From: Agostino, Julia
To: Row, Stuart
Subject: FW: Decision on access application
Date: Wednesday, 16 September 2020 3:23:43 PM

Dear Stuart

Please find my FOI decision, below and attached documents for OLA's disclosure log which can be updated from Tuesday of next week, as per s28(4) of the FOI Act.

Kind regards

Julia

From: Agostino, Julia
Sent: Wednesday, 16 September 2020 3:21 PM
To: [redacted]
Subject: Decision on access application

[redacted]

DECISION ON YOUR ACCESS APPLICATION

I refer to your access application made under the *Freedom of Information Act 2016* (FOI Act), dated 31 August 2020 and received by the Office of the Legislative Assembly (OLA) by email on the same date.

This application requested access to: *Documents related to the Canberra Liberals delegation - MLAs and their staff - to China in March 2019.*

I am an Information Officer appointed by the Clerk of the Legislative Assembly for the ACT under section 18 of the Act to deal with access applications made under Part 5 of the Act.

Decision

I have identified 13 documents containing information within the scope of your access application. These are outlined in the attached Schedule of Documents.

I have decided to give full access to all documents identified, so far as they relate to your access application.

You will note several redactions. I advise that the information redacted is not within the scope of your request. Specifically, documents 1 and 7 contain information that is unrelated to your request because it is (a) personal relating to the correspondent; and (b) relating to a different matter; document 9 includes all action items from the Speaker's meeting, not just that related to your access application.

Disclosure log

Please note that section 28 of the FOI Act requires publication of access applications and any information subsequently released on our disclosure log which can be accessed at: https://www.parliament.act.gov.au/f/tru/resource-center/freedom-of-information_test

This means that if access to the information is granted, it will also be made publicly available on our website, unless the access application is an application for your personal, business, commercial, financial or professional information.

Review rights

You may apply to the ACT Ombudsman to review my decision under section 73 of the FOI Act.

An application for review must be made in writing within 20 days of receipt of this decision notice.

You may submit a request for review of my decision to the ACT Ombudsman by writing in one of the following ways:

Email (preferred):	actfoi@ombudsman.gov.au
Post:	The ACT Ombudsman GPO Box 442 CANBERRA ACT 2601

More information about the ACT Ombudsman review is available on their website at www.ombudsman.act.gov.au.

Yours sincerely

Julia Agostino
Deputy Clerk and Serjeant-at-Arms of the Legislative Assembly for the Australian Capital Territory
P 02 62050171 | F 02 62053109 |M 0466 028 562| E julia.agostino@parliament.act.gov.au
Please note that I do not work every second Friday.

The Office of the Legislative Assembly:
Providing professional services and reliable, impartial
advice to support, strengthen and promote the institution
of parliament in the ACT.

www.parliament.act.gov.au

Schedule of documents

[redacted] – *OLA*

Document reference number	Page number	Date	Description	Decision	Category or Factor
1.	1-2	11 February 2019	Email regarding Liberal members' and staffers' trip to China	Release	Redacted information is out of scope.
2.	3-4	4 August 2020	Emails regarding timesheets for travel	Release	
3.	5-6	18 March 2019	Emails between OLA staff and Liberal members regarding mobile devices and travel overseas	Release	
4.	7-9	1 March 2019 – 18 March 2019	Emails between OLA staff and Nicole Lawder regarding mobile devices and travel overseas	Release	
5.	11-13	11- 26 February 2019	Emails between OLA and JACS staff regarding Assembly ICT devices	Release	
6.	15	19 February 2019	Email containing proposed advice about using Assembly ICT devices whilst overseas	Release	
7.	17	17 February 2019	Emails regarding trip	Release	Redacted information is out of scope.
8.	19	12 February 2019	Email between Clerk and Speaker regarding trip	Release	

9.	21-22	11 February 2019	Record of Actions from Speaker's meeting	Release	Redacted information is out of scope.
10.	23-24	4 and 11 February 2019	Media Release forwarded in emails of 4 and 11 February 2019	Release	
11.	25-27	Undated	Untitled document about maintaining secure ICT devices whilst overseas	Release	
12.	28-35	Undated	Australian Government - Business Liaison Unit: BLU Travel Advice pamphlet	Release	
13.	26	Undated	ACT Government Contact Reporting and Awareness Scheme pamphlet	Release	

***Please note: blank pages are backs of scanned documents and have not been listed in this table**

From: Duncan, Tom
To: Agostino, Julia
Cc: Duckworth, Ian
Subject: [redacted]
Date: Monday, 31 August 2020 1:17:20 PM
Attachments: image001.png

Julia

In anticipation of your request for documents, this is the only email I have.

Tom Duncan
Clerk of the Legislative Assembly
P 02 620 50191 | E tom.duncan@parliament.act.gov.au

Office of the Legislative Assembly:
Professionalism • Independence • Honesty • Integrity • Impartiality • Transparency
www.parliament.act.gov.au

From: Duckworth, Ian
Sent: Monday, 11 February 2019 9:06 AM
To: Duncan, Tom <Tom.Duncan@parliament.act.gov.au>
Cc: Rogers, Emma <Emma.Rogers@parliament.act.gov.au>
Subject: [redacted]

[redacted]

When you're in, let's talk 3 Lib MLAs + 7 Advisers on a "self-funded" trip to China. I could be wrong but my instinct tells me that some assumptions may have been made about how this will work and we may have to provide some advice to clarify things.

You will, or may, have your own issues/ queries but, from my perspective:

- it appears that it would not categorised as Assembly business - unless the Speaker ruled it so [redacted]
- participating advisers would not be regarded as on duty and would need to take leave of absence [redacted]
- the Territory would not provide travel insurance;
- Assembly provided ICT devices could not be taken into China.

[redacted]

[redacted]

Let's chat

Ian Duckworth
Executive Manager, Business Support | Office of the Legislative Assembly
Phone: (02) 6205 0181 | Mobile: 0417 663389
Email: ian.duckworth@parliament.act.gov.au
GPO Box 1020 Canberra ACT 2601
www.parliament.act.gov.au

The Office of the Legislative Assembly:
Providing professional services and reliable, impartial
advice to support, strengthen and promote the institution
of parliament in the ACT.

Please consider our environment before printing this e-mail.

-----Original Message-----
From: Duncan, Tom
Sent: Monday, 11 February 2019 7:46 AM
To: Pearce, Hannah <Hannah.Pearce@parliament.act.gov.au>; Agostino, Julia <Julia.Agostino@parliament.act.gov.au>; Duckworth, Ian <Ian.Duckworth@parliament.act.gov.au>
Subject: [redacted]

[redacted]

Duckworth, Ian

From: Rogers, Emma
Sent: Tuesday, 4 August 2020 4:53 PM
To: Duckworth, Ian
Subject: FW: Timesheets - China [SEC=UNCLASSIFIED]

UNCLASSIFIED

Emma Rogers
Payroll Project Manager | Business Support Branch
P 02 62050150 | E emma.rogers@parliament.act.gov.au

From: Duckworth, Ian <Ian.Duckworth@parliament.act.gov.au>
Sent: Tuesday, 30 April 2019 7:29 PM
To: Prentice, Malcolm <Malcolm.Prentice@parliament.act.gov.au>
Cc: Rogers, Emma <Emma.Rogers@parliament.act.gov.au>
Subject: FW: Timesheets - China [SEC=UNCLASSIFIED]

Mal

This is an issue that the Speaker has taken a keen interest in. As of last Monday, my advice to her was we still thought there were two of the apparent seven who went on the trip who we had not been able to identify and that Emma was liaising closely with Steven Kryger to sort it out.

But this advice – which I do not intend to challenge – explains that there were only five, not seven, staff who went along. So, next Monday, it will be desirable for you to explain to the Speaker that the issue has been resolved to our satisfaction and that all staff who went on the trip used TOIL.

Case closed!

Ian Duckworth
Executive Manager, Business Support | Office of the Legislative Assembly
Phone: (02) 6205 0181 | Mobile: 0417 663389
Email: ian.duckworth@parliament.act.gov.au
GPO Box 1020 Canberra ACT 2601
www.parliament.act.gov.au

The Office of the Legislative Assembly:
Providing professional services and reliable, impartial advice to support, strengthen and promote the institution
of parliament in the ACT.

From: Rogers, Emma
Sent: Tuesday, 30 April 2019 1:45 PM
To: Duckworth, Ian <Ian.Duckworth@parliament.act.gov.au>
Subject: FW: Timesheets - China [SEC=UNCLASSIFIED]

FYI

Emma Rogers
Manager, HR and Entitlements
P 02 62050150 | F 02 62050442 | E
emma.rogers@parliament.act.gov.au

From: Kryger, Steven
Sent: Tuesday, 30 April 2019 12:34 PM
To: Rogers, Emma <Emma.Rogers@parliament.act.gov.au>
Subject: Re: Timesheets question [SEC=UNCLASSIFIED]

Yes

From: "Rogers, Emma" <Emma.Rogers@parliament.act.gov.au>
Date: Tuesday, 30 April 2019 at 12:33 pm
To: "Kryger, Steven" <Steven.Kryger@parliament.act.gov.au>
Subject: Timesheets question [SEC=UNCLASSIFIED]

Hi Steven

I am just finishing up an audit of timesheets, which include staff who travelled to China. As discussed earlier today, can I confirm with you that there were only five staff members who travelled to China and not seven, which was reported in the media?

Many thanks,

Emma Rogers
Manager, HR and Entitlements
Business Support Branch
P 02 62050150 | E emma.rogers@parliament.act.gov.au
GPO Box 1020 Canberra ACT 2601

The Office of the Legislative Assembly:
Providing professional services and reliable, impartial advice to support, strengthen and promote the institution of parliament in the ACT.

http://www.parliament.act.gov.au

Duckworth, Ian

From: Kryger, Steven
Sent: Monday, 18 March 2019 12:12 PM
To: Szychowska, Valeria
Subject: CM9: Re: Mobile devices and overseas travel [SEC=UNCLASSIFIED]

Hi Val,

I can confirm that no Assembly devices were taken or used by members and/or their staff while they were in China. No USBs or Bluetooth devices were received as gifts or purchased while in China.

Steve

From: "Szychowska, Valeria" <Valeria.Szychowska@parliament.act.gov.au>
Date: Monday, 18 March 2019 at 11:35 am
To: "Kryger, Steven" <Steven.Kryger@parliament.act.gov.au>
Subject: RE: Mobile devices and overseas travel [SEC=UNCLASSIFIED]

Thank you for returning my call Steven,
As discussed, please see my email advice below. I didn't receive a response from Mr Coe or Mr Milligan on this so I'm just following up to make sure that no mobile devices were taken or used by members and/or their staff while they were I China.

The attached provides important information on the measures that should be taken to protect mobile devices and the information stored on them when travelling to high security risk countries such as China. Suggest you please read the information and let me know if anyone has any concerns.

Also, if members or staff received any gifts while they were in China, in the form of USB or Bluetooth enabled devices, I can arrange for those to be checked by the SSICT security team to ensure that they do not pose a threat to the Assembly and ACT Government IT network.

Regards, Val Szychowska
Assembly IT Manager
Civic Square, 196 London Circuit (GPO Box 1020) CANBERRA ACT 2601
T 02 62050126 | F 02 62050025 | E valeria.szychowska@parliament.act.gov.au

From: Szychowska, Valeria
Sent: Friday, 1 March 2019 4:15 PM
To: Coe, Alistair <Alistair.Coe@parliament.act.gov.au>; Lawder, Nicole <Nicole.Lawder@parliament.act.gov.au>; Milligan, James <James.Milligan@parliament.act.gov.au>
Subject: Mobile devices and overseas travel [SEC=UNCLASSIFIED]
Importance: High

Hello Mr Coe, Ms Lawder and Mr Milligan,
Hope you are well.

I am just following up on some advice I received, that you and/or your staff are planning an overseas trip to China that is privately funded and non-Assembly business related, correct?

Uncertain on whether you or your staff are planning to take any Assembly and/or privately owned mobile devices on your trip, however, I must advise you that OLA sought advice from JACS' recently about the security posture of China for another travel requirement and JACS confirmed that China is a high security risk destination.

Given the above and the potential security risks associated with using mobile devices in China, please note the following:

a) Assembly provided mobile devices such as laptops and iPads must not be taken to any high risk security destination, including China
b) It is recommended that privately owned mobile devices should not be taken to China either, instead, new mobile devices and chargers should be purchased and used while in China
c) If you or your staff intend on taking privately owned mobile devices to China:
    a) I must arrange for the attached remote access services (i.e. MobileIron and Acronis) to be disabled before the device leaves Australia
    b) I will arrange for those services to be restored when the devices return to Australia
    c) For me to arrange the above, I need to know which devices you plan to take and the dates you will be in China.

Other important things to note when taking mobile devices to China:

a) All SIM cards in mobile devices should be removed or disabled
b) All Wi-Fi services should be disabled when not in use and only connect to trusted hotspots
c) You may access your Assembly mailbox using Outlook Web Access (OWA), however, you must register for Multi-factor Authentication (MFA) first
d) MFA must be setup while you are logged into the Assembly IT network as you will not be able to do this outside the network.
   The Assembly IT Support Office can assist you with this
e) You should maintain full possession/control of your mobile device as well as the power adaptor (including charger and cable)
f) If the mobile device and/or charger goes missing, or you leave it unattended anywhere, including a hotel room, consider those devices compromised.
   Travellers have reported their mobile devices and/or charging equipment being installed with hacking devices, and in some cases, the chargers were replaced with similar chargers with built-in hacking devices.

Please let me know if you require further clarification on the above, otherwise, let me know whether I should arrange for any remote access services to be disabled before you or your staff go on this trip.

Thank you, Val Szychowska
Assembly IT Manager
Civic Square, 196 London Circuit (GPO Box 1020) CANBERRA ACT 2601
T 02 62050126 | F 02 62050025 | E valeria.szychowska@parliament.act.gov.au

Duckworth, Ian

From: Lawder, Nicole
Sent: Monday, 18 March 2019 5:40 PM
To: Szychowska, Valeria
Subject: CM9: RE: Mobile devices and overseas travel [SEC=UNCLASSIFIED]

Thanks

Nicole Lawder MLA | Member for Brindabella | ACT Legislative Assembly
Deputy Leader of the Opposition

GPO Box 1020 Canberra ACT 2601

P: (02) 6205 0323
E: lawder@parliament.act.gov.au

From: Szychowska, Valeria
Sent: Monday, 18 March 2019 10:58 AM
To: Lawder, Nicole <Nicole.Lawder@parliament.act.gov.au>
Subject: RE: Mobile devices and overseas travel [SEC=UNCLASSIFIED]

Good morning Ms Lawder.
Just following up on your trip to China recently.

The attached provides important information on the measures that should be taken to protect your mobile devices and the information stored on them when travelling to high security risk countries. Would you please read the information and let me know if you have any concerns.

Please note that if you or your staff received any gifts in the form of USB or Bluetooth enabled devices, I can arrange for those to be checked by the SSICT security team to ensure that they do not pose a threat to the Assembly and ACT Government IT network.

Thanks, Val
Assembly IT Manager - x50126

From: Lawder, Nicole
Sent: Monday, 4 March 2019 8:49 AM
To: Szychowska, Valeria <Valeria.Szychowska@parliament.act.gov.au>
Subject: RE: Mobile devices and overseas travel [SEC=UNCLASSIFIED]

Thanks not planning to take Assembly iPad.
Regards

8

Nicole

Nicole Lawder MLA | Member for Brindabella | ACT Legislative Assembly
Deputy Leader of the Opposition

GPO Box 1020 Canberra ACT 2601

P: (02) 6205 0323
E: lawder@parliament.act.gov.au

From: Szychowska, Valeria
Sent: Friday, 1 March 2019 4:15 PM
To: Coe, Alistair <Alistair.Coe@parliament.act.gov.au>; Lawder, Nicole <Nicole.Lawder@parliament.act.gov.au>; Milligan, James <James.Milligan@parliament.act.gov.au>
Subject: Mobile devices and overseas travel [SEC=UNCLASSIFIED]
Importance: High

Hello Mr Coe, Ms Lawder and Mr Milligan,
Hope you are well.

I am just following up on some advice I received, that you and/or your staff are planning an overseas trip to China that is privately funded and non-Assembly business related, correct?

Uncertain on whether you or your staff are planning to take any Assembly and/or privately owned mobile devices on your trip, however, I must advise you that OLA sought advice from JACS' recently about the security posture of China for another travel requirement and JACS confirmed that China is a high security risk destination.

Given the above and the potential security risks associated with using mobile devices in China, please note the following:

a) Assembly provided mobile devices such as laptops and iPads must not be taken to any high risk security destination, including China
b) It is recommended that privately owned mobile devices should not be taken to China either, instead, new mobile devices and chargers should be purchased and used while in China
c) If you or your staff intend on taking privately owned mobile devices to China:
    a) I must arrange for the attached remote access services (i.e. MobileIron and Acronis) to be disabled before the device leaves Australia
    b) I will arrange for those services to be restored when the devices return to Australia
    c) For me to arrange the above, I need to know which devices you plan to take and the dates you will be in China.

Other important things to note when taking mobile devices to China:

a) All SIM cards in mobile devices should be removed or disabled
b) All Wi-Fi services should be disabled when not in use and only connect to trusted hotspots
c) You may access your Assembly mailbox using Outlook Web Access (OWA), however, you must register for Multi-factor Authentication (MFA) first

d) MFA must be setup while you are logged into the Assembly IT network as you will not be able to do this outside the network.
   The Assembly IT Support Office can assist you with this
e) You should maintain full possession/control of your mobile device as well as the power adaptor (including charger and cable)
f) If the mobile device and/or charger goes missing, or you leave it unattended anywhere, including a hotel room, consider those devices compromised.
   Travellers have reported their mobile devices and/or charging equipment being installed with hacking devices, and in some cases, the chargers were replaced with similar chargers with built-in hacking devices.

Please let me know if you require further clarification on the above, otherwise, let me know whether I should arrange for any remote access services to be disabled before you or your staff go on this trip.

Thank you, Val Szychowska
Assembly IT Manager
Civic Square, 196 London Circuit (GPO Box 1020) CANBERRA ACT 2601
T 02 62050126 | F 02 62050025 | E valeria.szychowska@parliament.act.gov.au

Duckworth, Ian

From: Wilson, Dougal
Sent: Tuesday, 26 February 2019 9:33 AM
To: Duckworth, Ian
Cc: Howard, Scott; Szychowska, Valeria
Subject: RE: Opposition delegation travelling O/S [DLM=For-Official-Use-Only]

Ian

Just to confirm, the Opposition delegation will not be taking any ACT Government ICT equipment with them to China?

Regards

Dougal Wilson | Assistant Director | Protective Security Policy
Phone: +61 2 6205 8196| Fax: +61 2 6207 8339| Email: dougal.wilson@act.gov.au
Security & Emergency Management Branch | **Justice and Community Safety** | ACT Government

---

From: Duckworth, Ian
Sent: Tuesday, 26 February 2019 8:03 AM
To: Wilson, Dougal <Dougal.Wilson@act.gov.au>
Cc: Howard, Scott <Scott.Howard@parliament.act.gov.au>; Szychowska, Valeria <Valeria.Szychowska@parliament.act.gov.au>
Subject: Re: Opposition delegation travelling O/S [DLM=For-Official-Use-Only]

Sorry Dougal - I've been away myself. The trip is not regarded as Assembly business- the information we have is that the trip is entirely private so, other than instructors we will give about non use of Assembly ICT devices and warnings about introducing any phone chargers or portable thumb drives, etc, there is no briefing required.

Sent from my iPhone

On 22 Feb 2019, at 9:00 am, Wilson, Dougal <Dougal.Wilson@act.gov.au> wrote:

> Ian, Scott or Val
>
> Do we have any further information on the Opposition delegation travelling to China?
>
> Regards
>
> **Dougal Wilson** | Assistant Director | Protective Security Policy
> Phone: +61 2 6205 8196| Fax: +61 2 6207 8339| Email: dougal.wilson@act.gov.au
> Security & Emergency Management Branch | **Justice and Community Safety** | ACT Government

From: Duckworth, Ian
Sent: Monday, 11 February 2019 5:15 PM
To: Wilson, Dougal <Dougal.Wilson@act.gov.au>
Cc: Burkevics, Bren <Bren.Burkevics@act.gov.au>; Duncan, Tom <Tom.Duncan@parliament.act.gov.au>
Subject: RE: Members of the Opposition travelling O/S [DLM=For-Official-Use-Only]

Dougal

Thanks. We're still exploring from this end the extent to which the Assembly is – or should be – associated with this travel proposal and so, over the coming days, I expect to find out more.

I will keep you posted.

Ian Duckworth
Executive Manager, Business Support | Office of the Legislative Assembly
Phone: (02) 6205 0181 | Mobile: 0417 663389
Email: ian.duckworth@parliament.act.gov.au
GPO Box 1020 Canberra ACT 2601
www.parliament.act.gov.au

<image002.jpg>

The Office of the Legislative Assembly:
Providing professional services and reliable, impartial advice to support, strengthen and promote the institution of parliament in the ACT.


Please consider our environment before printing this e-mail.

From: Wilson, Dougal
Sent: Monday, 11 February 2019 12:36 PM
To: Duckworth, Ian <Ian.Duckworth@parliament.act.gov.au>
Cc: Burkevics, Bren <Bren.Burkevics@act.gov.au>
Subject: Members of the Opposition travelling O/S [DLM=For-Official-Use-Only]

Ian

I raised the matter of providing a security briefing to Opposition members with Bren and following clearance from CMO we've been given the go ahead.

If you could confirm when they will be travelling I can start co-ordinating with ASIO a time and date to provide the delegation with a defensive travel briefing. We try to conduct these briefings in the week immediately prior to departure so information is as up to date as it can be.

Regards

Dougal Wilson | Manager |Protective Security Policy
Phone: +61 2 6205 8196| Fax: +61 2 6207 8339| Email: dougal.wilson@act.gov.au
Security & Emergency Management Branch | **Justice and Community Safety** | ACT Government

Duckworth, Ian

From: Row, Stuart
Sent: Tuesday, 19 February 2019 3:22 PM
To: Duckworth, Ian
Subject: China IT security [SEC=UNCLASSIFIED]

Ian,

Is this the kind of thing you are after?

The following security advice relates to the feasibility of taking Assembly IT hardware to China:

- Laptops – not to be taken into China. They will be considered to be compromised upon return.
- Mobile phones – may be taken, but all remote access services to the Assembly IT network must be disabled. Connection via trusted W-Fi networks is acceptable when required and can be used to access mailboxes via OWA.
- USB drives or other storage devices – not to be taken and/or returned as they will be considered to be compromised.

Note that mobile phones and chargers should remain in the user's control at all times. If they go missing or are left in hotel rooms they will be considered to be compromised as there is a high chance they may have had hacking devices installed.

Gifts received during your stay should also be treated with caution as they may be fitted with some form of surveillance or hacking technology.

Cheers,

Stuart Row
Manager, Information and Digital Services | Office of the Legislative Assembly
T (02) 6207 5919 |E stuart.row@parliament.act.gov.au

Duckworth, Ian

From: Duncan, Tom
Sent: Sunday, 17 February 2019 4:40 PM
To: Duckworth, Ian
Subject: Opposition China trip

We may get asked about this tomorrow. I know you have received assurances that it is all private and leave is being taken, but have we covered insurance /security issues?

[redacted] I'll pop over @ 9.30ish and we can discuss.

Sent from my iPad

Begin forwarded message:

> **From:** "Burch, Joy" <Joy.Burch@parliament.act.gov.au>
> **Date:** 12 February 2019 at 4:08:07 pm AEDT
> **To:** "Duncan, Tom" <Tom.Duncan@parliament.act.gov.au>
>
> Leading a delegation. Have you had any talks with them yet

Duckworth, Ian

From: Duncan, Tom
Sent: Tuesday, 12 February 2019 4:14 PM
To: Burch, Joy
Cc: Duckworth, Ian
Subject: China delegation

Madam Speaker

I haven't but I'll check with Ian.

Sent from my iPad

On 12 Feb 2019, at 4:08 pm, Burch, Joy <Joy.Burch@parliament.act.gov.au> wrote:

> Leading a delegation. Have you had any talks with them yet

LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

SPEAKER'S MEETING

RECORD OF ACTIONS REQUIRED
MONDAY, 11 FEBRUARY 2019
10.00 AM

Attendees:	Madam Speaker	Tom Duncan (Clerk)
		Julia Agostino (Deputy Clerk)
		Ian Duckworth (Executive Manager)
Apology:	Melinda Gonczarek (Chief of Staff)	Hannah Pearce (Acting Executive Project Officer)

The meeting began at 10.05 am.

The Speaker was briefed on the following matters—

	Action Item	Responsible officer
1.	[redacted]	[redacted]
2.		
3.		
4.		

Action Item	Responsible officer
5. Other Business – [redacted] [redacted] – Self-funded delegation to China by the Leader of the Opposition, Deputy Leader of the Opposition and Mr Milligan, including 7 advisors. Action: Clerk to add item to agenda for the next Standing Committee on Administration and Procedure if matter is not discussed with the Leader of the Opposition before the meeting. – [redacted]	Clerk

The meeting concluded at 10.51 am.

Duckworth, Ian

From: Duncan, Tom
Sent: Tuesday, 4 August 2020 4:31 PM
To: Duckworth, Ian
Subject: FW: MEDIA RELEASE: Canberra Liberals to visit China [SEC=UNCLASSIFIED]

Tom Duncan
Clerk of the Legislative Assembly
P 02 620 50191 | E tom.duncan@parliament.act.gov.au

Office of the Legislative Assembly:
Professionalism • Independence • Honesty • Integrity • Impartiality • Transparency
www.parliament.act.gov.au

From: LA Library
Sent: Monday, 11 February 2019 7:55 AM
Subject: MEDIA RELEASE: Canberra Liberals to visit China [SEC=UNCLASSIFIED]

Alistair Coe MLA
ACT Leader of the Opposition
Member for Yerrabi

MEDIA RELEASE
Sunday February 10, 2019

Canberra Liberals to visit China

Strengthening Canberra's economic and cultural ties will be the focus of the first ever delegation to China by an ACT Opposition, Canberra Liberals Leader Alistair Coe said.

In the lead-up to the 20th anniversary since Liberal Chief Minister Kate Carnell established a sister city relationship with Beijing, Canberra Liberals Leader Alistair Coe said he is proud to be leading a delegation that will strengthen Canberra's connections with China.

"Almost twenty years ago, Canberra and China embarked on a journey to develop mutually rewarding ties in business, education, culture and trade," Mr Coe said.

The self-funded delegation will focus on education, tourism, aviation, IT, health as well as developing relationships with provincial and municipal governments.

"Our cities can learn a lot from each other," Mr Coe said.

"There are already many Canberra businesses that have strong relationships with businesses in China.

"Our education, technology, construction and tourism industries all have strong links to Chinese markets.

"We have thousands of citizens, residents, students and visitors that come from China that contribute enormously to our City. The Canberra Liberals appreciate their contribution to Canberra and look forward to further developing our relationship with China.

When: March 9 – 16, 2019

Where: The delegation will visit Beijing, Shanghai, Fuzhou and Xiamen

Why: To strengthen economic and cultural ties with China

Media contact Deborah Seccombe:
P (02) 6205 1580 **M** 0451 255 891 **E** Deborah.seccombe@parliament.act.gov.au

Excerpt from Minister and Senior Executive Protective Security Protocol

Portable Electronic Devices

Smartphones, tablets and notebooks share many of the vulnerabilities of larger desktop computers but the attributes that make them easy to carry, use, and modify open them to a range of attacks. The very portability of small electronic devices makes them easy to steal giving a determined attacker enough time to defeat most security features and gain access to any stored information.

Seemingly legitimate software applications can also pose a serious security risk if privileged or sensitive information is stored on electronic devices. These applications have been developed to by-pass operating system security features and access or download stored information. Even legitimate device software can be exploited allowing attackers to eavesdrop, crash phone software, or conduct other attacks.

To safeguard against information security risks associated with portable electronic devices the following actions are recommended:

- minimise the amount of privileged or sensitive information stored on devices that are regularly taken out of secure environments such as executive offices or the Legislative Assembly building;
- do not connect devices to courtesy recharge points;
- do not use your device to transmit sensitive information, where possible;
- keep your device secure or in your possession at all times;
- consider the security of the accessories connected to your device (Bluetooth keyboards etc); and
- Report the loss, theft or suspected compromise of any device(s) to SSICT and SEMB as soon as possible.

Travelling Overseas – prior to travel

Members of Australian Government Delegations, including Ministers, staff and contractors, have been and will continue to be attractive targets for foreign intelligence services during official travel. Portfolios relevant to trade, finance, infrastructure, security and legal policy are likely to attract attention from foreign intelligence services. Foreign Intelligence agencies are seeking to obtain understanding into how Australia considers business decisions.

All business and social engagements present an opportunity for individuals, be they foreign operatives, political activities, commercial entities or criminals, to acquire information.

Before you travel with official information

- Review the publicly accessible information that exists about you as an individual. Your presence on social media, public internet sites and memberships lists or publications may describe where you work, and the nature of work you undertake, increasing the likelihood that you are a 'person of interest'.

- Avoid using the social media features of travel organiser software (such as Tripit, Worldmate, Kayak, Traxo and the like) to broadcast your precise dates, locations and travel intentions on the web.

- Only take the minimum amount of information you require to conduct your affairs in public locations or while abroad.

For those members with ACT Government issued ICT devices it is recommended that Shared Services ICT (SSICT) is consulted, prior to travel, to assist with the following:

- baseline (back up) the device prior to departure and again on return;
- disable unnecessary features and software;
- check latest antivirus and firewall protection products are installed;
- minimise administrative privileges on the device; or
- request the issue of a 'clean' device for overseas use only.

Travelling Overseas – Precautions in a foreign country

Information security

All nations maintain some form of security service that share a common purpose, gathering information to protect or promote their country's interests. Travelling overseas will put you on foreign intelligence services (FIS) home ground, subject to local laws that may include inspecting personal luggage and surrendering electronic devices for examination.

The greatest advantage to be gained by FIS is when a target is unaware that their information security has been breached. To enable this without tipping their hand intelligence gathering is a long game and relies on collecting small bits of information to build a bigger picture, known as aggregation of data.

While the information you carry might not appear overly significant all of it is valuable to a FIS.

Safeguarding official information while overseas:

- Understand the information you are carrying and protect privileged information;
- Carry all sensitive information irrespective of the form (paper documents, computer, mobile devices) on your person;
- Never check it in, or leave any sensitive information unattended including in hotel room safes or in safety deposit boxes with reception;
- Do not plug your information assets into unknown devices (such as docking stations provided in hotel rooms and lobbies);
- Do not permit others to plug devices into your information assets;
- Treat your password, log-in and on-screen information as you would your personal banking PIN;
- Disable wireless and Bluetooth capabilities and the ability to 'auto join' networks.

Personal security

While in a foreign country the following actions are recommended:

- Ensure you know the whereabouts of your travel delegation;
- Be aware of your surroundings;
- Have an emergency plan with contact numbers;
- Use lockable luggage;
- Identify the closest Australian Embassy or Consulate for emergencies; and
- Understand the information you are carrying and protect privileged information.
- Free USB keys, DVD's, CD's and software may contain malicious code which is designed to steal, harm or otherwise compromise your security
- Accept 'gifts' but do not use them.
- Report loss, theft or suspicious activities to SEMB or your Agency Security Executive.

Australian Government

Business Liaison Unit

BLU travel advice

BLU travel advice

This guide highlights security issues to be aware of and personal precautions you can take during overseas business travel.

This guide does not provide exhaustive advice on travel safety. General travel security information can be obtained from the Department of Foreign Affairs and Trade (DFAT) travel advisory website.

www.smartraveller.gov.au

Protect Yourself

Before you travel

Research your destination and the security situation.

Access DFAT country specific travel advisories and subscribe to receive email updates.

Register your travel and contact details with DFAT, or once you arrive with the local Australian Embassy, High Commission or Consulate.

Take copies of important documents with you (passport, tickets, visas, travellers' cheques, credit card numbers, insurance policy and phone card details) and keep separate to the originals.

Inform others of your travel plans and supply them with copies of your itinerary and important documents.

Ensure you have comprehensive travel insurance and check what circumstances and activities are not covered by your policy.

Take relevant contact details with you in case of an emergency.

While you are travelling

Business travellers present a potentially vulnerable target and you should put measures in place to ensure your physical security. Report any suspicious activity to your security manager.

Be aware of your surroundings and alert to anything that arouses suspicion about your own personal safety, including:

- Unusual contact or undue or persistent questioning not consistent with a given situation or professional dealing;
- Suspicion of being followed;
- Suspicion of locks being tampered with;
- Incidents of theft or suspected or actual break-ins (including premises and vehicles);
- Unusual behaviour by domestic staff;
- Photography and filming;
- Packages or bags left unattended; and
- Vehicles that appear 'out of place'.

Terrorism

Terrorism is an ongoing threat in many countries and attacks can occur without warning. Australians could be caught up in attacks directed at others.

When planning your travel, consider the kind of places known to be terrorist targets—including those frequented by foreigners and symbols or infrastructure associated with government, military or Western interests—and the level of security provided.

You should avoid demonstrations and protests as they may turn violent.

Espionage

Corporate espionage is an increasingly serious threat for the business traveller. In many countries, the activities of intelligence services can extend to collection of information for the strategic gain of their business community.

Foreign intelligence services benefit from a 'home advantage' and will take an opportunistic approach to obtaining information. Targeting methods include luggage searches, extensive questioning and manipulation of mobile and electronic devices. In addition, personal approaches from intelligence services may be undertaken for the purpose of cultivation or compromise of an individual to gain insider access to company information.

Australian business travellers should be alert to the possibility of covert collection of sensitive information and take measures to ensure not only the safety and security of themselves, but also their business information.

If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained.

At the airport:

- Lock your luggage to prevent tampering and theft.
- Do not check your laptop in as luggage. Carry sensitive material, laptops, removable media and valuables with you.
- Avoid luggage being taken out of your sight during inspection.
- Inspect locks and contents of luggage for evidence of tampering.
- Be aware airport security checkpoints are particularly vulnerable areas for theft.

At the hotel:

- Upon arrival ensure your hotel room matches the reservation.
- Be aware hotel rooms and safes are not secure.
- Do not discuss your movements while in the room or on your personal or room telephone.
- Do not leave documents, identification papers, itineraries or any electronic devices in the room.

Protect Your Information

- Reduce sensitive material and equipment to a minimum.
- Be discrete about work and personal circumstances.
- Be aware of suspicious and/or persistent approaches or contact.
- Beware of 'phishing'—foreign security services and criminals may present as someone you trust to obtain personal or sensitive information.
- Be aware your conversations may not be private or secure, even within what is considered to be 'secure premises' such as meeting venues, hotel rooms or offices.
- Do not use non-company computers to log into your company's network. Always consider any information conveyed through a non-company computer to be compromised, even if it is encrypted.
- Be wary of using computers in airport lounges, hotels and internet cafes.

Electronic devices

- If feasible, use a ‘clean’ laptop, phone and email account while travelling.
- Patch applications and operating systems— ensure up-to-date firewalls, encryption and anti-virus software is installed. Implement application whitelisting and limit administration privileges.
- Ensure strong passwords are used and they are not stored with the laptop. Change all passwords when you return.
- Back-up your data before you travel.
- Disable Bluetooth and wireless capabilities and the ability to ‘auto-join’ networks, as well as any other feature or software not required for the trip.
- Do not connect to open Wi-fi networks for business purposes. Only wireless connections that are needed and can be secured should be enabled.
- Avoid connecting removable media and electronic storage devices to your device.
- Avoid connecting phones to hotel docking stations as these can be used to upload malicious software.
- Encrypt emails where possible.
- Clear your internet browser after each use: delete history files, caches, cookies, URL and temporary internet files.
- Do not leave electronic devices unattended.
- Use a non-descript carrying case for laptops.
- When you return check all your electronic devices for malicious software or evidence of compromise.
- For further information security advice and mitigation strategies access the Defence Signals Directorate website at www.dsd.gov.au.
- CERT Australia is the single point of contact for cyber security issues affecting Australian businesses. In the event of compromise, or for further assistance, contact info@cert.gov.au or 1300 172 499.

Further Information

ASIO's Business Liaison Unit

» Access the website at www.blu.asio.gov.au or contact (02) 6234 1668.

CERT Australia

» Access the website at www.cert.gov.au.

Department of Foreign Affairs and Trade

» Further travel advice is available on the Smart Traveller website at www.smartraveller.gov.au

» DFAT 24-hour Consular Emergency Centre: 1300 555 135 (from within Australia) (+61 2) 6261 3305 (from overseas)

» In Australia, DFAT in Canberra may be contacted on (02) 6261 3305.

» Contact details for Australian Embassies, High Commissions and Consulates are available at www.dfat.gov.au/missions/index.html.

Notes

Contact Reporting Form

Details of Contact

(If space is insufficient, please include an attachment)

Time: .....

Date: .....

Location: .....

Means of Contact: .....

In Person ☐

Telephone ☐

Correspondence ☐

If Other, please specify:

.....

.....

.....

Names of Persons Present (including Designations and Nationality):

.....

.....

.....

Reason or Occasion:

Business ☐

Social ☐

Personal ☐

Official ☐

Incidental ☐

Other ☐

Contact Initiated By ☐

Unit or Firm Rep ☐

Foreign Rep ☐

Other ☐

If Other, please specify:

.....

.....

.....

Topics of Conversation Significant to Security (Or details of incident):

.....

.....

.....

Further Contact (Outline any arrangements made):

.....

.....

.....

Details of Person Making the Report

.....

Signature

(Hard Copy Only)

Printed Name: .....

Designation/Position: .....

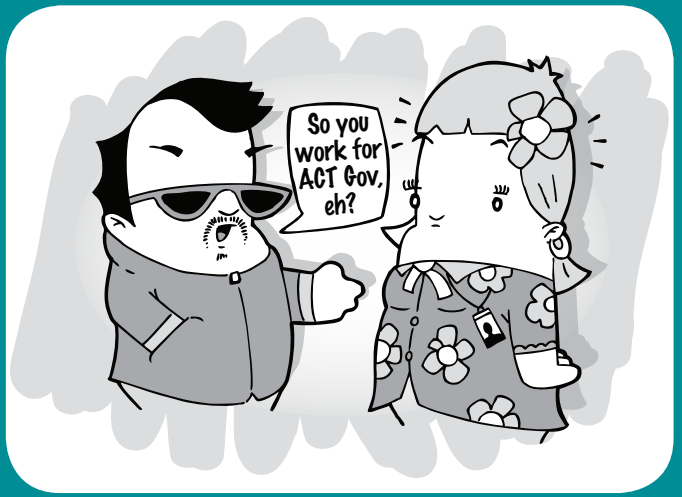
Phone: .....

Date: .....

The Completed Contact Report must be provided to your Agency Security Adviser.

ACT Government

ACT Government Contact Reporting and Awareness Scheme



ACT Government Awareness and Contact Reporting Scheme

The Justice and Community Safety Directorate, Security and Emergency Management Branch (JACS SEMB) manages the ACT Government Awareness and Contact Reporting Scheme. This scheme links to Commonwealth agencies. It assists in the identification of intelligence or hostile activity directed against Australia and its interests, government employees and contractors, and people who hold an Commonwealth security clearance. It assists to identify trends, including:

- What information is of interest to foreign intelligence services;
- Who is interested in it; and
- The methods the foreign intelligence services are prepared to use to collect the information.

Reporting Criteria

Contact Reports should be made when contact, either official or social, with embassy or foreign government officials within Australia, seems persistent, suspicious, or becomes ongoing. Foreign officials can include trade or business representatives.

ACT Government employees should also complete a contact report for instances when an individual or group, regardless of nationality, seeks to obtain official information they do not have a need to access.

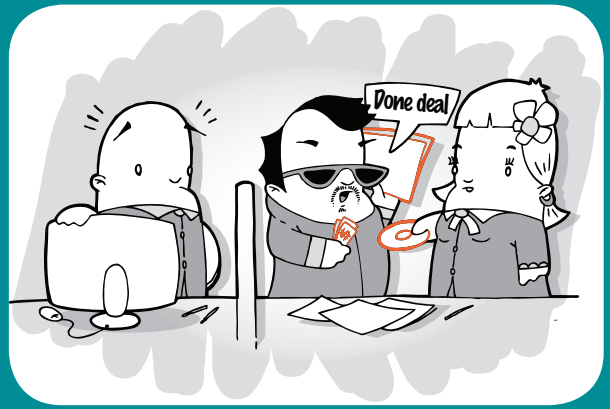
Types of Contact?

Relationships or contacts often happen when a persons job requires communication with foreign, commercial or issue motivated representatives. Contacts can also occur through other scenarios such as:

- Invitations to attend functions;
- Written correspondence;
- Hobby group meetings;
- Visits to embassies or Consulates; or
- E-mail or internet chat sites.

The initial overture might be subtle, but there could be indicators that arouse suspicion including:

- An inordinate interest in a persons official, social or personal activities;
- A fascination with some particular
- aspect of their work;
- Introducing another person who takes a similar interest;
- Encouragement to participate in questionable or illegal activity; or
- Offers of inappropriate hospitality or gifts.



Reporting Procedures

If you believe you have been contacted, the matter must be reported to your Agency Security Advisor or the Justice and Community Safety Directorate, Security and Emergency Management Branch as soon as possible after the contact has occurred by filling out the contact report overleaf.

How Will My Report Be Managed ?

Once the contact reporting form is completed your Agency Security Advisor, will forward the form to Security Emergency Management Branch, which has overall responsibility for the coordination of the ACT Government Contact Reporting and Awareness Scheme. The Security and Emergency Management Branch will then forward the information to the Commonwealth. This information will assist in the provision of a range of comprehensive threat assessments and security advice.