the requirements of Defence Security Policy. A security risk assessment must be undertaken as part of the planning process for all significant procurement activity.

Defence provides security support and advice to contractors through:

- the Defence Industry Security Program (DISP). A business, whether a prime contractor or subcontractor, is required to obtain and maintain membership of the Defence Industry Security Program when it will be accessing, handling or storing classified information. All Defence Industry Security Program members must comply with the security standards required by the Defence Security Manual, Australian Government Protective Security Policy Framework, and the Australian Government Information Security Manual.
- the Centre for Defence Industry Capability (CDIC); and
- the Australian Cyber Security Centre (ACSC).



In August 2017, the CDIC, Defence and ACSC delivered seven Defence Industry Security and Cyber Awareness Forums across Australia to provide contextual cyber security threats affecting Australia's defence industry. The forums provided information about preventative strategies and resources.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

<mime-attachment>

s7



From: Media
Sent: Thursday, 12 October 2017 3:10 PM
To: SP&I-SP-Exec; CIOG Media;  
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon all,

FYSA- please see attached for your urgent attention and response.

DSVS has advised they are not best placed to respond and advise that Export control Branch, ASD, CIOG, ACSC and AG are best placed to provide a response.

The journalist has requested a response by 1700 today, I will manage his expectations.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Scanlan, Steven MR
Sent: Thursday, 12 October 2017 2:58 PM
To: Media; Chifley, Damien MR
Cc: West, Peter MR 2; Keesing, Col MR; s7 [REDACTED] 'Wong, Sam'; Wong, Sam MR; Wardle, Peter MR; Forth, John MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Media

DS&VS is not best placed to respond to this Media enquiry as it largely relates to export controls. I have provided some guidance to assist in responding to this request including potential POCs. The content below is not cleared for public release.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfil those obligations?

- Export Controls Branch is best placed to answer this question (I understand that these are legal obligations)
- I understand the company in question was part of the Australia Community not the Defence Industry Security Program. DS&VS through Security Operations Branch provide support to this initiative under export controls direction (Peter Wardle and John Forth can advise if required).

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

- Export Control Branch is best placed to answer.

Has it reviewed how Australian contractors generally maintain their ICT security?

- CIOG, ASD or ACSC (and CERT in AGD) are best placed to answer. I would suggest that ACSC report that led to this query is an example of Defence constantly reviewing and providing advice to industry broadly on good cyber security such as the Top 4 and Essential 8.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- DSVS is not aware of any general directive; however through our outreach and engagement the importance of good information security controls is emphasised in particular applying ASD recommended Essential 8.
- The CDIC play a role here (Sam Wong) – recent CDIC roadshow talking about good cyber security.
- ACSC play a role here s7
- CIOG play a role here (Col Keesing)

Kind regards
Steve

Steven Scanlan

A/g Assistant Secretary
Security Policy and Programs
Defence Security & Vetting Service
Department of Defence
t + 61 2 6266 3638 | e Steven.Scanlan@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Madge, Bronwyn MS
Sent: Thursday, 12 October 2017 1:50 PM
To: Scanlan, Steven MR
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Steve,

One for you.

✓ Cheers,
Bronwyn

Bronwyn Madge | Director Vetting Governance and Review

a CP3-4-099
t 7 0133 e bronwyn.madge@defence.gov.au
HOURS

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:48 PM
To: Madge, Bronwyn MS
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Bronwyn,

Please see attached for your action, if it could be returned to MECC ASAP it would be greatly appreciated.

SP&I have advised this is best tasked to you for a response (see below).

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:37 PM
To: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

I have also sent back the OpenText task with the comment below. SP is not the best placed to respond to the questions posed.

Regards,

Louanne

Louanne (Holmback-Piggott) | Assistant Director

Strategic Policy Division | Department of Defence

R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Chifley, Damien MR
Sent: Thursday, 12 October 2017 13:25
To: Holmback-Piggott, Louanne MS
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Louanne,

I think that this is best responded to by DSVS who run the Defence Industry Security Program and this is all related to things that were the subject of recommendations from the review conducted last year.

I think it was called the Defence Industry Security Review.

The best bet would be Peter West's branch.

Thanks

Damien

Damien Chifley
Director Defence Export Assessments and Regimes
Defence Export Controls Branch

Department of Defence R1-1-A037 PO Box 7910 Canberra BC ACT 2610
phone +61 2 626 51122 | s22 | email damien.chifley@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:16 PM
To: Chifley, Damien MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

See attached, let me know if you are going to take it on.

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence

R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 13:14
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please find attached the template for the below David Wroe enquiry.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:02 PM
To: SP&I-SP-Exec
Cc: SP&I Group Coord; Media
Subject: FW: Questions on contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please see the below from s47F

I will template this up and send through for your action.

David has requested this by COB.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

From: s47F [redacted]@fairfaxmedia.com.au]
Sent: Thursday, 12 October 2017 12:23 PM
To: Media
Subject: Questions on contractor IT breach

Hi guys,

I have some questions on the data breach by a Defence contractor.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?
Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?
Has it reviewed how Australian contractors generally maintain their ICT security?
Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

Can I get answers by 5pm?

thanks,

s47F [redacted]
Defence & National Security Correspondent

s47F [redacted]

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

s7



s7



s7



s7



Skorupa, Jessica MISS

From: Zorzi, Adam MR on behalf of CIOG Media
Sent: Thursday, 12 October 2017 3:32 PM
To: Media
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up
Flag Status: Completed

Categories: SC

UNCLASSIFIED

Hi Sarah,

I have forwarded the enquiry to ICT Security Branch (CIOG) to see whether it sits with them, or they are in a position to provide a response.

AS ICTSB is not in the office this afternoon, so it is currently with Col Keesing (Director ICT Security Management).

Kind regards,

Adam Zorzi | CIOG Communications

Commercial & Business Enablement
 Chief Information Officer Group | Department of Defence
 APW/05-062 | Anzac Park West | PO Box 7953 | Canberra BC | ACT 2610
 P: 02 614 44433

IMPORTANT This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 3:10 PM
To: SP&I-SP-Exec; CIOG Media; [REDACTED] s7 [REDACTED]
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon all,

FYSA- please see attached for your urgent attention and response.

DSVS has advised they are not best placed to respond and advise that Export control Branch, ASD, CIOG, ACSC and AG are best placed to provide a response.

The journalist has requested a response by 1700 today, I will manage his expectations.

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1000
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Scanlan, Steven MR
Sent: Thursday, 12 October 2017 2:58 PM
To: Media; Chifley, Damien MR
Cc: West, Peter MR 2; Keesing, Col MR; s7 Wong, Sam; Wong, Sam MR; Wardle, Peter MR; Forth, John MR
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Media

DS&VS is not best placed to respond to this Media enquiry as it largely relates to export controls. I have provided some guidance to assist in responding to this request including potential POCs. The content below is not cleared for public release.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfil those obligations?

- Export Controls Branch is best placed to answer this question (I understand that these are legal obligations)
- I understand the company in question was part of the Australia Community not the Defence Industry Security Program. DS&VS through Security Operations Branch provide support to this initiative under export controls direction (Peter Wardle and John Forth can advise if required).

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

- Export Control Branch is best placed to answer.

Has it reviewed how Australian contractors generally maintain their ICT security?

- CIOG, ASD or ACSC (and CERT in AGD) are best placed to answer. I would suggest that ACSC report that led to this query is an example of Defence constantly reviewing and providing advice to industry broadly on good cyber security such as the Top 4 and Essential 8.

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

- DSVS is not aware of any general directive; however through our outreach and engagement the importance of good information security controls is emphasised in particular applying ASD recommended Essential 8.
- The CDIC play a role here (Sam Wong) – recent CDIC roadshow talking about good cyber security.
- ACSC play a role here s7

- CIOG play a role here (Col Keesing)

Kind regards
Steve

Steven Scanlan

A/g Assistant Secretary
Security Policy and Programs
Defence Security & Vetting Service
Department of Defence
t + 61 2 6266 3638 | e Steven.Scanlan@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Madge, Bronwyn MS
Sent: Thursday, 12 October 2017 1:50 PM
To: Scanlan, Steven MR
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Steve,

One for you,

Cheers,
Bronwyn

Bronwyn Madge | Director Vetting Governance and Review

a CP3-4-099
7 0133 e bronwyn.madge@defence.gov.au
HOURS

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 1:48 PM
To: Madge, Bronwyn MS
Cc: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon Bronwyn,

Please see attached for your action, if it could be returned to MECC ASAP it would be greatly appreciated.

SP&I have advised this is best tasked to you for a response (see below).

Kind regards,

Sarah Collins | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:37 PM
To: Media
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

I have also sent back the OpenText task with the comment below. SP is not the best placed to respond to the questions posed.

Regards,

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence
R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Chifley, Damien MR
Sent: Thursday, 12 October 2017 13:25
To: Holmback-Piggott, Louanne MS
Subject: RE: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Louanne,

I think that this is best responded to by DSVS who run the Defence Industry Security Program and this is all related to things that were the subject of recommendations from the review conducted last year.

I think it was called the Defence Industry Security Review.

The best bet would be Peter West's branch.

Thanks

Damien

Damien Chifley
Director Defence Export Assessments and Regimes
Defence Export Controls Branch

Department of Defence R1-1-A037 PO Box 7910 Canberra BC ACT 2610
phone +61 2 626 51122 | mobile s22 [REDACTED] | email damien.chifley@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Holmback-Piggott, Louanne MS
Sent: Thursday, 12 October 2017 1:16 PM
To: Chifley, Damien MR
Subject: FW: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

See attached, let me know if you are going to take it on.

Louanne

Louanne Holmback-Piggott | Assistant Director
Strategic Policy Division | Department of Defence
R1-01-A009 Russell Offices | PO Box 7901 | Canberra BC | ACT 2610
P: +61 2 6265 3800 | E: Louanne.Holmback-Piggott@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media
Sent: Thursday, 12 October 2017 13:14
To: SP&I-SP-Exec

Cc: SP&I Group Coord; Media

Subject: CT - 002945 - Contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please find attached the template for the below s47F enquiry.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACT 2600
P: +61 2 6127 1999
E: media@defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Media

Sent: Thursday, 12 October 2017 1:02 PM

To: SP&I-SP-Exec

Cc: SP&I Group Coord; Media

Subject: FW: Questions on contractor IT breach [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon SP,

Please see the below from s47F

I will template this up and send through for your action.

David has requested this by COB.

Happy to discuss.

Regards,

Nick

Nick Stewart | Public Affairs Officer
Defence Media | Department of Defence

Russell Offices | Canberra ACl 2600
P +61 2 6127 1899
E media@defence.gov.au

From: [REDACTED] s7 [REDACTED]@fairfaxmedia.com.au]
Sent: Thursday, 12 October 2017 12:23 PM
To: Media
Subject: Questions on contractor IT breach

Hi guys,

I have some questions on the data breach by a Defence contractor.

What obligations does Defence have to ensure that a contractor to the Defence Department is meeting ITAR obligations and what steps does it take to fulfill those obligations?

Has Defence reviewed since this incident how it oversees compliance with ITAR by Australian contractors?

Has it reviewed how Australian contractors generally maintain their ICT security?

Has Defence issued any general directive to contractors since this incident to remind them of their IT security obligations?

Can I get answers by 5pm?

thanks,

s47F [REDACTED]

Defence & National Security Correspondent

s47F [REDACTED]

Fairfax Media

The information contained in this e-mail message and any accompanying files is or may be confidential. If you are not the intended recipient, any use, dissemination, reliance, forwarding, printing or copying of this e-mail or any attached files is unauthorised. This e-mail is subject to copyright. No part of it should be reproduced, adapted or communicated without the written consent of the copyright owner. If you have received this e-mail in error please advise the sender immediately by return e-mail or telephone and delete all copies. Fairfax Media does not guarantee the accuracy or completeness of any information contained in this e-mail or attached files. Internet communications are not secure, therefore Fairfax Media does not accept legal responsibility for the contents of this message or attached files.

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.