

From: s. 11C(1)(a)
To: s. 22(1)(a)(ii)
Cc: s. 22(1)(a)(ii); s. 22(1)(a)(ii) s. 22(1)(a)(ii) [Jacob McMahon \(DFAT\)](#); s. 22(1)(a)(ii)
Subject: RE: Potential meeting with UK DSMA Secretary, Brig Geoffrey Dodds, May 2022 [SEC=PROTECTED]
Date: Saturday, 26 March 2022 12:22:36 AM
Attachments: [image001.gif](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)

~~PROTECTED~~

Hi s. 22(1)(a)(ii)

Apologies for the delay, it's all be a bit wild here, but I feel (she says optimistically) like I'm finally catching up.

No worries, here is the more detailed read-out of Marc's meeting with Brigadier Dodds (it's a bit rough, but gets the main points across!):

• s. 47C(1)

DSMA and Committee structure

- The DSMA office is made up of Brigadier Dodds, a part-time PA and two deputies (each do one month on, one month off on alternate months). The Committee itself is made up of nominees from each of the relevant government agencies and major media outlets, and are overseen by the DSMA. The Committee reviews DSMA's performance every six months. Committee members are not required to be cleared, although government and secretariat members are all cleared to Australia's PV-equivalent.

Engagement with journos and media

- s. 33(a)(iii), s. 47C(1)
- s. 33(a)(iii), s. 47C(1)
- s. 33(a)(iii), s. 47C(1)

s. 33(a)(iii), s. 47C(1)

- s. 33(a)(iii), s. 47C(1)

- s. 33(a)(iii), s. 47C(1)

Recent initiatives

- s. 33(a)(iii), s. 47C(1)

- s. 33(a)(iii), s. 47C(1)

Next steps

- s. 47C(1)

Hope this helps!

Cheers,

s. 11C(1)(a)

s. 11C(1)(a)

A/g Counsellor

Department of Home Affairs

Australian High Commission, Australia House

Strand, London WC2B 4LA

Ph: s. 22(1)(a)(ii) | M: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) [@dfat.gov.au](mailto:s.22(1)(a)(ii)@dfat.gov.au)

Home



OFFICIAL: Sensitive

M18 – Meeting brief – United Kingdom Defence and Security Media Advisory Committee (DSMA)

Context and objectives

Purpose of the meeting
Seek overview of the UK's Defence and Security Media Advisory (DSMA) System
What we want
s. 47C(1)
What they want
N/A
Handling notes
<i>The Australian Government is currently in caretaker. No major commitments, agreements or policy matters can be settled that might bind any incoming government.</i>

Key messages

- You are meeting with the Secretary of the UK DSMA Committee, Brigadier Geoffrey Dodds. A short biography is at [Attachment A](#)

- s. 47C(1)

- s. 47C(1)

- s. 47C(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL: Sensitive

OFFICIAL: Sensitive

- S. 47F(1)
- S. 47C(1)

UK DSMA System

- The DSMA system consists of:
 - ‘DSMA-Notices’ which outline specific types of classified or sensitive information that media should seek advice on prior to publication,
 - a DSMA Committee to review and update the content of the DSMA Notices, and
 - a DSMA Secretary who oversees the system and acts as a single point of contact for Government and the media.
- Further information about the DSMA System and its components is at **Attachment B**.

S. 47C(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL: Sensitive

OFFICIAL: Sensitive

S. 47C(1)

Background

Past engagement with the DSMA Secretary

- Deputy Secretary Marc Ablong met with DSMA Secretary Brigadier Dodds while in London in December 2021.
- The introductory meeting focussed on the operation of the DSMA Committee, the role of the Secretary, the use of DSMA standing notices and how the Committee worked in partnership with media to provide advice on stories of defence and security importance.

Sensitivities

- S. 47C(1)

Point of contact

Press freedoms

s. 22(1)(a)(ii), Director Law Enforcement Powers, s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Attachment A – Biography Geoffrey Dodds



Brigadier Geoffrey Dodds commenced as Secretary of the United Kingdom's Defence and Security Media Advisory (DSMA) Committee in November 2016.

Prior to that, Brig Dodds spent 36 years in the British Army as a Sapper Officer serving operationally in command appointments in the Falkland Islands, Bosnia, Kosovo and Iraq. He has also served in United Nations Headquarters as a military planner, in various NATO posts and in military diplomatic appointments worldwide.

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Attachment B – Overview of the UK DSMA System

- The DSMA system is well-established and has been in place for more than 100 years.
- The purpose of the DSMA-notice system is to prevent inadvertent public disclosure of information that would compromise UK military and intelligence operations and methods, put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.
- The DSMA system consists of the following components:
 - 'DSMA-Notices' which are publicly available written descriptions of specific types of classified or sensitive information. The media is asked to seek advice from the DSMA Secretary on any stories which may contain information that falls into any of the five DSMA-Notice categories:
 - Military operations, plans and capabilities
 - Nuclear and non-nuclear weapon systems and equipment
 - Military counter-terrorist forces, special forces and intelligence agency operations, activities, communication methods and techniques
 - Physical property and assets
 - Personnel and their families who work in sensitive positions
 - A DSMA Committee which comprises senior representatives from Government and the media. The Committee meets every six months (or as needed) to review and update the content of the DSMA-Notices and explore any concerns or issues with the system.
 - When it is judged necessary to amend the DSMA-Notices, the appropriate Government department(s) forward a draft proposal to the media members for consideration and agreement.
 - A DSMA Secretary who oversees the system and acts as a single point of contact for Government and the media on DSMA policy issues. The Secretary gives advice on the system as well as individual cases.
 - The Secretary is supported by a part-time PA and two deputies who each work one month on, one month off, on alternate months.
 - The current DSMA Secretary, Brig Geoffrey Dodds, was appointed shortly after the Leveson Inquiry into the culture, practices and ethics of the press, which called out disreputable behaviour in the media. Consequently, the DSMA was seen as a positive force at that time.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL: Sensitive

From: s. 22(1)(a)(ii)
To: s. 22(1)(a)(ii); s. 22(1)(a)(ii)
Cc: s. 22(1)(a)(ii)
Subject: DSMA notes [SEC=OFFICIAL:Sensitive]
Date: Friday, 20 May 2022 2:10:35 PM
Attachments: [image001.jpg](#)

OFFICIAL: Sensitive

Hi s. 22(1)(a)(ii) and s. 22(1)(a)(ii),

Please see my (admittedly rough) notes from our meeting with the DSMA Secretary. Please feel free to give me a call if there is anything that you'd like clarified.

I hope they are somewhat helpful alongside our readout from the other day.

Cheers

s. 22(1)(a)(ii)

DSMA meeting notes (meeting with Brigadier Geoffrey Dodds OBE and Post)

S. 47C(1)

S. 47C(1)

s. 22(1)(a)(ii)

A/g Director | Cross-border Data Policy Section

National Security Policy Branch | Electronic Surveillance and Law Enforcement Policy Division

Department of Home Affairs

P: s. 22(1)(a)(ii) M: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) [@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)

s. 22(1)(a)(ii)

cid:image002.jpg@01D5EC92.FDA72E30



OFFICIAL: Sensitive

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

From: s. 22(1)(a)(ii)
To: [Susan MCKEAG](#)
Cc: s. 22(1)(a)(ii)
Subject: FW: Request for Report on Review of DSMA System [SEC=OFFICIAL:Sensitive]
Date: Thursday, 23 June 2022 8:46:06 AM
Attachments: [image001.gif](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.jpg](#)
[image006.jpg](#)
[Review of the Defence Advisory Notice System - TOR.pdf](#)
[20150312-DPBAC Review Report-Final-O.pdf](#)
[20150315-GOVERNMENT RESPONSE TO THE REVIEW OF THE DPBAC -O \(6\).pdf](#)

OFFICIAL: Sensitive

Hi Susan,

For visibility. We will go through and provide a summary for you and Andrew.

s. 22(1)(a)(ii)

OFFICIAL: Sensitive

From: s. 11C(1)(a) s. 22(1)(a)(ii) @dfat.gov.au>
Sent: Thursday, 23 June 2022 1:55 AM
To: s. 22(1)(a)(ii) @homeaffairs.gov.au>
Cc: s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>; s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>; s. 22(1)(a)(ii) @dfat.gov.au>; s. 22(1)(a)(ii) s. 22(1)(a)(ii) @dfat.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>
Subject: RE: Request for Report on Review of DSMA System [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 22(1)(a)(ii)

Many thanks again for your patience with me on this one.

As promised, I've reached out to Brigadier Dodds and he provided the attached documents. They are:

- A copy of the 2015 Independent Review of the then-DPBAC and its notice system
- A copy of the Review's ToRs
- Government response to the review (noting the Government did not accept all recommendations from the review)

Brigadier Dodds has kindly offered to take any questions you and the team may have on the report, so please don't hesitate to let us know if you would like us to follow-up!

As a side note, s. 22(1)(a)(ii) and I have been very kindly invited to attend a DSMA Committee Reception next week Wednesday evening. If there's anything in particular you would like us to follow-up or ask of Brigadier Dodds or of the Committee while we're there please don't hesitate to let us know.

Cheers,

s. 11C(1)(a)

s. 11C(1)(a)

First Secretary (National Security)

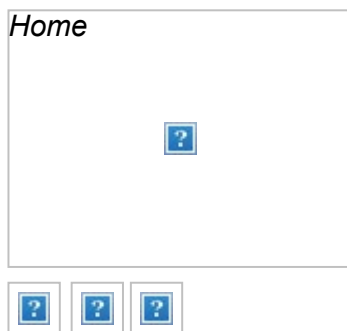
Department of Home Affairs

Australian High Commission, Australia House

Strand, London WC2B 4LA

Ph: s. 22(1)(a)(ii) | **M:** s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) [@dfat.gov.au](mailto:s.22(1)(a)(ii)@dfat.gov.au)



From: s. 11C(1)(a)

Sent: Friday, 17 June 2022 3:15 PM

To: s. 22(1)(a)(ii) [@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)>

Cc: s. 22(1)(a)(ii) [@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)>; s. 22(1)(a)(ii)

s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>; s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>

Subject: Re: Request for Report on Review of DSMA System[SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 22(1)(a)(ii)

My sincere apologies - between senior official visits and travel for work I've gotten very behind with my emails! I will action this first thing next week and hopefully have something useful for you :)

Cheers,

s. 11C(1)(a)

s. 11C(1)(a)

First Secretary (National Security)
Department of Home Affairs
Australian High Commission, Australia House
Strand, London WC2B 4LA

Ph: s. 22(1)(a)(ii) | M: s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) [@dfat.gov.au](mailto:s.22(1)(a)(ii)@dfat.gov.au)

OFFICIAL: Sensitive

From: s. 22(1)(a)(ii) [@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)>
Date: Friday, 17 June 2022 at 06:08:33
To: s. 11C(1)(a) s. 22(1)(a)(ii) [@dfat.gov.au](mailto:s.22(1)(a)(ii)@dfat.gov.au)>
Cc: s. 22(1)(a)(ii) [r@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)r@homeaffairs.gov.au)>, s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>, s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>
Subject: RE: Request for Report on Review of DSMA System [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 11C(1)(a)

I hope you're well. Thought I would follow up on the below to see if you had managed to obtain a copy of the report?

Many thanks!

Kind regards,
s. 22(1)(a)(ii)

s. 22(1)(a)(ii) Law Enforcement Powers Section | Electronic Surveillance and Law Enforcement Policy
Division | P: s. 22(1)(a)(ii)

OFFICIAL: Sensitive

From: s. 22(1)(a)(ii)
Sent: Thursday, 9 June 2022 5:12 PM
To: s. 11C(1)(a) s. 22(1)(a)(ii) [@dfat.gov.au](mailto:s.22(1)(a)(ii)@dfat.gov.au)>
Cc: s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>; s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>; s. 22(1)(a)(ii) [@HOMEAFFAIRS.GOV.AU](mailto:s.22(1)(a)(ii)@HOMEAFFAIRS.GOV.AU)>
Subject: Request for Report on Review of DSMA System [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 11C(1)(a)

Many thanks for your assistance in setting up the meeting between Andrew and Brigadier Dodds last month – it was a very fruitful discussion and has given us lots of food for thought.

When Andrew returned from his trip, he mentioned that there had been a 2015 review into the DSMA Notice System (I think it was then known as the 'DA-Notice System') which made recommendations for changes to the system. I think the review is also mentioned on the DSMA website. We were wondering whether we might be able to obtain a copy of the review/report if there is one – is this something you might be able to help with? I apologise if the report is publicly available, we did do a bit of Googling but couldn't find anything.

s. 47C(1)

In your opinion, is this something that would be possible to set up, or something you think the DSMA would be open to? Just putting the feelers out at this stage so no need to arrange anything yet! We will need to consult Commonwealth stakeholders first before we set up a meeting. Once we have done this we can get back in touch with you.

Many thanks in advance.

Kind regards,
s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Assistant Director
Law Enforcement Powers Section
Electronic Surveillance and Law Enforcement Policy Division
Strategy and Law Enforcement Group
Department of Home Affairs
Ph: s. 22(1)(a)(ii) s. 22(1)(a)(ii)@homeaffairs.gov.au

Acknowledgement of Country Signature Block Graphic 2022



OFFICIAL: Sensitive

From: s. 11C(1)(a), s. 22(1)(a)(ii)@dfat.gov.au>

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Sent: Thursday, 14 April 2022 12:47 AM

To: S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>; Electronic Surveillance Reforms

S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>

Cc: S. 22(1)(a)(ii) <[REDACTED]@HOMEAFFAIRS.GOV.AU>; S. 22(1)(a)(ii)

S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>; S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>

Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi S. 22(1)(a)(ii)

Hope all is going well on your end!

Just quickly jumping in to note that we confirmed today that Brigadier Dodds is available to meet with Andrew on the 10th of May

Cheers,

S. 22(1)(a)(ii)

S. 22(1)(a)(ii)

First Secretary (National Security)

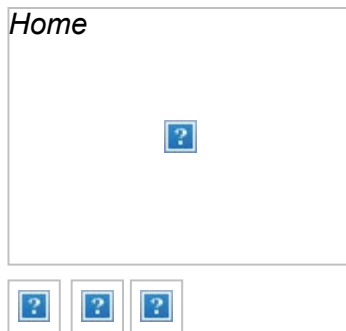
Department of Home Affairs

Australian High Commission, Australia House

Strand, London WC2B 4LA

Ph: S. 22(1)(a)(ii) | **M:** S. 22(1)(a)(ii)

E: S. 22(1)(a)(ii) <[REDACTED]@dfat.gov.au>



From S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>

Sent: Wednesday, 13 April 2022 5:32 AM

To: Electronic Surveillance Reforms S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>;

S. 22(1)(a)(ii) <[REDACTED]@dfat.gov.au>

Cc: S. 22(1)(a)(ii) <[REDACTED]@HOMEAFFAIRS.GOV.AU>; S. 22(1)(a)(ii)

S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>; S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>

Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Amazing – thanks so much both. Appreciate all your assistance with this.

s. 22(1)(a)(ii)

OFFICIAL: Sensitive

From: Electronic Surveillance Reforms

Sent: Wednesday, 13 April 2022 2:32 PM

To: s. 22(1)(a)(ii) <[redacted]@homeaffairs.gov.au>; Electronic Surveillance Reforms

s. 22(1)(a)(ii) <[redacted]@homeaffairs.gov.au>; s. 11C(1)(a) (DFAT)

s. 22(1)(a)(ii) <[redacted]@dfat.gov.au>

Cc: s. 22(1)(a)(ii) <[redacted]@HOMEAFFAIRS.GOV.AU>; s. 22(1)(a)(ii)

s. 22(1)(a)(ii) <[redacted]@homeaffairs.gov.au>; s. 22(1)(a)(ii) <[redacted]@homeaffairs.gov.au>

Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 22(1)(a)(ii)

Thanks for reaching out. s. 11C(1)(a) has been doing an amazing job of the organisation and it's my understanding that the UK DSMA is certainly in the works. Whilst a time hasn't been confirmed as of yet, in s. 22(1)(a)(ii) absence I will update you when we have further confirmation.

s. 11C(1)(a) – thanks for all your hard working in getting this locked in.

Let me know if you have any further questions.

Kind regards,

s. 22(1)(a)(ii)

Policy Officer | Governance & Engagement Section

Electronic Surveillance Reform Branch

Electronic Surveillance and Law Enforcement Policy Division

Department of Home Affairs

Tel: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) <[redacted]@homeaffairs.gov.au>

OFFICIAL: Sensitive

From: S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>
Sent: Wednesday, 13 April 2022 1:05 PM
To: Electronic Surveillance Reforms S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>;
S. 11C(1)(a) (DFAT) S. 22(1)(a)(ii) <[REDACTED]@dfat.gov.au>
Cc: S. 22(1)(a)(ii) <[REDACTED]@HOMEAFFAIRS.GOV.AU>; S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>;
S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>; S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>
Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK
Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi [REDACTED] and [REDACTED] (and team),

I just wanted to reach out and see how the meeting with the UK DSMA scheduling was tracking?

[REDACTED] is currently on leave, and I can't remember if it was Post or ESS reaching on to UK DSMA to schedule the meeting.

Thanks for all your assistance with this.

S. 22(1)(a)(ii)

S. 22(1)(a)(ii)

Director | Law Enforcement Powers

Law Enforcement Policy Branch | Electronic Surveillance and Law Enforcement Policy Division

Department of Home Affairs

P: S. 22(1)(a)(ii) | M: S. 22(1)(a)(ii) | E: [REDACTED]@homeaffairs.gov.au



OFFICIAL: Sensitive

From: Electronic Surveillance Reforms
Sent: Monday, 4 April 2022 10:20 AM
To: S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>
Cc: S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>; S. 22(1)(a)(ii) <[REDACTED]@HOMEAFFAIRS.GOV.AU>;
S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>
Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK

Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi [REDACTED]

No apologies needed, completely understand the situation.

Thank you for providing us with those briefs and for all your work in assisting with the development of the briefing pack.

Appreciate if you could please keep us updated (as you have been) on any developments on the UK DSMA meeting.

Kind regards,

s. 22(1)(a)(ii)

Policy Officer | Governance & Engagement Section

Electronic Surveillance Reform Branch

Electronic Surveillance and Law Enforcement Policy Division

Department of Home Affairs

Tel: [REDACTED]

E: [REDACTED] [@homeaffairs.gov.au](mailto:[REDACTED]@homeaffairs.gov.au)

OFFICIAL: Sensitive

From: [REDACTED] [@homeaffairs.gov.au](mailto:[REDACTED]@homeaffairs.gov.au)>

Sent: Monday, 4 April 2022 9:24 AM

To: Electronic Surveillance Reforms [REDACTED] [@homeaffairs.gov.au](mailto:[REDACTED]@homeaffairs.gov.au)>

Cc: [REDACTED] [@homeaffairs.gov.au](mailto:[REDACTED]@homeaffairs.gov.au)>; [REDACTED]

[REDACTED] [@HOMEAFFAIRS.GOV.AU](mailto:[REDACTED]@HOMEAFFAIRS.GOV.AU)>

Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK
Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi team

Apologies for missing the deadline on this, I unwell on Friday.

Please find [attached](#) Background Brief 9 – Press Freedom and Law Enforcement Reforms and Meeting Brief – UK DSMA Secretary. As far as I know, the meeting with the DSMA Secretary has not been locked in yet but I will follow up Post today to see how it is coming along and keep you

updated.

ESS has reviewed the content in the background brief that relates to them. There are also a couple of highlighted lines in both briefs which may change when/if the meeting with the DSMA Secretary goes ahead.

Please feel free to get in touch if you have any questions.

Kind regards,

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Assistant Director
Law Enforcement Powers Section
Electronic Surveillance and Law Enforcement Policy Division
Strategy and Law Enforcement Group
Department of Home Affairs
Ph: s. 22(1)(a)(ii) | s. 22(1)(a)(ii)@homeaffairs.gov.au

OFFICIAL: Sensitive

From: Electronic Surveillance Reforms s. 22(1)(a)(ii)@homeaffairs.gov.au>
Sent: Friday, 18 March 2022 9:12 AM
To: s. 22(1)(a)(ii)@homeaffairs.gov.au>
Cc: s. 22(1)(a)(ii)@homeaffairs.gov.au>
Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 22(1)(a)(ii)

Thanks heaps for reaching out and assisting with this whole process. I understand those briefs may need some tweaking as things become more clear. We too anticipate a few additions/tweaks after the due date.

Appreciate you keeping me updated on any developments with that meeting and if any changes need to be made.

Grateful for all your help with this.

Kind regards,

s. 22(1)(a)(ii)

Policy Officer | Governance & Engagement Section
Electronic Surveillance Reform Branch
Electronic Surveillance and Law Enforcement Policy Division

Department of Home Affairs

Tel: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) @homeaffairs.gov.au

OFFICIAL: Sensitive

From: s. 22(1)(a)(ii) @homeaffairs.gov.au>

Sent: Thursday, 17 March 2022 4:25 PM

To: Electronic Surveillance Reforms s. 22(1)(a)(ii) @homeaffairs.gov.au>

Cc: s. 22(1)(a)(ii) @homeaffairs.gov.au>

Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi s. 22(1)(a)(ii)

We've started drafting B9 – Law enforcement powers reform projects and Press Freedom and should not have trouble meeting your 1 April deadline.

As you know, we are trying to set up a meeting between Andrew and the UK DSMA while he is in London. I thought I would just flag with you that depending on when/if that meeting gets confirmed, our brief may require some tweaking after the 1 April due date (e.g. from a meeting brief to a background brief, or vice versa). However, I'll be in touch if that is required.

Thanks,

s. 22(1)(a)

s. 22(1)(a)(ii)

Assistant Director

Law Enforcement Powers Section

Electronic Surveillance and Law Enforcement Policy Division

Strategy and Law Enforcement Group

Department of Home Affairs

Ph: s. 22(1)(a)(ii) | s. 22(1)(a)(ii) @homeaffairs.gov.au

OFFICIAL: Sensitive

From: Electronic Surveillance Reforms s. 22(1)(a)(ii) @homeaffairs.gov.au>

Sent: Thursday, 17 March 2022 12:55 PM

To: Electronic Surveillance Reforms s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)

s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @ag.gov.au; s. 22(1)(a)(ii)

s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) s. 22(1)(a)(ii) @homeaffairs.gov.au>;
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>;
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>;
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>;
Cyber Crime Online Safety Policy s. 22(1)(a)(ii) @homeaffairs.gov.au>;
s. 22(1)(a)(ii) @homeaffairs.gov.au>
Cc: Cross-Border Data Policy s. 22(1)(a)(ii) @homeaffairs.gov.au>; Electronic
Surveillance Section s. 22(1)(a)(ii) @homeaffairs.gov.au>; CTCC Executive
Support s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>; Cybercrime Policy & Cooperation
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>; Digital Industry Policy
s. 22(1)(a)(ii) @homeaffairs.gov.au>; Online Terrorism Policy
s. 22(1)(a)(ii) @homeaffairs.gov.au>; ESLEPD Coordination
s. 22(1)(a)(ii) @homeaffairs.gov.au>; ESR Governance and Engagement
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>

Subject: RE: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK
Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Dear Colleagues,

Thank you for your continued engagement with the briefing pack for ESR's April travel to US, Canada and the UK.

We are making progress on our planning and are starting to lock-in meetings with our international stakeholders. We will provide updates if there are any changes in the itinerary or meetings.

There is still plenty of time until the tasking timeline of **Friday 1st April**. But to help us manage this sizeable briefing pack, we would be grateful if you can **provide an update on your progress**. Please reach out if you have any questions or require any additional clarity or assistance.

Please let me know early if you foresee any difficulties providing AS-cleared by Friday 1st April.

Looking forward to receiving your briefings in the coming weeks.

Kind regards,

s. 22(1)(a)(ii)

Policy Officer | Governance & Engagement Section

Electronic Surveillance Reform Branch

Electronic Surveillance and Law Enforcement Policy Division

Department of Home Affairs

Tel: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) @homeaffairs.gov.au

OFFICIAL: Sensitive

From: Electronic Surveillance Reforms s. 22(1)(a)(ii) @homeaffairs.gov.au>
Sent: Friday, 4 March 2022 2:52 PM
To: s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @ag.gov.au; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) s. 22(1)(a)(ii) @homeaffairs.gov.au>;
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii) @homeaffairs.gov.au>;
Cyber Crime Online Safety Policy s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>
Cc: Cross-Border Data Policy s. 22(1)(a)(ii) @homeaffairs.gov.au>; Electronic
Surveillance Section s. 22(1)(a)(ii) @homeaffairs.gov.au>; CTCC Executive
Support s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>; Cybercrime Policy & Cooperation
s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @homeaffairs.gov.au>; Digital Industry Policy
s. 22(1)(a)(ii) @homeaffairs.gov.au>; Online Terrorism Policy
s. 22(1)(a)(ii) @homeaffairs.gov.au>; ESLEPD Coordination
s. 22(1)(a)(ii) @homeaffairs.gov.au>; ESR Governance and Engagement
s. 22(1)(a)(ii) @homeaffairs.gov.au>; Electronic Surveillance Reforms
s. 22(1)(a)(ii) @homeaffairs.gov.au>
Subject: FOR ACTION BY COB 1 APR: Briefing For FAS Electronic Surveillance – US, Canada, UK
Travel [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Dear colleagues,

FAS Electronic Surveillance Division Andrew Warnes along with s. 22(1)(a)(ii) and s. 22(1)(a) s. 22(1)(a)(ii) are scheduled to travel to the US, Canada and the UK on the 26th April.

The travel gives FAS ESD the opportunity to consult with Government agencies and industry representatives on the implementation of the Australia-US CLOUD Act Agreement and on electronic surveillance reforms.

We would be grateful for your input into their **briefing pack**.

Please see the attached **Briefing Index** which includes an overview of each meeting and the input

required from your teams. We also welcome any additional input you may wish to provide. **Please let us know if you identify any additional briefs for inclusion.** Background and meeting briefs templates are also attached.

Grateful for your input by **COB Friday 1st April** to allow time to collate before the delegation departs.

Happy for line areas to decide on appropriate levels of clearance.

Some areas previously submitted input to the briefing pack for our (cancelled) February trip, and as such there may be extensive overlap in the briefs. Grateful if you could please review and resubmit those briefs.

Thank you very much in advance for your various input and expertise, and please feel free to get in contact with myself or **s. 22(1)(a)(ii)** [@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au) if there are any concerns.

Kind regards,

s. 22(1)(a)(ii)

Policy Officer | Governance & Engagement Section

Electronic Surveillance Reform Branch

Electronic Surveillance Division

Department of Home Affairs

Tel: **s. 22(1)(a)(ii)**

E: **s. 22(1)(a)(ii)** [@homeaffairs.gov.au](mailto:s.22(1)(a)(ii)@homeaffairs.gov.au)

OFFICIAL: Sensitive

Important Notice: The content of this email is intended only for use by the individual or entity to whom it is addressed. If you have received this email by mistake, please advise the sender and delete the message and attachments immediately. This email, including attachments, may contain confidential, sensitive, legally privileged and/or copyright information.

Any review, retransmission, dissemination or other use of this information by persons or entities other than the intended recipient is prohibited. The Department of Home Affairs and ABF respect your privacy and have obligations under the Privacy Act 1988.

Unsolicited commercial emails MUST NOT be sent to the originator of this email.



**THE DEFENCE ADVISORY NOTICE SYSTEM AND
THE DEFENCE PRESS AND BROADCASTING ADVISORY COMMITTEE

REPORT OF THE REVIEW**

March 2015

CONTENTS

	<u>Page</u>
Summary	3
Introduction	4
Background and history	4
Current working of the system	5
International comparisons	6
Views of stakeholders	7
The key issues	7
The need for the system	8
The UK government and media context	10
MOD's stewardship	12
Effectiveness and efficiency of the current system	13
The DA Notices	15
Structure and operations of the Committee	15
Structure and operations of the Secretariat	17
Financial responsibilities	18
Conclusions of the review	18
Recommendations	25
Annex A: Terms of Reference of the review	28
Annex B: Those consulted in the review	30
Annex C: DA-Notice requests for advice May 2011- May 2014	31

SUMMARY

For over 100 years the D-Notice, or DA-Notice, system has operated in a unique co-operation between the UK government and national media to avoid the inadvertent disclosure of information that might damage national security. We were asked to review the system's continuing fitness for purpose in an age of instant global digital communication and whether there were ways of making it more effective.

We found widespread support for this voluntary system which, at relatively modest cost, continues to work to avoid inadvertent disclosure, even if it cannot always succeed, especially with often offshore-based non-mainstream media. This is work that has value, both to government and media, as well as to individuals whose lives might be put at risk by the publication of sensitive information. The system is not intended to deal with deliberate disclosure; these are matters for other instruments, such as injunctions and the Official Secrets Acts, within the UK's jurisdiction.

There are weaknesses in the present system, notably a lack of direction within the Committee that oversees the system, patchy engagement by government departments (which has contributed to uncertainty within the media about the strength of the government commitment to the system), weak accountability and questions about which government department is best placed to operate the system. These need to be addressed.

The key changes that we recommend are the appointment of an independent chair, to be supported by a vice-chair representing government and a vice-chair representing the media, to form a top leadership group to oversee the secretariat, deal with business between committee meetings and to give a new sense of direction. Membership should be expanded to include elements of new digital media and intelligence and security agencies that are beneficiaries of the system. The committee and the notices it issues should be renamed to reflect better their purpose.

Introduction

1. This review was initiated to re-examine the purpose and effectiveness of the Defence, Press and Broadcasting Advisory Committee (DPBAC) and the associated Defence Advisory (DA) -Notice system, from the perspectives of the government, the media and the wider public, and in the contemporary context of 24/7 global media. It was sponsored by the Permanent Secretary of the Ministry of Defence (MOD). The full terms of reference of the review are at Annex A.

2. The review team began its work in June 2014: chaired by s. 47F(1) [REDACTED], team members were s. 47F(1) [REDACTED], and s. 47F(1) [REDACTED]. The team's task was to provide an independent view, without any preconceptions, on the issues set out in the remit.

3. The review invited views from all members of the DPBAC, government and the media, who were approached directly, and from interested parties more widely, through an announcement placed on the DPBAC website. A list of those consulted is at Annex B. The Minister for the Armed Forces wrote to the chairs of the three Parliamentary committees that were most relevant: the Defence Select Committee, the Home Affairs Select Committee and the Intelligence and Security Committee to inform them of the review.

Background and History

4. The DPBAC oversees a voluntary code which operates between the UK Government departments which have responsibilities for national security and the media. DPBAC uses the DA-Notice system as its key instrument of influence. The objective of the DA-Notice system is to prevent inadvertent disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such

operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives and is advisory in nature.

5. This approach, in one form or another, dates back to 1912, when it was decided that a system was needed to avoid the disclosure of information that might be of value to a potential enemy. From the outset it was a system jointly operated by government and media. During the war years, the system was replaced by censorship. In 1971 the existing plethora of D Notices were cancelled and replaced by 12 standing notices that were intended to have a degree of permanence and which it was hoped would provide editors and others in the media with clear guidance on those subjects which concerned national security and where it would be desirable to consult the secretary of the committee. In 1993 the committee took its present name and in 2000 the number of standing DA-Notices was reduced to five and these are:

- DA-Notice 01. Military operations, plans and capabilities
- DA-Notice 02. Nuclear and non-nuclear weapons and equipment
- DA-Notice 03. Ciphers and secure communications
- DA-Notice 04. Sensitive installations and home addresses
- DA-Notice 05. UK security and intelligence services and special forces.

Current working of the system

6. The current membership and terms of reference of the DPBAC are at <http://www.dnotice.org.uk/>. The DPBAC is supported by a small Secretariat of four staff (three advisers and one administrative assistant) based in the MOD. The Secretariat issues advisory notices, maintains contacts with the media and briefs interested audiences on how the system works. The Secretariat responds to media requests for advice on the application of DA-Notices, but will also approach journalists if it learns of a possible story that might be covered by the content of any of the DA-Notices. These discussions are carried out in confidence. DPBAC and the DA-Notice system do not concern themselves with information that may cause political and official embarrassment; the system is there purely to identify and advise upon material that might cause a risk to life or to national security. This is explained

on the DPBAC web site <http://www.dnotice.org.uk/faqs.htm#system>.

7. Ignoring a DA-Notice carries with it no legal consequences per se, but the review team were informed that it was a very important reference point for editors in reaching decisions about what to publish. In serious cases, the government department concerned can seek a court injunction to stop something being published. Where secret material has been unlawfully disclosed or published there is the ultimate sanction of a criminal prosecution under the Official Secrets Acts, though such prosecutions in recent years have been very rare (and directed against the discloser rather than the media).

International comparisons

8. In 2010 the DPBAC Secretariat carried out a survey of 15 countries to see whether they had any comparable arrangements or might offer examples of how the system might be improved¹. From this survey it was apparent that no country had any comparable system to provide guidance to the media to prevent inadvertent disclosure of information that might put at risk the safety of those involved in military or intelligence operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives. Other countries relied on legal sanctions to protect national security information and would use the criminal law to prosecute those who have leaked information, rather than the journalists or media who published the information. There are usually no mechanisms for discouraging the media from publishing sensitive information, apart from this ultimate threat of prosecution, which appears rarely to be used. The review team inquired through FCO channels whether there had been any significant changes since the survey in 2010 and were told that there were not, with the exception of Australia.

9. Australia has no formal system for notices of the DA-type. However, the Australian government has recently asked media organisations to give notice ahead of publication so that government has the opportunity to give a view on whether publication would result in a major threat to national security or a threat to life. The process has not so far been tested. Recent changes to

¹ D/DPBAC/3/6 dated 15 Oct 2010

Australian national security laws provide for jail sentences of up to ten years for anyone, including journalists, disclosing details of 'special intelligence operations'.

10. We concur with the conclusions of the 2010 review that national culture plays an important part in the way that all countries view mechanisms to regulate media discussion of national security issues. In the USA, for example, freedom of speech is enshrined in the constitution through the First Amendment, and contacts between the media and official sources far exceed in depth and breadth those that exist in the UK. Such contacts are routinely used to confirm the facts of a story but may also be used by government agencies to discourage publication, with varying results. In the Snowden case (the release of sensitive information by a former CIA contractor), The Guardian reported having fruitful discussions with senior subject matter experts in the Department of Justice (DoJ) and the National Security Agency (NSA), and agreed to redact portions of their material as a result. However, in one respect, the US system imposes a more restrictive regime than in the UK: the Espionage Act - which criminalises the gathering, receipt, and dissemination of national defence-related information. We did not seek further evidence from the DoJ or NSA.

Views of stakeholders

11. We encouraged all those with an interest to submit their views to the review, either in writing or in person and many responses were received. Most were from those government departments or agencies and media organisations that were members of the Committee or represented on it. We also received a paper on the system by s. 47F(1).

The Key Issues

12. The key issues that emerged from our review were:

- a. whether there was a continuing need for such a system, taking into account changes in the way news was delivered and accessed, and what purpose the system was intended to serve;

- b. how the system operated within the UK government's broader approach to media relations;
- c. whether the MOD was still the right departmental home for this system;
- d. how effective and efficient the current system was in achieving its stated objectives;
- e. whether the current ambit and definition of the DA-Notices continued to be relevant;
- f. whether the current structure and operations of the Committee were best suited to realising its objectives;
- g. how the Secretariat was staffed and how it operated;
- h. whether accountabilities were correctly defined and located;
- i. whether financial responsibilities were correctly assigned.

The Need for the System

13. Challenge to the existence of the system comes from a variety of sources: the impact of new digital media - unregulated, often offshore, fluid and easily accessed - as first shown in 2010 by the Wikileaks release, orchestrated by Julian Assange, of Iraq and Afghan war intelligence; and then, three years later by the Edward Snowden case. The Snowden leaks of American intelligence strategies and practices, in particular, seemed to demonstrate the difficulty of exercising any kind of restraint through the DA-Notice system: Snowden had passed on a great deal of sensitive material to news outlets in London, Washington and Hamburg. All operated in different legal and regulatory environments, but the internet has in effect created a single global public domain.

14. The ease with which new media outlets can be established, and accessed by the public, presents an obvious challenge to the more traditional print and broadcast media. They have often responded by creating a powerful digital presence themselves, but it remains the case that the public now have many more options for obtaining information - of variable quality and trustworthiness.

15. The Snowden case presented these challenges in stark relief. Some of the material gathered by The Guardian (via its New York office) related to GCHQ and was thus of interest to the UK media. Before publication, The Guardian sought information from the US Administration both about the accuracy of the material and its potential damage to national security, and was able to agree a number of changes - including the names of individuals

at risk - to what would otherwise have been published. The Washington Post adopted the same approach. The US administration and its agencies did not welcome the revelations, but they felt constitutionally obliged to co-operate, just as the print media felt morally obliged to avoid putting lives at risk. In the UK, however, The Guardian felt inhibited from approaching government sources, initially because of a fear that government would seek an injunction against publication in its entirety - even though the same stories, duly reviewed in Washington, could and would be published in the US and available in the UK. After The Guardian published its initial tranche of material in the UK, some engagement with government developed, both with the DPBAC Secretariat and with GCHQ.

16. Views varied about the implications of these developments, although a number of common themes emerged. There was general recognition that the proliferation of smaller websites around the world was a problem to which there was no obvious answer. On the one hand, its flow was difficult to control or even to influence; on the other hand, major print and broadcast news outlets enjoyed greater degrees of trust and visibility. The view from media representatives was overwhelmingly in favour of continuing a voluntary system aimed at avoiding inadvertent disclosure of sensitive information. From some government officials such support was more qualified, either because the system could not prevent deliberate disclosure of security-sensitive information, or because the system had a limited reach beyond the mainstream UK-based media. Nonetheless, officials still concluded that the system overall had merit and was worth maintaining, especially if the UK mainstream media continued to value it. There was broad agreement from all sides that no system would be 100% effective in avoiding accidental disclosures, especially with the range of media that existed globally. However, there was a widespread and strongly held view that the system should not be abandoned because it could not be completely effective. What it could achieve - for example, in terms of not putting lives in jeopardy - was still of clear value, especially as its most effective area of coverage was the mainstream media, which was the area of the media most trusted by the public. It was a system accessible to all, and arguably one that was of particular value to local and regional media and book publishers without the depth of government contacts enjoyed by much of the national media.

17. It was clear that one question which frequently divided the official and media sides was whether or not information could be regarded as being in the public domain. The Committee agreed its definition of information widely in the public domain in 2009, providing the Secretariat with criteria written

around where and how the information has been published, and how authoritative and accessible it is. It was suggested that unless material had been published by a newspaper or broadcaster known to be a reliable news provider with access to official sources, it would not be regarded with much credibility by potential enemies, and could therefore be ignored. Official witnesses largely endorsed this, with one saying information published on an obscure website might be read and believed by one terrorist cell in a hundred - if it was published in a national newspaper they would all see it and believe it. The media side tended to take the view that once a piece of information was known - particularly if it was published by mainstream American digital media, which is widely read here - search engines and Google alerts would mean it would rapidly be available to anyone who had an interest in it.

18. It was also accepted that a system that sought to go further and legally lay down what could or could not be published would be a very different system; one more akin to the system of censorship that had replaced the D-Notice system during the two World Wars. This was not explored further.

The UK government and media context

19. In comparing the ways in which different countries managed these issues, it was readily apparent that national context and culture were the key determinants. In the US the lack of prior restraint (injunctions against publication) and the constitutional safeguards for freedom of expression have led to expectations on the part of media and government that journalists would enjoy relatively free access to government officials. The UK context is very different. In general access by the media to government sources of information is more tightly controlled and there is an expectation that contacts will usually be through government press officers, rather than direct between journalists and departmental subject matter experts. It is important to recognise that for a limited number of trusted journalists and media organisations, direct access to highly-placed contacts in government is well established, but this is the exception rather than the rule.

20. Over the last 30 years the intelligence and security agencies in the UK have moved from an almost total absence of public profile and limited

contact with the media, to a position today where their existence is avowed, they recruit through a public process and their heads are named and appear publicly. They have also provided briefing sessions for parliamentarians and have a range of contacts with the media. There are, though, still significant differences between the UK departments and agencies concerned in their relations with the media.

- a. The MOD has a large press office with extensive media contacts, but is very restrained in what it will say about Special Forces (SF). Special Forces are probably the least willing of all the agencies to engage with the media (in spite of a certain amount of leaking and self-publicity by ex-SF members) and tend to stick to the formula of 'neither confirm nor deny' any information related to SF. This can make it quite difficult for the media to judge the veracity of some of the stories that are put to them or to weigh the security implications.
- b. MI5 has three officers, who are authorised to speak to representatives of the mainstream media, which in practice means a number of journalists at national newspapers and broadcasters.
- c. MI6 employ two government press officers on the same basis.
- d. GCHQ has operated a press office, which supports its media communications strategy generally, for a number of years; after Snowden, the agency appointed a senior serving officer to oversee the agency's response to the media leaks.

All the agencies have direct contacts with the media, to a greater or lesser extent, but they also use the DPBAC and its Secretariat to field enquiries about intelligence and security matters on their behalf and to act as an intermediary between themselves and the media where they have not established their own relationships of trust. They also use the DPBAC on those occasions when general advice needs to be circulated to the media

21. We noted both these very different approaches between UK departments and agencies to media contacts –and that all of them are very different from the approach taken in the USA. The US agencies carry out more 'on the record' unclassified background briefings and it was clear to the review team that for a variety of reasons UK agencies have chosen not to operate in the same way as their US counterparts, and that this was unlikely to change significantly in the immediate future. Although we were told that there was no fundamental difference between the UK and US in access to and release of classified information, the differences in the depth and breadth of media contacts between the two allies is always likely to present

issues around disclosure that a voluntary system in the UK cannot prevent.

22. It is a matter of observation, too, that relations between the British press, the government and the political parties have seldom been so fragile. We do not comment on the events leading up to the Leveson inquiry, but it is necessary to note that the press has overwhelmingly shunned the Government's attempts to impose Lord Justice Leveson's recommendations through the device of a Royal Charter (drawn up, it should be noted, in the Cabinet Office) on the grounds that a Charter which can only be changed by Parliament opens the way for political interference in the regulation of journalism. There has been immense opposition to any attempt to impose statutory regulation, which may in part explain the media side's enthusiasm to make the voluntary DA-Notice system work - and their concern that the perceived lack of engagement on the official side may be a precursor to an attempt to impose a system enforced by legal sanctions.

The MOD's stewardship of the DPBAC and the DA-Notice system

23. The Committee and the system it manages have been run from the Ministry of Defence ever since 1912, when the Admiralty and War Office decided they needed a system to avoid disclosing information that might be of value to an enemy. Although many of the enquiries received by the Secretariat still relate to military matters, especially the activities of Special Forces, a large proportion of the inquiries relate to the activities of the three intelligence and security agencies. However there is no consistent trend; all depends on what topics are of media interest at the time. Of 624 enquiries received by the Secretariat in the three years to May 2014, 281 related to the intelligence and security agencies. We have heard that the Secretariat is adept at fielding such inquiries, having established good contacts with the agencies concerned and the media side appear not to have experienced any difficulties in their dealings with the Secretariat in such areas. There is a widespread awareness that a more logical home for the DPBAC and DA-Notice system could be the Cabinet Office, since the National Security Council, as part of the Cabinet Office, operates as the cross-government home for national security. However there are very mixed views about whether, at this point in time at least, it would be desirable to move the system. Strained relations between government and media, post-Leveson, the perception of poor senior level engagement by government in the

Committee, weaknesses in the Committee structure, uncertain accountability within the system, all contribute to a feeling of unease that a transfer of stewardship now could lead to system breakdown.

24. We were challenged to answer the question whether the system would in practice work any better in the Cabinet Office than it does in the MOD and in particular whether it would command the same confidence that media representatives currently have in the present system. A particular issue was whether the system would retain its independence in a location that was perceived as more overtly political and under the sway of the government media management machine. We were told that there were plans for some other organisations relating to national security to be lodged in MOD and one option would therefore be to base the system still within MOD even if responsibility were transferred to the National Security Council.

25. Although the system could be placed under the National Security Council (whether or not it was physically located in MOD), and no doubt appropriate assurances could be given that its independence would be retained, the review team were told that this would not completely assuage suspicions. It was also questioned whether a transfer of responsibility to the Cabinet Office would mean that it would be less likely that retired military officers would be recruited to staff the Secretariat. While it was accepted that other public servants could fulfil the role, it was argued that retired military officers, with no career to advance and a culture of loyalty to the Crown rather than to the government of the day are more readily perceived as independent.

Effectiveness and efficiency of the current system

Effectiveness

26. We heard from all sides that effectiveness depends on the degree of trust that both sides have in the system: that it must be genuinely independent, focused solely on an objective view of national security and what causes damage, and at the same time discreet and accessible. We found that there was a high degree of trust in the Secretariat; nobody doubted that the advice they received was well-founded and as objective as possible. The evidence we received was that the media were confident that the advice was simply focused on risk to national security and never biased by any wish to avoid reputational damage. The Secretariat was not a departmental or agency press office. Advice was always available when

they needed it, which was crucial to media operating 24 hours a day.

27. The review team's impression was that there was very good engagement with media organisations signed-up to the system and it appeared to work well – not least because responsible media organisations took the issue of inadvertent disclosure that risked life and/or national security very seriously. To be effective an equal commitment from government departments to the operation of the system was necessary and we were made aware of some instances where ignorance of the system had led to behaviour that was not as consistent day to day as it should be.

28. Beyond that, the views we heard on effectiveness were largely shaped by differing perceptions of what the system was intended to achieve. A few felt that it should be re-directed at preventing the deliberate disclosure of security-sensitive information, and against that yardstick viewed it as ineffective. A clear majority believed its key role was preventing inadvertent disclosure. Against that more modest yardstick, most judged that the system was very effective most of the time. We were given examples of where the system had failed; most involved human error in the media, either mainstream or fringe. The general view was that occasional failures did not mean that the system as a whole was failing.

Efficiency

29. We were told that the system costs around £0.25M a year to run, mostly the staff and associated costs of the Secretariat. The costs are borne by the MOD and form part of the MOD's Top Office Group budget. However, they are not separately identified and reported to the Secretariat or to the Committee.

30. The primary outputs are the advice that is given to the media and the use they make of it. In the three years from May 2011 to May 2014 there were 624 requests for advice. Details are given at Annex C. The Secretariat reports these contacts in six monthly reports to the Committee, together with other activity over the reporting period, such as briefings and talks to journalists and academics. These are all reports of activity rather than outcomes.

The DA-Notices

31. The review explored with stakeholders whether the ambit of the current DA-Notices and the way they were written was still appropriate for the times. We found a general recognition that a case could be made for expanding the ambit of the Notices; that case would be that national security now embraces not only the traditional areas such as military secrets and intelligence activities, but could also extend to the impact of organised crime, the operations of the banking system and safeguarding national infrastructure such as the power system and telecommunications. However, all those whom we consulted agreed that it would be very undesirable to extend the DA-Notice system in such a way. Some of these areas might already be covered in relation to national security (e.g. communications interception methods that might be used equally against organised crime as against terrorists). But there was also a strong feeling that any expansion of DA-Notices beyond their current narrowly-focused range would cause suspicion, a loss of trust, and a sense of mission creep - and that it would require much greater resources to support an expanded remit. There was nevertheless acknowledgment that the time is ripe for a general review of the current DA-Notices to reflect the experience of operating them over the last decade and a half, paying attention, for example, to inadvertent disclosure of tactics, techniques and procedures (TTPs) and sensitive information in relation to people/families with security and counter-terrorist duties. Such a review would create a context in which to communicate better and more widely the nature of the system and role of the DPBAC.

Structure and operations of the Committee

32. The Committee is chaired by the Permanent Secretary at the MOD and the Vice-Chairman is selected from the media who have signed-up to the system. There are four other members representing the government: the Permanent Secretary of the Home Office, the Director for National Security, FCO, the Deputy National Security Adviser, Cabinet Office and the Director General Security Policy, MOD. There are 15 members representing the media nominated by the Newspaper Publishers' Association, the Professional Publishers Association, the Press Association, the Newspaper Society, the Book Publishers Association, the Society of Editors, the Scottish Newspaper Society, the BBC, Sky News, ITV and ITN.

33. We heard mixed views on the effectiveness of the Committee. The media representatives found that its informal pre-meetings, attended by the media and the Secretariat, were more useful than the later full Committee sessions which included government representatives. These full meetings seemed too rigidly stylised, basically the reporting by the Secretariat of issues received and addressed. These views, significantly, were shared by the representatives of the government, who felt that they were too routine and that there was too little substantive business to debate— though it must be said this was not true of the meeting attended by two members of the review team, which was brisk and business-like, despite the absence of any representative from the MOD or the Home Office. This perception may well account for the tendency among government representatives for principals to send deputies or more junior representatives to the meetings rather than attending themselves. Chairmanship seems to depend on who is available on the day. This has led to a strongly held view among the media that the official side's commitment to the Committee and the DA-Notice system has waned. The point was made to us forcefully that a voluntary system depends not only on trust but also engagement and this cannot be achieved without regular high-level participation and commitment, which is currently not always evident.

34. The review team received considerable evidence that the relationship between the Committee and the Secretariat was strong and the Secretary regularly briefs the Chairman and Vice-Chairman on issues and developments. However, accountability was not clearly defined. The Committee has no formal responsibility for the appointment, activities and performance of the Secretary and his staff. Appointments are made by the MOD as part of its normal appointments process, although the Vice-Chairman of the Committee, representing media representatives, is a member of the selection panel for the appointment of the Secretary. There is a clear view that accountability must be strengthened and defined more formally, with the Committee setting objectives and more systematically assessing performance. Any system of this complexity needs to be shown to be working.

35. We also heard a case for expanding the membership. The three intelligence and security agencies and MOD Special Forces are not members of the Committee, though they are represented indirectly by their sponsoring departments. It was argued that, since one of the keys to success in this business was better understanding, there would be considerable advantage in these agencies being part of the Committee structure in some way, either permanently or occasionally.

36. It was also suggested that efforts should be made to include representatives of new digital media on the Committee, though it was readily acknowledged that this was far from easy to achieve. This area of the media is often not UK-based, it is highly fluid, has no representative structures and is in general less willing to subscribe to any form of voluntary code. Following initial engagement in 2008, Google withdrew from the Committee in 2013 after the Snowden disclosures. Current Committee membership does not include any purely digital media organisations (though most of the mainstream media organizations have a digital presence). Expansion of the Committee might of course tend to militate against effectiveness and efficiency; a suggestion was made that it might be divided into sub-groups - perhaps with a smaller, digital sub-group meeting at more frequent intervals in order to keep better pace with technological change.

Structure and operations of the Secretariat

37. There has been a recent review of the functions, organization and staffing of the Secretariat². This led to the employment of a third DA-Notice adviser, bringing the strength of the Secretariat to four: the Secretary, two deputy secretaries and a part-time personal secretary. All posts are permanent. The Secretary is full-time, London based but able to work on a flexible basis. The two deputy secretaries are part-time; one is also London-based but the other is home-based and receives travel and subsistence allowances when working in London. The London-based advisers receive on-call allowance; the home-based adviser does not. The lack of consistency of treatment with regard to terms and conditions of employment and out of office/home based working was raised as an issue undermining efficiency and effectiveness. Arrangements for performance reporting are also not optimum: they are carried out by the MOD Permanent Secretary, although he does not have close and regular contact with the Secretariat.

38. The job specifications for these roles do not require a military background. However, retired senior military officers, who currently fill all three Secretary/Deputy Secretary roles, tend to have the knowledge of security issues, ability to react quickly, understanding of the media, communications strengths and manifest independence of mind that the job demands. The possibility of broadening the background and skill-sets of the

²D/DPBAC/5/2/1/4 dated 14 Dec 2011

advisers was discussed with respondents. Although this was agreed as desirable, the intelligence and security agencies noted the difficulty of offering their own staff (or encouraging their former staff to apply) for a role within the Secretariat, setting the need for transparency within the Secretariat against the paramount need of their staff and former staff for lifetime anonymity. This is an obstacle to applicants from the intelligence and security agencies applying for posts in the Secretariat. As to direct engagement in DPBAC, we understand the intelligence and security agencies would be happy to consider offering their staff for such a role provided concerns about anonymity could be met.

Financial responsibilities

39. The system is funded solely by the MOD as a function of custom and practice. In the days when national security mainly concerned military secrets' that may have been appropriate, but it is questionable whether this is still the case today. Benefits are obtained both by the media, who seek to avoid making mistakes that might jeopardise lives or national security and inflict reputational damage on themselves, and by government, which has a clear interest in preserving national security and safeguarding lives. Although the cost of the system is relatively modest, leaving all the cost to be borne by one party, not itself always the main beneficiary, does not properly reflect its value and is likely to weaken support from the sole funder. If costs were apportioned between beneficiaries it would also encourage their engagement and allow for a more informed view to be taken of costs and benefits.

Conclusions of the Review

40. We reached the following conclusions.

The need for the system

41. If the system were to be dissolved the media would be left without a robust system to avoid inadvertent disclosure, with all the potential for them to reveal information that could be both harmful to national or personal security, as well as to their own reputation. Undoubtedly a relatively small

well-established and well-connected group of journalists and media organisations would continue to obtain guidance directly from government departments. However, most parts of the media, including local and regional newspapers and broadcasters and book publishers, would not. Government departments and agencies would get more direct approaches; this would be problematic for some, especially the intelligence and security agencies, which would certainly need to invest considerably more resources than at present and develop a stronger capability to handle the media. Some journalists would simply write up a story without trying to check the security implications. But in any event the media would lose access to an independent and trusted source of advice on national security matters and any advice received direct from departments and agencies themselves might be undermined by a perception that it might be driven by concerns about reputational damage rather than any impact on national security. The system is modest in cost to operate and although we cannot quantify the number of occasions when it has mitigated inadvertent risk to national security or to life, we have heard numerous examples of this happening. When the system has not worked this has often been because of a lack of understanding; some journalists or editors, and some officials, being unaware of this resource or how to approach it.

We conclude that the system should be maintained but there is a compelling case for changes to further strengthen its operation including more active promotion of its functions to the media and government departments.

42. We considered whether the purpose of the system should continue to be to prevent accidental disclosure of information that might imperil life or national security; or whether it should attempt to go further, to prevent deliberate disclosure of such information or to impose sanctions on those who ignore its advice. No voluntary system can prevent deliberate disclosure and protection of official information in this way is a matter for legal instruments such as injunctions or the Official Secrets Acts - with all the problems this approach raises in a digital age of cross-border publication.

We conclude that the purpose of the system should remain that of preventing inadvertent disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives. Any extension to the remit would not command support of the media and would involve powers antithetical to a voluntary system of self regulation.

The Committee

43. We believe that the Committee needs to change if it is to serve its stated purpose. A first step might be to change its title to reflect better the nature of its business. We would suggest something on the lines of 'National Security Media Advisory Committee'; admittedly somewhat cumbersome though no more so than its present title.

44. The Committee currently lacks consistent direction, apparently a reflection of time pressures on those able to act as chairman. Different officials take the chair, from one meeting to another, sometimes at short notice. This can lead to a lack of forward thinking and additional responsibility devolving to the Secretariat. Consequently, meetings can fall into a pattern of routine reports with too little substantive business to transact. The review team were surprised to learn that major security issues, such as the ramifications of the Snowden case, have not been thought sufficiently pressing either to necessitate an extra meeting of the full Committee when they were unrolling, or to merit discussion at a regular meeting many months later (though we understand that they were discussed by the media side of the Committee). To provide this leadership we believe that the structure of the Committee should be reviewed. Whether or not the system continues to be stewarded by the MOD we believe that its wider national security remit needs to be acknowledged and a chair should be appointed who can both reflect this wider remit and devote sufficient time to managing the Committee actively.

45. We believe that the chair should be neither a representative of government nor of the media - the system is described as 'independent' and the chair should be independent of both. Its utility and success depend, crucially, on trust and confidence between the media and government: that the advice that is given to the media concerning the effect on national security or the safety of individuals is objective and not coloured by any desire to avoid reputational damage or to project a favourable image. That trust and confidence currently is strong, so far as the Secretariat is concerned. But, under the present structure, it will remain only as long as the Secretariat continues to be independent-minded and the official side and its chairman, to whom the Secretariat reports, continue to respect that independence. We

believe that the longevity and success of the system would be bolstered by having a chair who is as independent as the Secretariat and better placed to protect that independence than any official side chair could be. It would also be presentationally better, so far as the wider public are concerned (and even in explaining its role to some within government). An independent chair would be well placed to take the long view and develop a strategic approach, which we believe is lacking at present.

46. How this chair should be selected and employed needs examination (though it will probably involve an advertised opening and then agreement between the two sides of the Committee, using the public appointments process) but we believe it should be a person of independent outlook, with a deep experience of national security issues and of working at high level. A recently retired head of one of the agencies would be a possibility. There should also be two vice-chairs: one from the media, as at present, and one from the government (possibly on the nomination of the Cabinet Secretary). We would envisage the chair and the two vice-chairs as the leadership team of the Committee, dealing with issues in between the scheduled meetings of the Committee and more closely overseeing the work of the Secretariat on behalf of the Committee as a whole.

We conclude that a restructuring of the leadership of DPBAC along these lines is essential if the system is to serve its stated purpose.

47. The review team considers that the membership of the Committee should be widened to include some elements of new digital media. We recognise that attempts have been made in the past to do just that, but that identifying suitable media organisations that might be prepared to join and to remain in the Committee poses a challenge. We would encourage the Committee to persist in its efforts. There should also be representation from the intelligence and security agencies, who are significant beneficiaries of the system. This need not be for every meeting but there should be an active communications channel between the agencies and members of the Committee. We are conscious that expanding the membership of the Committee in the ways we propose could present their own problems; to reiterate, one possible solution might be to divide the Committee into sub-groups for specific areas.

We conclude that there is clear advantage in widening the membership to include representation from the intelligence and security agencies and some elements of the new digital media.

Departmental stewardship

48. We approached the question of which department should have stewardship of the system by considering where it might work best. One possibility would be to turn the Committee into an advisory non-departmental public body (NDPB). This would have the advantage of putting it more publicly at arm's length from Ministers and creating more transparency and accountability. Against that, it would not necessarily make the system work better, there would be a certain bureaucratic cost and we were aware that there may be limited enthusiasm for creating a new NDPB.

49. We agreed with the view from many stakeholders that a more logical home for the DPBAC and DA-Notice system may be under the National Security Council in the Cabinet Office, as the cross-government home for national security. However there are very mixed views about whether at this point in time it would be desirable to move the system's base. The key question is whether a move to the Cabinet Office would improve the effectiveness and efficiency of the system and in particular sustain and enhance the confidence in it from the media that the system enjoys under the stewardship of the MOD. The review team could see no grounds on which we could argue that trust in the system would be improved by a move to the Cabinet Office, and there is a clear current risk that it might be damaged because of a reduced level of trust on the part of the media.

50. We acknowledge an argument that if significant changes are to be made to the system it may be best if these were implemented in one step. However, we believe that the current fragile confidence in the system and lack of direction militate against a move at this time. Moreover, we consider that the issue of departmental stewardship is secondary to the issue of restoring trust and confidence and to creating a fully accountable and effective system for a government-media security dialogue. The implications of a possible move to the Cabinet Office, and the timing of such a move, should be explored within the Committee.

We therefore conclude that whilst trust and confidence is fragile, and an overhaul of the Committee and its structures is the priority, a move of departmental home would be a step too far at this time. The implications and timing of such a move should be explored within the Committee so that the issue can be addressed after other changes recommended in this review

have been implemented and shown their worth.

Effectiveness and efficiency

51. We considered how effective and efficient the system was in achieving its stated purpose. We heard anecdotal evidence indicating successes, and one or two failures. But there are no statistics prepared that show the number of occasions when the advice sought was followed, or not followed. The information on activity is helpful up to a point but does not fully answer questions about effectiveness and efficiency. It could be expected that significant failures on the part of the media to seek or follow the advice offered would be highlighted in the six-monthly reports to the Committee, and we were aware of instances of this. The fact that there are relatively few of these is reassuring, but is not a complete substitute for some quantification. A constraint may be the confidential nature of discussions between the Secretariat and individual journalists and editors, which makes it difficult to reveal details to the Committee. The constraint is a real one, but even a summary showing a schedule of advice accepted or ignored, together with a statement of costs incurred in operating this service, may be of value to the Committee as a measure of performance, even though the Committee may not be able to probe the implications very far. As part of this the performance reporting arrangements for the Secretariat need to be addressed.

We conclude that the MOD should separately identify and report the costs associated with the system, through the Secretariat to the Committee so that value for money can be assessed and that the Secretariat should provide further information on outputs in reports to the Committee. We also conclude that performance reporting on the Secretary and his deputies should be carried out by the vice-chair representing the government side, as first reporting officer, and by the chair, consulting the media side vice-chair, as second reporting officer.

52. We heard generous praise of the Secretariat and the way it operates. Some described it as the linchpin of the system and it was clear that there was a high degree of confidence in its service. However, noting the different terms and conditions of the three advisers, we believe that these should be aligned; all three advisers should be London based and entitled to on-call allowances. When a vacancy occurs, job descriptions should be reviewed to ensure the right balance between personal qualities such as communications

skills, independence of mind, and knowledge of the modern media; the Committee should also be consulted. A balance of skills and strengths in the Secretariat should be the objective, as well as the obvious prerequisites of choosing the best applicant and equality of opportunity. The strengths of former military officers, in terms of personal qualities and experience, are clear, and we accept that the Secretariat cannot encompass representatives of all the agencies it serves (and that this is not necessary, so long as the Secretariat builds an appropriate understanding and close contact with the agencies); but the appointment process, including how the posts are advertised and described, should be such as to encourage the widest range of suitable applicants.

We conclude that the MOD should move to align the terms and conditions of the advisers. It is also important to review the job specification and appointment process as set out above.

The DA Notices

53. We considered the DA-Notices themselves and particularly the case for expanding their ambit. The five standing DA-Notices date from 1993 and were updated in 2000, reflecting the changed situation arising from the end of the Cold War and then current threat levels. There have been further amendments from time to time. DA Notice 4 was amended in 2005 to include the footnote on CNI ; DA Notice 5 was reviewed in 2007 (in the light of the Terrorism Act; it was amended in 2009 to include the footnote on SOCA and was reviewed again in 2013 when SOCA handed over to the NCA and further additions to the Notice were proposed. Although there is an argument, as set out earlier, that the range of threats to national security is now even more diverse and touches many aspects of national life, we believe that expanding the remit runs the risk of weakening confidence in the system and making it unmanageable, as well as requiring substantial new resources. However, we detected an appetite from government departments and the media for updating and clarifying the language of the current DA-Notices, in particular to reflect the experience of operating them over the last decade and a half. We recommend DA-Notices are re-named, possibly as 'Security Advisory Notices' instead of 'Defence Advisory Notices', thus reflecting their scope more closely.

We conclude that DA-Notices should be renamed, that the ambit of the current DA-Notices should be retained, but that the Committee should carry

out a review of the Notices, consulting widely, with a view to refreshing the language and improving understanding of their purpose and the system as a whole.

Financial responsibilities

54. Although, as we heard, the system benefits a range of interests in the media and government, the costs are all borne by the MOD. We do not think this is equitable or sustainable and, even though the costs are relatively small, it would help if they were borne more equitably, which we also think would encourage engagement and accountability. We do not propose that the media should be asked to contribute, as cost attributions would be difficult and the principle of media payments to a government system that advises against the publication of some news stories might seem a trifle baroque.

We conclude that an equitable and straightforward split of costs should be equal shares divided between MOD, the Home Office and the FCO; this would amount to about £0.1M a year for each department.

Recommendations

55. We recommend that:

- a. The purpose of the system should remain that of preventing inadvertent disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.
- b. A restructuring of the leadership of the Committee is essential if the system is to serve its stated purpose. An independent chair should be appointed, and be supported by two vice-chairs, one from the media and one from government. These members should form a top leadership group to direct the Secretariat and to ensure that key issues are brought before the full Committee. Membership of the Committee should be widened to include representation from the intelligence and security agencies and elements of the new digital media.
- c. The Committee should be renamed to reflect its purpose better: the 'National Security Media Advisory Committee' is a possibility.

- d. There is a compelling case for changes to strengthen the operation of the system including more active promotion of it to the media and government departments.
- e. A more logical home for the DPBAC and DA-Notice system may be under the National Security Council in the Cabinet Office, as the cross-government home for national security. However, trust and confidence is currently fragile and the Committee and the system it operates need to be made more effective before such a move is made. We consider that these changes are the priority. The issue of departmental home should be discussed by the Committee so that it can be addressed after other changes recommended in this review have been implemented and shown their worth.
- f. The MOD should provide cost information through the Secretariat to the Committee and the Secretariat should provide more information on outputs in reports to the Committee. There should be clear accountability, including performance reporting, from the Secretariat to the Committee. MOD should move to align the terms and conditions of the advisers when a vacancy occurs and to review the job specification and appointment process to ensure the best field of candidates.
- g. The DA-Notices should be renamed, possibly as 'Security Advisory Notices'. The ambit of the current DA-Notices should be retained, but the Committee should carry out a review of the Notices, consulting widely, with a view to refreshing the language and improving understanding of their purpose and the system as a whole.
- h. An equitable and straightforward split of costs should be agreed between MOD, the Home Office and the FCO.

56. In conclusion, the DA-Notice system only functions with consent and support from the media and the government. It is and can only remain voluntary. Its modest cost guards against the consequences of inadvertent disclosure and it probably saves more money than is spent by relieving the need for extra press resources across the range of government departments and security agencies. Perhaps the greatest challenges to such a voluntary system are neglect and exaggerated expectation. To address these twin problems the review team believes there is an imperative to make the system fit for modern purpose; in the language of the Notices, effective operation of the Committee, the expertise available within and to the Committee, and the need to promote the value of the system more confidently within the UK. This is not a routine matter, nor one that can be tackled in two or three formal

hours of plenary session a year. Both government and media partners have a need to engage with the demands of the digital era. We have outlined here our most immediate thoughts on updating and revising the system. Both sides want it to endure. But this, for media as for government, is vital, continuing work in progress. All these conclusions, founded on continuing co-operation, may naturally need to be re-evaluated in the light of any future recommendations for a reformed Official Secrets Act

ANNEX A

TERMS OF REFERENCE

REVIEW OF THE DPBAC AND DA NOTICE SYSTEM

To review the purpose, utility and effectiveness of the Committee and the system, from the perspectives of government, media and the wider public; and to make recommendations.

The review will:

- examine the objective of the system, i.e. to limit the inadvertent public disclosure of information by mainstream press, broadcasting and internet media organisations where release would pose a risk to life or to national security;
- take account of developments in communications technology, changes in media practice and how the public now access information;
- assess UK arrangements against those of other countries to determine any lessons and best practice of relevance to this review;
- make recommendations.

Composition of Review Team

The review team will be led by s. 47F(1) [redacted]
[redacted]; the other team members will be s. 47F(1) [redacted]
[redacted]; s. 47F(1) [redacted]
[redacted]; and s. 47F(1) [redacted]
[redacted].

Sponsor

The review is sponsored by the Permanent Secretary at MOD, to whom the team will report. For day to day contact, and for administrative purposes, the sponsor's point of contact will be the Directorate of Defence Communications in MOD. The team will provide regular progress reports to the sponsor's representative.

Consultation and Working Arrangements

The team will consult members of the DPBAC and other stakeholders in government and media. Within two weeks of the initiation of the review the team will present a plan to the sponsor for the conduct of the review, to include an outline programme and estimate of time and cost. The team should present its report and recommendations to the sponsor by the end of October 2014.

ANNEX B

THOSE CONSULTED IN THE COURSE OF THE REVIEW

Cabinet Office

Ministry of Defence

Foreign and Commonwealth Office

Home Office

National Crime Agency

Intelligence and Security Agencies

BBC

Daily Mail

The Guardian

IHS Global PLC

ITV News

The Independent/London Evening Standard

Little, Brown PLC

News UK

Newspaper Society

Newspaper Publishers' Association

Press Association

Professional Publishers' Association

Sky News

Society of Editors

Telegraph Media Group

ANNEX C

DA Notice Requests for Advice – May-Nov 11³

Subject Area	Serial Numbers	Comments	Total
Special Forces	1553, 1555, 1557, 1558, 1562, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1573, 1574, 1578, 1579, 1584, 1588, 1591, 1596, 1597, 1600, 1607, 1611, 1619, 1624, 1625, 1627, 1628, 1629, 1630, 1631, 1634, 1635, 1639, 1644, 1647, 1655,	Ops, personnel, Tebbut rescue, Montecristo capture by RM,	39
Intel Agencies	1560, 1575, 1576, 1580, 1582, 1585, 1587, 1589, 1589, 1590, 1595, 1601, 1605, 1612, 1617, 1637, 1638, 1640, 1641, 1642, 1643, 1646, 1656, 1660, 1661, 1666, 1667, 1668, 1653,	Names, Libyan involvement, location of outstations,	29
Current Military Ops	1610, 1613, 1614, 1632, 1645, 1649, 1650, 1657,		8
Equipment	1556, 1592, 1615, 1616, 1618, 1620, 1623, 1625, 1651, 1652, 1662, 1663, 1664, 1665,	Exactor, IED detection	14
Counter-Terrorism	1577, 1621,		2
DA Notice System	1559, 1563, 1572, 1581, 1583, 1586, 1593, 1594, 1598, 1602, 1604, 1606, 1608, 1626, 1658, 1659,	‘D For Discretion’, Wikileaks,	16
Miscellaneous	1554, 1561, 1603, 1609, 1622, 1633, 1636, 1648, 1669,	HMS Conqueror, Riots, Live Oak, Porton Down experiments, corruption, Official Leaks,	9
Total			117

DA Notice Requests for Advice – Nov 11- May 12

Subject Area	Serial Numbers	Comments	Total
Special Forces	1688, 1693, 1694, 1696, 1697, 1702, 1705, 1708, 1719, 1720, 1721, 1734, 1750, 1790.	London Olympics, Failed hostage rescue op in Nigeria,	14
Intel Agencies	1689, 1690, 1692, 1699, 1701, 1703, 1704, 1707, 1710, 1711, 1712, 1713, 1714, 1715, 1716,	Rendition, Agency cooperation with Gaddafi’s ESO, Inquest into	50

³³ Source: DPBAC Secretariat, Sep 2014

	1717, 1722, 1724, 1725, 1727, 1728, 1729, 1730, 1731, 1735, 1736, 1737, 1739, 1745, 1747, 1752, 1762, 1764, 1766, 1767, 1770, 1771, 1772, 1773, 1775, 1776, 1777, 1778, 1781, 1783, 1784, 1785, 1787, 1788, 1792	the death of G Williams	
Current Military Ops	1748,	Prince W's SAR in Falklands	1
Equipment	1774, 1780, 1789,	JSF B v C variants	3
Counter-Terrorism	1706, 1751, 1753, 1754, 1755, 1756, 1760, 1763, 1769, 1774,		10
DA Notice System	1695, 1698, 1723, 1726, 1733, 1740, 1741, 1742, 1743, 1744, 1746, 1757, 1758, 1759, 1768, 1779, 1782, 1786,	Prince Harry's future op deployment, D Notices and Moslem demos, FOI, Review of DPBAC Sec, Final Chapters of Official History	18
Miscellaneous	1691, 1700, 1709, 1718, 1732, 1738, 1749, 1761, 1765, 1789, 1792	D Info Com, UFOs, Porton Down 'victims', FOI issues	11
Total			107

DA Notice Requests for Advice – May-Nov 12

Subject Area	Serial Numbers	Comments	Total
Special Forces	1795, 1796, 1797, 1806, 1808, 1815, 1823, 1830, 1843,	Olympics, planned SF rescue op in Afghanistan, alleged SF involvement in Syria,	9
Intel Agencies	1793, 1798, 1800, 1801, 1802, 1804, 1807, 1809, 1811, 1812, 1813, 1814, 1822, 1827, 1828, 1829, 1833, 1836, 1839, 1840, 1842, 1848, 1850, 1851, 1858	Naming, DPBAC meeting with C,	25
Current and Recent Military	1831, 1832, 1855,	Northern Ireland troubles	3

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Ops			
Equipment	1816, 1818, 1820, 1864	Trident, C2 Systems,	4
Counter-Terrorism			
DA Notice System and Application of 'D Notices'	1794, 1799, 1803, 1805, 1810, 1821, 1824, 1825, 1826, 1834, 1835, 1837, 1838, 1841, 1834, 1844, 1845, 1846, 1849, 1852, 1853, 1854	Website, historical 'D Notices', Official History, Impact of social media, relationship with PCC, Marylyn Foreman (aka, Mandy Rice-Davies), Kuala Lumpur war crimes Tribunal, Green Book, Al Hilli family murders, Managing NatSec disclosures	22
Miscellaneous	1817, 1819, 1847, 1859	Lost lap tops/briefcases, K Galalae	4
Total			67

DA Notice Requests for Advice – Nov 12 - May 13

Subject Area	Serial Numbers	Comments	Total
Special Forces	1878, 1883, 1890, 1895, 1909, 1912, 1916, 1918, 1920, 1921, 1837,	Sgt Nightingale, Naming, Historical ops,	19
Intel Agencies	1879, 1881, 1882, 1884, 1892, 1893, 1902, 1903, 1905, 1906, 1908, 1909, 1910, 1911, 1923, 1924, 1927, 1931,	Naming	24
Current and Recent Military Ops	1900, 1907, 1913, 1914, 1922,	Northern Ireland, Possible SF rescue op in Nigeria,	5
Equipment		Astute capabilities	1
Counter-Terrorism	1883, 1932, 1934,		3

DA Notice System and Application of 'D Notices'	1875, 1878, 1880, 1886, 1887, 1888, 1889, 1896, 1997, 1898, 1899, 1901, 1904, 1915, 1917, 1919, 1925, 1926, 1928, 1929, 1930, 1935, 1936, 1938,	PQ re paedo, D Notices and SM, Op ORE, Dunblane Massacre, Number of DAN issued, Naming of people by DA Notices, coastal erosion through dredging,	24
Miscellaneous	1877, 1885, 1991, 1894, 1933, 1937		7
Total	1860-1938		83

DA Notice Requests for Advice – May-Nov 13

Subject Area	Serial Numbers	Comments	Total
Special Forces	1942, 1950, 2008, 2027, 2028, 2031, 2032,	Death of Princess Dianna	7
Intel Agencies	1943, 1944, 1946, 1947, 1948, 1951, 1952, 1953, 1954, 1955, 1956, 1967, 1958, 1960, 1961, 1963, 1964, 1965, 1966, 1968, 1969, 1970, 1971, 1972, 1975, 1979, 1987, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2002, 2003, 2004, 2005, 2006, 2007, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2023, 2024, 2025, 2026, 2029, 2033, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2060, 2061, 2062, 2063	Naming, Snowden disclosures, death of Princess Dianna	85
Current and Recent Military Ops	1974, 1984, 1985, 1986, 2035, 2043,	Tellic	6
Equipment	0	0	0

Counter-Terrorism	1941, 2001,	Internet chat rooms	2
DA Notice System and Application of 'D Notices'	1945, 1962, 1967, 1973, 1977, 1980, 1981, 1982, 1983, 2011, 2012, 2021, 2030, 2036, 2059, 2064,	Foreign misrepresentation Twitter Accounts, 'Fighting for Justice', deaths of SF on Brecon Beacons, AR to DPBAC, admin links between DPBAC Sec and DMC, aerial photography	16
Miscellaneous	1940,1949, 1959, 1976, 1978, 2010, 2022, 2034	Hollie Greig, MP in Brothel, Secret Listeners, Scottish independence, Spadeadam, WW2 air op,	8
Total			124

DA Notice Requests for Advice – Nov 13 to May 14

Subject Area	Serial Numbers	Comments	Total
Special Forces	2079, 2149, 2175, 2181, 2182, 2189,	Failed SF raid involving death of Capt R Holloway, Naming and photos of ex-DSFs, Lord Ashcroft book	6
Intel Agencies	2065, 2066,2067, 2068, 2069,2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2080, 2081, 2082, 2084, 2086, 2087, 2091,2092, 2093, 2094, 2098, 2102, 2103, 2106, 2107, 2108, 2109, 2111, 2112, 2113, 2114, 2115, 2116, 2118, 2119, 2124, 2126, 2127, 2130, 2131, 2132, 2135, 2137, 2138,	Snowden disclosures, naming, houses in South London, Ian Lobham's successor	68

	2139, 2140, 2141, 2144, 2146, 2148, 2150, 2152, 2153, 2157, 2158, 2162, 2164, 2165, 2166, 2171, 2180, 2185, 2186, 2188		
Current and Recent Military Ops	2104, 2154, 2163, 2167,	RAdS project, Op Tellic, 'Secret Listeners'	4
Equipment			0
Counter-Terrorism	2133, 2145,	Cloud Systems & Jihadists	2
Nuclear Wpns and Nuclear Security	2090,	AWC Guarding	1
DA Notice System and Application of 'D Notices'	2083, 2085, 2088, 2089, 2095, 2096, 2097, 2099, 2100, 2101, 2105, 2110, 2120, 2121, 2122, 2123, 2124, 2125, 2128, 2129, 2142, 2143, 2147, 2151, 2155, 2156, 2159, 2160, 2168, 2170, 2172, 2173, 2174, 2176, 2178, 2179, 2183, 2184, 2187, 2190,	DA Notices and VCJD, Peter Barron & Jane Crust resignations, MPS & Child pornography, Op Ore, Danish BC on UK policy on Iraqi interpreters, Cab Office OSA, Case studies to RMAS	40
Miscellaneous	2117, 2134, 2136, 2161, 2169, 2177,	New DT editor. Historic issues, Fracking, Danish BC re Iraqi interpreters	6
Total			126

**GOVERNMENT RESPONSE TO THE REVIEW OF THE DEFENCE ADVISORY
NOTICE SYSTEM AND THE DEFENCE PRESS AND BROADCASTING
ADVISORY COMMITTEE**

Last year, the Ministry of Defence initiated a review of the Defence Advisory Notice (DA Notice) System and the Defence Press and Broadcasting Advisory Committee (DPBAC), the Terms of Reference for which were published on the DPBAC's public website (www.dnotice.org.uk).

I am very grateful to the review team led by s. 47F(1)
[REDACTED] and comprising s. 47F(1)
[REDACTED], s. 47F(1)
[REDACTED], and s. 47F(1)
[REDACTED], for their very comprehensive work on the review. I
welcome their final Report, which I am confident represents an independent,
objective and thorough analysis of the issues that have a bearing on the DPBAC and
DA Notice system.

The Government agrees with the majority of the findings of the review, and considers
that the implementation of the recommendations will lead to an improved DA Notice
system and DPBAC with clearer accountabilities. Where recommendations are not
accepted in full, we endeavour to accede to the spirit of their intent.

Our response to each of the recommendations is at Annex. We will proceed to
implement the accepted recommendations in the coming months.

S. 47F(1)

ANNEX A

DETAILED RESPONSE TO THE EIGHT RECOMMENDATIONS OF THE REVIEW

- 1. The purpose of the system should remain that of preventing inadvertent disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.**

The Government agrees that the purpose of the system should remain that of preventing inadvertent disclosure of information that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.

- 2. A restructuring of the leadership of the Committee is essential if the system is to serve its stated purpose. An independent chair should be appointed, and be supported by two vice-chairs, one from the media and one from government. These members should form a top leadership group to direct the Secretariat and to ensure that key issues are brought before the full Committee. Membership of the Committee should be widened to include representation from the intelligence and security agencies and elements of the new digital media.**

We agree that the effective leadership of the Committee is essential to ensure its ongoing efficacy. It is considered that the best means of achieving this is through a senior Government official whose role is best aligned with the work of the Committee and who is able to devote the necessary time to overseeing that work and the DA Notice process. Whilst we acknowledge that the appointment of an independent Chair could help to reinforce the fact that the DPBAC oversees a voluntary code and that notices and advice are issued with the agreement of media representatives, it is ultimately the Government that meets the costs of the Committee and the system, and that is responsible for the security matters on which the DPBAC issues advice, and must therefore be accountable for the Committee and its work. As such, we propose that the MOD Director General, Security Policy and Operations takes over as the permanent Chair of the Committee. The Director General, Security Policy is

closely involved in the work about which DA Notice advice is issued, and regularly engages with Government colleagues who are members of the Committee. As part of this role, the new Chair will take over the performance reporting arrangements for the DPBAC Secretariat.

We agree that given the growing importance of digital and social media, the Committee membership should be widened to include representatives of these media organisations as appropriate. In addition, whilst it would not be appropriate for representatives from the Government Agencies to be permanent members of the Committee, we agree that they may be invited to attend meetings of the DPBAC on an ad hoc basis and as required.

3. The Committee should be renamed to reflect its purpose better: the 'National Security Media Advisory Committee' is a possibility.

We agree that a new name that better reflects the current role of the Committee should be adopted, and that further consultation of stakeholders should be undertaken to determine what that name should be.

4. There is a compelling case for changes to strengthen the operation of the system including more active promotion of it to the media and government departments.

The Government notes that effort has been made to date to raise awareness of the role of the DPBAC and DA Notice system by the DPBAC Secretariat, but agrees that work should continue to be done to actively promote the Committee's work, particularly in light of the improvements being made following the Review.

5. A more logical home for the DPBAC and DA-Notice system may be under the National Security Council in the Cabinet Office, as the cross-government home for national security. However, trust and confidence is currently fragile and the Committee and the system it operates need to be made more effective before such a move is made. We consider that these changes are the priority. The issue of departmental home should be discussed by the Committee so that it can be addressed after other changes recommended in this review have been implemented and shown their worth.

We agree that implementing the improvements proposed under this Review should be the immediate priority and that options for the location of the DPBAC should be revisited at an appropriate time in the future. Moving the Committee to the Cabinet Office is but one option; we would need to consider the pros and cons of all options, including maintaining the current arrangements, at the point when this issue is looked at again.

- 6. The MOD should provide cost information through the Secretariat to the Committee and the Secretariat should provide more information on outputs in reports to the Committee. There should be clear accountability, including performance reporting, from the Secretariat to the Committee. MOD should move to align the terms and conditions of the advisers when a vacancy occurs and to review the job specification and appointment process to ensure the best field of candidates.**

We agree that there should be clearer accountability, including performance reporting, of the DPBAC Secretariat to the Committee, and that the Secretariat should agree with the new Chair and the Committee clear objectives and reporting criteria for the coming financial year.

We also agree that the terms and conditions of the Secretariat team should be aligned as vacancies arise, and that new advisors should be recruited to refreshed job specifications through the most appropriate means to ensure the widest field of suitable candidates.

- 7. The DA-Notices should be renamed, possibly as 'Security Advisory Notices'. The ambit of the current DA-Notices should be retained, but the Committee should carry out a review of the Notices, consulting widely, with a view to refreshing the language and improving understanding of their purpose and the system as a whole.**

We agree that there may be merit in renaming the DA Notices to better reflect their purpose and to align with the new name of the Committee, although the nature and scope of the current DA Notices should be retained. We agree that a further review of the Notices should be undertaken by the Secretariat with a view to updating and simplifying the language used and ensuring a common understanding of their scope

and purpose across the wider internal and external audiences.

8. An equitable and straightforward split of costs should be agreed between MOD, the Home Office and the FCO.

Whilst we see the merit in moving to a position whereby the costs of the DPBAC and Secretariat are shared by each of the Departments with a key stake in them, we consider that the administrative burden of implementing this recommendation would be disproportionate to the small sums involved and therefore agree that the costs should continue to fall to one department and that this should remain the MOD.

From: s. 22(1)(a)(ii)
To: s. 11C(1)(a) (DFAT)
Cc: s. 22(1)(a)(ii) s. 22(1)(a)(iii) ; s. 22(1)(a)(ii) ; s. 22(1)(a)(ii) ; s. 22(1)(a)(ii) Europe Engagement
Subject: RE: Request for Report on Review of DSMA System [SEC=OFFICIAL:Sensitive]
Date: Tuesday, 28 June 2022 3:16:15 PM
Attachments: [image001.gif](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.jpg](#)
[image006.jpg](#)

OFFICIAL: Sensitive

Hi s. 11C(1)(a)

Thanks again for this – the report from the 2015 Review has been immensely helpful in understanding the evolution of the DSMA system in the UK.

Please see below a few follow-up questions we have. If you find an appropriate opportunity at the DSMA Committee Reception, we would be grateful if you could try and track down some answers for us. Apologies for the delay in getting these to you – I hope we got them to you with enough notice!

- Has the DSMA Committee had any progress in getting digital industry engaged as part of the Committee or sub-groups? We understand that when Andrew met with Brig Dodds last, he indicated that he does not provide advice to digital media organisations.
- How involved or engaged are UK intelligence and security agencies in the DSMA system? Does Brig Dodds ever receive pushback or are agencies generally supportive and willing to engage? We note only the Defence, Home and Foreign ministries are represented on the Committee so are curious as to the level of engagement they have.
- How is the system dealing with the diversification of national security threats, for example, into things like critical infrastructure and even organised crime (e.g. undercover law enforcement operations)? Do media outlets ever consult the DSMA Secretary when they want to report on these kinds of issues, noting they do not fall within the scope of the Notices, which are focused on military and intelligence issues?
- Has there been any progress regarding the inclusion of staff in the DSMA Secretariat who have a national security/intelligence background?

Kind regards,

s. 22(1)(a)

s. 22(1)(a)(ii) | Law Enforcement Powers Section | Electronic Surveillance and Law Enforcement Policy Division | P: s. 22(1)(a)(ii)

OFFICIAL: Sensitive

OFFICIAL:Sensitive

Printed by S. 22(1)(a)(ii) - 10:27 AM Friday, 8 July 2022

IC75680L

Title: Overview of US, Canada and UK engagement on electronic surveillance and cross-border data (CLOUD) Act implementation
MRN: IC75680L 26/05/2022 10:16:07 AM
To: London; Ottawa; San Francisco; Washington
Cc: RR : USA Posts
From: Canberra (CHCH/HOMEAFF)
From File:
EDRMS
Files:
References: LH642397L, LH642895L
Response: Routine, Information Only

Summary

s. 22(1)(a)(ii)



1. s. 22(1)(a)(ii)



s. 22(1)(a)(ii)

2. s. 22(1)(a)(ii)



3. s. 22(1)(a)(ii)



4. s. 22(1)(a)(ii)



OFFICIAL:Sensitive

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

OFFICIAL:Sensitive

Printed by s. 22(1)(a)(ii) - 10:27 AM Friday, 8 July 2022

IC75680L

s. 22(1)(a)(ii)



5. s. 22(1)(a)(ii)



6. s. 22(1)(a)(ii)



s. 22(1)(a)(ii)

7. s. 22(1)(a)(ii)



8. s. 22(1)(a)(ii)



9. s. 22(1)(a)(ii)



10. s. 22(1)(a)(ii)



s. 22(1)(a)(ii)

11. s. 22(1)(a)(ii)



12. s. 22(1)(a)(ii)



OFFICIAL:Sensitive

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

OFFICIAL:Sensitive

Printed by s. 22(1)(a)(ii) - 10:27 AM Friday, 8 July 2022

IC75680L

s. 22(1)(a)(ii)

[Redacted]

13. s. 22(1)(a)(ii)

[Redacted]

14. s. 22(1)(a)(ii)

[Redacted]

15. s. 22(1)(a)(ii)

[Redacted]

16. Following-on from Deputy Secretary Ablong's visit in December (LH642397L), the delegation met with the Secretary of the Defence and Security Media Advisory (DSMA) Committee, Brigadier Geoffrey Dodds OBE, to learn more about the work of the DSMA Committee and its engagement with the media. s. 47C(1)

[Redacted]

s. 22(1)(a)(ii)

17. s. 22(1)(a)(ii)

[Redacted]

18. s. 22(1)(a)(ii)

[Redacted]

19. s. 22(1)(a)(ii)

[Redacted]

text ends

Sent by: s. 22(1)(a)(ii)

Prepared by: s. 22(1)(a)(ii)

Approved by: s. 22(1)(a)(ii)

Topics: INTERNATIONAL SECURITY/Intelligence Policy, LEGAL/International Law

Canberra distribution

OFFICIAL:Sensitive

Released by Department of Home Affairs
under the Freedom of Information Act 1982

From: [Warnes, Andrew](#)
To: [Geoffrey Dodds](#)
Cc: s. 47F(1) [@mod.gov.uk](#); s. 47F(1) s. 47F(1)
Subject: RE: Request for further meeting - Australian Government [SEC=OFFICIAL]
Date: Friday, 7 October 2022 3:57:00 PM
Attachments: [image001.png](#)

OFFICIAL

That's fantastic. We will work with s. 47F(1) and tee up a time.

Many thanks

Andrew

OFFICIAL

From: Geoffrey Dodds s. 47F(1) [@dsma.uk](#)>
Sent: Thursday, 6 October 2022 8:21 PM
To: Warnes, Andrew s. 22(1)(a)(ii) [@ag.gov.au](#)>
Cc: s. 11C(1)(a) s. 22(1)(a)(ii) [@dfat.gov.au](#)>; s. 22(1)(a)(ii) [@ag.gov.au](#)>; s. 22(1)(a)(ii) [@ag.gov.au](#)>; s. 22(1)(a)(ii) [@ag.gov.au](#)>; s. 22(1)(a)(ii) [@ag.gov.au](#)>; s. 47F(1) [@mod.gov.uk](#); s. 47F(1) [@mod.gov.uk](#); s. 47F(1) [@mod.gov.uk](#)>
Subject: Re: Request for further meeting - Australian Government [SEC=OFFICIAL]

CAUTION: This email originated from outside of the organisation. Do not follow guidance, click links, or open attachments unless you recognise the sender and know the content is safe.

Dear Andrew,

Many thanks for your email. How very good to hear from you again.

I would be very happy to contribute to an online discussion/Q&A session at your convenience.

Given the time difference, I imagine you would prefer early morning or late evening UK time slot? I would be happy to do either but if given the choice, would prefer early morning UK time.

I have included my MOD email address in the cc line above and suggest an MS Teams discussion on that means would be best. s. 47F(1) is the best contact for making arrangements.

Best wishes,
Geoffrey

Brigadier (Retired) Geoffrey Dodds | Secretary | Defence and Security Media Advisory Committee | 4.4.113 | Ministry of Defence Main Building | 2 Horse Guards Avenue |

Whitehall | LONDON SW1A 2HB | Office s. 47F(1) Mobile s. 47F(1)
| s. 47F(1)@dsma.uk | www.dsma.uk

From: Warnes, Andrew s. 22(1)(a)(ii) @ag.gov.au>
Sent: 06 October 2022 05:38
To: Geoffrey Dodds s. 47F(1)@dsma.uk>
Cc: s. 11C(1)(a) s. 22(1)(a)(ii) @dfat.gov.au>; s. 22(1)(a)(ii) @ag.gov.au>; s. 22(1)(a)(ii) @ag.gov.au>; s. 22(1)(a)(ii) @ag.gov.au>; s. 22(1)(a)(ii) @ag.gov.au>
Subject: Request for further meeting - Australian Government [SEC=OFFICIAL]

OFFICIAL

Dear Brigadier Dodds

It was great to meet with you in May this year to learn more about the work of the Defence Security Media Advisory (DSMA) Committee and its engagement with the media. s. 47C(1)

[Redacted]

s. 47C(1)

[Redacted]

If you would be happy to engage in a virtual meeting please let me know the best contact to work with to make appropriate arrangements.

Kind Regards

Andrew

Andrew Warnes | First Assistant Secretary
Criminal Justice Division
Attorney-General's Department
Tel s. 22(1)(a)(ii) s. 22(1)(a)(ii)@ag.gov.au

2586 Indigenous signature block NEW5 (2)



OFFICIAL

BILATERAL MEETING – Dominic Wilson, Chair, Defence and Security Media Advisory Committee, United Kingdom

Dominic Wilson

Director General Security Policy, Ministry of Defence and Chair, Defence and Security Media Advisory Committee

Time TBC, 45 minutes allocated. Thursday 1 August 2019, London

Context and objectives

What we want

• s. 47C(1)

What they want

- To share the United Kingdom's experience in this field.

Handling note

s. 47C(1)

s. 47C(1)

Talking points

- Thank you for meeting with me to discuss the policy framework surrounding the Defence and Security Media Advisory Committee arrangement.
- This enduring tension between press freedoms and national security has been brought into focus again recently in Australia, with the Australian Federal Police executing two separate search warrants relating to allegations of publishing classified material, contrary to provisions of our *Crimes Act 1914*.
 - Of course, the publication of classified material is an extremely serious matter that has the potential to undermine Australia's national security.

- However, these raids have been viewed domestically and internationally as an attack on press freedom, including at the recent Global Conference for Media Freedom in London.
- We believe that a sensible balance needs to be reached between protecting our national interest in the face of ever-evolving security challenges and upholding the public's right to know.
- Australia once had a similar system to that of the UK, however it fell into disuse some time ago. What I'm interested in understanding is how you have evolved and maintained your system to maintain its effectiveness in the contemporary setting that of the internet and 24/7 hour news cycle.

Questions you may wish to ask

- Whether the DSMA-notice system delivers the intended outcomes, or whether there are areas where it is not as effective as it could be?
- Why the Voluntary Code works in the United Kingdom, noting your cultural setting, history and relationship between the media and government outside of the national security context.
- Whether there have been situations where the media deliberately did not seek advice from the Committee
- Describe how the public narrative relating to the DSMA Notices has evolved and the public's reaction to it, including criticism of government trying to obfuscate information it doesn't want the public to know.
- Describe the rationale for there being no sanctions available to the Committee where advice is not sought, and the effectiveness of that approach.
- Explain the legal obligations of the DSMA Committee, including when asked to provide information by the Metropolitan Police.
- Whether there is sufficient digital media representation on the Committee, and the lessons learned engaging with digital media.
- Considerations that go into the development of new DSMA notices, including anticipating need, or being reactive to requests from industry.
- Describe the intangible reputational elements that contribute to the effectiveness of the DSMA construct, and whether it varies based on the personality of individuals occupying critical roles.

Background

The Defence and Security Media Advisory Committee oversees a voluntary code which operates between the Government departments which have responsibilities for national security and the media. It uses the Defence and Security Media Advisory (DSMA)-notice system as its vehicle.

The aim of the DSMA-notice system is to prevent inadvertent public disclosure of information that would compromise United Kingdom military and intelligence operations and methods; or put at risk the safety of those involved in such

operations; or lead to attacks that would damage the critical national infrastructure and/or endanger lives.

Although not subject to the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002, the DSMA Committee is committed to practising a policy of maximum disclosure of its activities consistent with the effective conduct of business and the need to ensure that it honours any assurance of confidentiality given to the individuals and organisations with which it deals.

Composition

The Committee is chaired by the Director General Security Policy, Ministry of Defence. Membership may be varied from time to time by agreement. At present there are four members representing Government departments, one each from the Home Office, the Ministry of Defence, the Foreign and Commonwealth Office and the Cabinet Office. There are currently seventeen members nominated by the Media; five by the News Media Association (NMA), two by the Committee's Chairs, one by the Professional Publishers Association (but has vacancies for two) and one each by the Scottish Newspaper Society, the Press Association, the BBC, ITN, ITV, Sky TV, the Society of Editors, IHS Markit (Jane's), the (Book) Publishers Association and two by the Committee's Chairs.

The media members select one of their number as Chair of their side and Vice-Chair of the Committee. He/she leads for their side at Committee meetings and provides a point of day-to-day contact for them and for the Secretary.

The DSMA Committee is served by a Secretary who acts as the Committee's executive office and two part-time Deputy Secretaries. The Secretary is responsible (on behalf of the Committee) for addressing any DSMA Notice policy issues which may need to be resolved. For two weeks in each four-week period, he also acts as the on-duty DSMA Notice adviser, offering DSMA Notice advice to the media on individual national security disclosure cases. Each of the deputies acts as the on-duty DSMA Notice adviser for one week in every four-week period. At all times there is a single point of contact and responsibility for offering DSMA Notice advice to the media.

Related briefs / attachments

Title
Classified pack – Attachment X: Cable XXXX

Point of contact

Engagement with the UK on the DSMA	Adam Meyer, Minister-Counsellor, Home Affairs, London. Ph: mobile s. 22(1)(a)(ii)
---	---

Biography of Dominic Wilson



Dominic Wilson

Director General Security Policy, Ministry of Defence and Chair of the Defence and Security Media Advisory Committee

Dominic Wilson is responsible for international security policy in the Middle East and North Africa, Sub-Saharan Africa, Asia-Pacific and Latin America, and for policy advice on a range of thematic issues including counter-terrorism, cyber, building stability overseas, conflict prevention and for support to the civil authorities in the UK.

Previous appointments:

- Director Operational Policy
- Director Security and Intelligence (Cabinet Office)
- Director Strategy and Resources

~~PROTECTED~~

Exported by s. 11C(1)(a) - 09:13 AM Monday, 13 December 2021

LH642397L

Title: UK: Visit to London by Deputy Secretary Strategy and National Resilience, Marc Ablong PSM
MRN: LH642397L 13/12/2021 09:08:42 AM GMT
To: Canberra
Cc: RR : Immigration Posts, Wellington
From: London
From File:
EDRMS
Files:
References: LH641830L, LH642144L, LH642319L, LH642375L, LH642377L, CE1008700L
Response: Routine, Information Only

Summary

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

~~PROTECTED~~

~~PROTECTED~~

Exported by S. 11C(1)(a) - 09:13 AM Monday, 13 December 2021

LH642397L

s. 22(1)(a)(ii)

Defence and Security Media Advisory Committee

22. Ablong met with the Secretary of the Defence and Security Media Advisory (DSMA) Committee, Brigadier Geoffrey Dodds OBE, to learn more about the work of the DSMA Committee and its engagement with the media. The discussion focussed on the operation of the Committee, the role of the Secretary, the use of D-notices and how the Committee worked in partnership with media to provide advice on stories of defence and security importance.

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

~~PROTECTED~~

s. 47F(1)

PA to Sec DSMA Committee

Microsoft Teams meeting

Join on your computer, mobile app or room device

[Click here to join the meeting](#)

Meeting ID: **S. 22(1)(a)(ii)**

Passcode: **S. 22(1)(a)**

[Download Teams](#) | [Join on the web](#)

[Learn More](#) | [Meeting options](#)

If you have received this transmission in error please notify us immediately by return e-mail and delete all copies. If this e-mail or any attachments have been sent to you in error, that error does not constitute waiver of any confidentiality, privilege or copyright in respect of information in the e-mail or attachments.

WARNING

This email message and any attached files may contain information that is confidential and subject of legal privilege intended only for use by the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the message to the intended recipient be advised that you have received this message in error and that any use, copying, circulation, forwarding, printing or publication of this message or attached files is strictly forbidden, as is the disclosure of the information contained therein. If you have received this message in error, please notify the sender immediately and delete it from your inbox.
AFP Web site: <http://www.afp.gov.au>



List of Invitees

Briefing with Brig Geoffrey Dodds, Secretary UK Defence and Security Media Advisory (DSMA) System

Recommendation 8 of the PJCIS Press Freedoms Inquiry

Name	Position	Agency	
Mr Andrew Warnes	First Assistant Secretary, Criminal Justice Division	Attorney-General's Department	s. 22(1)(a)(ii) @ag.gov.au
Ms Susan McKeag	Assistant Secretary, Criminal Law Policy Branch	Attorney-General's Department	s. 22(1)(a)(ii) @ag.gov.au
Mr Luke McGowan	Assistant Secretary, Joint and Enabler Analysis	Department of Defence	s. 22(1)(a)(ii) @defence.gov.au
Mr Steve McGlynn	First Assistant Director-General, People, Property and Legal	Department of Defence	s. 22(1)(a)(ii) @defence.gov.au
s. 22(1)(a)(ii)	Director, Special Counsel Defence Security	Department of Defence	s. 22(1)(a)(ii) @defence.gov.au
Mr Lachlan Colquhoun	First Assistant Secretary, National Security Division	Department of Prime Minister and Cabinet	s. 22(1)(a)(ii) @pmc.gov.au
Mr Brendan Dowling	First Assistant Secretary, Digital and Technology Policy Division	Department of Home Affairs	s. 22(1)(a)(ii) @homeaffairs.gov.au
s. 22(1)(a)(ii)	Legal Adviser	Department of Foreign Affairs and Trade	s. 22(1)(a)(ii) @dfat.gov.au
Ms Ciara Spencer	First Assistant Secretary, International Security Division	Department of Foreign Affairs and Trade	s. 22(1)(a)(ii) @dfat.gov.au
s. 22(1)(a)(ii)	Commonwealth Solicitor	Commonwealth Director of Public Prosecutions	s. 22(1)(a)(ii) @cdpp.gov.au

s. 22(1)(a)(ii)	Manager, Government and Executive Advice	Australian Federal Police	s. 22(1)(a)(ii)	Page 2 of 2 @agd.gov.au
-----------------	--	---------------------------	-----------------	--

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)		Home Affairs	s. 22(1)(a)(ii)	@agd.gov.au
-----------------	--	--------------	-----------------	-----------------------------



Agenda

Briefing on UK Defence and Security Media Advisory (DSMA) System

With Brigadier Geoffrey Dodds, DSMA Secretary

Wednesday 2 November 2022, 7pm-8pm AEDT (8am-9am GMT)

Item	Topic	Lead	Time
1	Welcome and introductions	Attorney-General's Department (AGD)	5 min
2	Background	AGD	5 min
3	Briefing on DSMA System	Brig Dodds, DSMA Secretary	10 min
4	Questions and discussion	AGD/All	35 min
5	Final comments and close	AGD	5 min



Australian Government
Attorney-General's Department

Meeting Agenda

Briefing on UK Defence and Security Media Advisory (DSMA) System

With Brigadier Geoffrey Dodds, DSMA Secretary

Wednesday 2 November 2022, 7pm-8pm AEDT (8am-9am GMT)

Topic	Talking Points
Welcome	• Welcome to country. • Introduce yourself. • Introduce Brigadier Geoffrey Dodds. ○ Brigadier Dodds is the Secretary of the UK Defence and Security Media Advisory (DSMA) System. He commenced as Secretary of the DSMA Committee in November 2016. ○ Prior to that he spent 36 years in the British Army and has served in United Nations Headquarters as a military planner, in various NATO posts and in military diplomatic appointments worldwide. • Invite introductions from participants [<i>handling note – [REDACTED] will not introduce themselves but will listen to the discussion and filter questions through LEPS</i>].
Background	• [REDACTED] • [REDACTED] • [REDACTED] • The UK model works well in the UK context, and we note that a review completed in 2015 found that both media and government remain supportive of the DSMA model.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Briefing on DSMA System	• Invite Brigadier Dodds to speak to the DSMA System.
Questions and discussion	• Thank Brigadier Dodds and invite questions on the DSMA System from agencies present. <u>Questions for Brigadier Dodds</u> <u>Advice to journalists</u> • <i>What form of advice is provided to journalists? (e.g. verbal, track changes on articles)?</i> • <i>What topics or issues do enquiries typically relate to?</i> • <i>Does advice centre around agreed sensitive matters in the notices, or do other considerations (e.g. public interest) factor in to advice?</i> • <i>What kind of detail, in addition to the text of the Notices, is provided by agencies via the DSMA System when agencies are also consulted?</i> • <i>Does advice extend to law enforcement activities, or is it limited to military and security agencies only?</i> ○ <i>If not, why not? If not, is there is risk of disconnect between what you advise can be published and what investigative bodies may consider an unauthorised disclosure of sensitive information?</i> <u>Consultation with agencies</u> • <i>Is direct engagement with government agencies the encouraged method for communications to occur?</i> ○ <i>Is the DSMA System promoted as a secondary/fall back option if it is unclear who the relevant government agency is, or if the agency is unable to provide a clear response?</i> • <i>Are there exceptions where you do not require/seek agreement from a journalist to consult with/inform an agency of an inquiry? For example, if there could be risk to life or serious risk to national security? If so:</i> ○ <i>What are the thresholds for informing an agency?</i> ○ <i>Are these exceptions explicitly captured in governance documents?</i> • <i>How often do you consult an agency to seek further advice or detail in order to inform your response to a journalist's enquiry?</i> ○ <i>What would normally prompt you to need to consult with an agency?</i> • <i>Have there been instances of a journalist not giving permission for you to consult with a relevant agency to seek further guidance or context?</i> ○ <i>What do you do in these situations?</i> ○ <i>Is the journalist's identity always kept confidential when consulting with an agency?</i> • <i>When consulted by a government agency considering initiating police or legal action against a media organisation or journalist, what information are you able to provide about your interactions with that organisation or journalist?</i>

	<u>Security considerations</u> • <i>Is there a risk that a journalist may inadvertently disclose classified information through their enquiry? If so, how is this managed or mitigated?</i> • <i>Are there concerns that sensitive conversations take place on unclassified telecommunication equipment?</i> • <i>Is there a risk that incomplete or inaccurate advice could be provided to a journalist due to lack of context around the subject of their enquiry? For example, additional context or detail you are not aware of, which would change how an enquiry should be understood and evaluated against the DSMA Notices (e.g. seemingly benign detail is actually highly sensitive)? Is this a risk in the DSMA System, and if so, how is it managed?</i> • <i>If you know there has been a leak of classified information, are you required to report that unauthorised disclosure, e.g. to the agency that owns that information?</i> • <i>How does the DSMA System handle issues relating to security breaches?</i> ○ <i>Are there mitigation strategies embedded in the DSMA System that serve to limit further security breaches of classified information beyond the initial breach of the journalist possessing the information?</i> • <i>Is the fact that a journalist has sought advice from you, and that advice did not indicate a national security risk, a defence against the Official Secrets Act?</i> • <i>Have there been instances where the media or a journalist have been advised not to publish but have published the information regardless?</i> • <i>What is the process for managing approaches by media or journalists who are clearly seeking to reduce the risk of prosecution for (or even seek immunity from) publishing sensitive national security information that is also arguably in the public interest?</i> <u>Logistics and operation</u> • <i>How often is the DSMA System consulted by media?</i> • <i>What is the process for appointing the DSMA Secretary and Deputies?</i> • <i>What IT systems are used in the DSMA office? (e.g. Ministry of Defence)</i> ○ <i>What type of information is retained or stored on the systems?</i> • <i>What is the relationship like between the DSMA System and government agencies?</i> • <i>Is there any oft-cited feedback from agencies regarding how the system operates?</i>
Final comments and close	• Thank Brigadier Dodds for his time. • Today's discussion will help inform and further refine our thinking around a consultation mechanism in Australia. • Thank participants for their attendance.



Australian Government
Attorney-General's Department

Questions

Briefing on UK Defence and Security Media Advisory (DSMA) System

With Brigadier Geoffrey Dodds, DSMA Secretary

Wednesday 2 November 2022, 8am-9am GMT (7pm-8pm AEDT)

Advice to journalists

- *What form of advice is provided to journalists? (e.g. verbal, track changes on articles)?*
- *What topics or issues do enquiries typically relate to?*
- *Does advice centre around agreed sensitive matters in the notices, or do other considerations (e.g. public interest) factor in to advice?*
- *What kind of detail, in addition to the text of the Notices, is provided by agencies via the DSMA System when agencies are also consulted?*
- *Does advice extend to law enforcement activities, or is it limited to military and security agencies only?*
 - *If not, why not? If not, is there is risk of disconnect between what you advise can be published and what investigative bodies may consider an unauthorised disclosure of sensitive information?*

Consultation with agencies

- *Is direct engagement with government agencies the encouraged method for communications to occur?*
 - *Is the DSMA System promoted as a secondary/fall back option if it is unclear who the relevant government agency is, or if the agency is unable to provide a clear response?*
- *Are there exceptions where you do not require/seek agreement from a journalist to consult with/inform an agency of an inquiry? For example, if there could be risk to life or serious risk to national security? If so:*
 - *What are the thresholds for informing an agency?*
 - *Are these exceptions explicitly captured in governance documents?*
- *How often do you consult an agency to seek further advice or detail in order to inform your response to a journalist's enquiry?*
 - *What would normally prompt you to need to consult with an agency?*
- *Have there been instances of a journalist not giving permission for you to consult with a relevant agency to seek further guidance or context?*
 - *What do you do in these situations?*
 - *Is the journalist's identity always kept confidential when consulting with an agency?*

Released by Department of Home Affairs
under the Freedom of Information Act 1982

- *When consulted by a government agency considering initiating police or legal action against a media organisation or journalist, what information are you able to provide about your interactions with that organisation or journalist?*

Security considerations

- *Is there a risk that a journalist may inadvertently disclose classified information through their enquiry? If so, how is this managed or mitigated?*
- *Are there concerns that sensitive conversations take place on unclassified telecommunication equipment?*
- *Is there a risk that incomplete or inaccurate advice could be provided to a journalist due to lack of context around the subject of their enquiry? For example, additional context or detail you are not aware of, which would change how an enquiry should be understood and evaluated against the DSMA Notices (e.g. seemingly benign detail is actually highly sensitive)? Is this a risk in the DSMA System, and if so, how is it managed?*
- *If you know there has been a leak of classified information, are you required to report that unauthorised disclosure, e.g. to the agency that owns that information?*
- *How does the DSMA System handle issues relating to security breaches?*
 - *Are there mitigation strategies embedded in the DSMA System that serve to limit further security breaches of classified information beyond the initial breach of the journalist possessing the information?*
- *Is the fact that a journalist has sought advice from you, and that advice did not indicate a national security risk, a defence against the Official Secrets Act?*
- *Have there been instances where the media or a journalist have been advised not to publish but have published the information regardless?*
- *What is the process for managing approaches by media or journalists who are clearly seeking to reduce the risk of prosecution for (or even seek immunity from) publishing sensitive national security information that is also arguably in the public interest?*

Logistics and operation

- *How often is the DSMA System consulted by media?*
- *What is the process for appointing the DSMA Secretary and Deputies?*
- *What IT systems are used in the DSMA office? (e.g. Ministry of Defence)*
 - *What type of information is retained or stored on the systems?*
- *What is the relationship like between the DSMA System and government agencies?*
- *Is there any oft-cited feedback from agencies regarding how the system operates?*

From: s. 22(1)(a)(ii)
To: s. 22(1)(a)(ii); s. 22(1)(a)(ii)
Subject: FW: NOTES FOR ONLINE DSMA BRIEFING - WED 2 NOV 22
Date: Wednesday, 2 November 2022 10:29:22 AM
Attachments: [DSMA Notice System Briefing.docx](#)
[Responses to AUS AGD.docx](#)

s. 33(a)(iii)

Hi,

Brigadier Dodds has sent me the attached documents overnight.

Thanks

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Executive Assistant to Andrew Warnes, First Assistant Secretary
Criminal Justice Division
Attorney-General's Department

P: s. 22(1)(a)(ii)

M: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au)

From: Geoffrey Dodds s. 47F(1)@dsma.uk>

Sent: Wednesday, 2 November 2022 2:58 AM

To: s. 22(1)(a)(ii) s. 22(1)(a)(ii)@ag.gov.au>

Cc: s. 47F(1)@dsma.uk>; Geoffrey Dodds s. 47F(1)@dsma.uk>

Subject: NOTES FOR ONLINE DSMA BRIEFING - WED 2 NOV 22

CAUTION: This email originated from outside of the organisation. Do not follow guidance, click links, or open attachments unless you recognise the sender and know the content is safe.

Good Morning s. 22(1)(a)(ii),

For the 2 Nov briefing, please find attached:

- My notes for item 3 (DSMA Briefing)
- Responses to AUS AGD questions (to be expanded upon during the meeting)
- Two examples of formal supplementary DSMA notices (for information)

Please feel free to distribute these documents to attendees ahead of the meeting.

Although the documents are unclassified, I would ask that the two supplementary notices are not distributed beyond the meeting attendees.

Kind Regards,
Geoffrey Dodds,

Brigadier (Retired) Geoffrey Dodds | Secretary | Defence and Security Media Advisory

Committee | 4.4.113 | Ministry of Defence Main Building | 2 Horse Guards Avenue |
Whitehall | LONDON SW1A 2HB | Office s. 47F(1) | Mobile s. 47F(1) .
| s. 47F(1)@dsma.uk | www.dsma.uk

DSMA Notice System Briefing

- The way in which the UK manages national security disclosures.
- Reconciles HMG's need to protect key Nat Sy info with the public's demands for a free media.
- The system is joint media/Gov, voluntary, non-statutory, senior. No sanctions. Assumes a positive buy-in from the UK media

DSMA Committee

- 5 HMG members (Chair, resources, sponsors)
- 17 Media members (Vice-Chair)
- Meets 2x pa & when required. Sets policy and issues guidance
- Delegates executive authority to Secretary every 6 months.
- Agrees the 5 standing notices which lie at the heart of the system.

Different Interpretations of the purpose of the system.

- Gov: To prevent the inadvertent publication or broadcast of information that could damage nat sy or increase the risk to people's lives.
- Media: To enable the media to publish/broadcast information it wants to - but without damaging national security.
- Imperfect system but valuable to both sides. 90% + success rate
- Alternatives?

Code of Confidentiality.

- Confidential comms media/DSMA secretariat. HMG & police agree/accept.
- Not subject to FOI acts.

Operation.

- Information widely available in the public domain (WAPD) - no DSMA action
- Often need to balance response time with security.
- HMG, Media and MOTP seek DSM advice. HMG currently in ascendancy.
- Staff, employed as civil servants, operate independently.
 - 1 Secretary FT, 2 Dep Secs (PT – one week per month), 1 Admin (PT)

Challenges.

- UK only system in a globalized information arena
- Tech Giants – when they strike a grand bargain with HMG.

Opportunities.

- Cyber recently incorporated into notices - 5 years!
- Counter Terrorism Police – work in progress (3 years to date)

Responses to AGD Questions – 2 Nov 22

In order presented

Advice To Journalists

Form of Advice:

- One to one/two: verbal, track changes, email (on separate, unclass IT).
- All editors: formal email (formal supplementary notice to all editors). But need to balance effect of supp notice with increasing media awareness.

Topics or Issues: Mainly: SPI, impending military action, methods & techniques. But depends on mil and security activity. Eg: Afghanistan – mil plans capabilities intentions

Public Interest. Of no concern when issuing advice. Focus is on the agreed text ion the standing notices.

Detail Provided by Agencies. Very little, if any. Occasional personal contact but 'need to know' limits detail.

Extension to Law Enforcement Activities. Historical, cultural media baggage.

- No Routine Policing
- NCA. Methods & techniques only.
- CTP. In progress

Consultation with Agencies

Direct Engagement with Government Agencies. Yes. In pri order, Js consult the IA/s directly, then or at the same time, DSMA.

Exceptions to permission to consult. Only in the most extreme circumstances.

- Credibility of Secretary and the system is at stake.
- Threshold is in the mind of the duty adviser.
- No governance documents exist.
- Snowden revelations example (2013). Media org did not seek DSM advice, IA too slow to involve DSMA.

How Often consult an IA. Almost every time but not always (IAs can prefer to avoid the attention that DSMA action could bring). Secretary offers advice using the agreed code. Need to balance IA consultation time with speed of response. Technical issues normally need consultation.

Instances of Js not giving permission to consult. No, never. Often ask/expect Secretary to consult. Caused by Js' need for accuracy? J's id always kept confidential.

Government Agency considering legal action. DSMA would not contribute to a Government agency considering legal action against a journalist.

Security Considerations.

Risk of J disclosing classified information (to DSMA?) during an inquiry. Risk exists but not in J's interest to do so? Have I misunderstood the question?

Conversations over unclass telecom eqpt. Yes – with both Government departments and the media. DSMA secretariat has

- OS phones for comms with OGDs.
- Civ mobile phones for comms with Js.
- Need to balance need for speed of response (if any) with security considerations.

Risk of Inaccurate advice to J. Risk exists. But J probably needs to backbrief editor that he/she has consulted DSMA and reassured 'no DSMA concerns'. So why deliberately mislead DSMA?

Requirement to report Leaks. No. DSMA does not get involved with leaks.

- It might get involved with the leaked information if it has not yet been published/broadcast. But if leaked and WAPD, no DSMA action.
- DSMA might report leaks inadvertently and unknowingly.

Issues Relating to Security Breaches. Leaks/inadvertent disclosure.

Information WAPD – no DSMA action.

Information not yet WAPD – almost certainly DSMA action.

DSMA consultation as a defence against prosecution.

No legal basis for this but:

1971. Ed D Telegraph accused of offence against OSA. Ed had consulted Sec/DSMA and was called as a defence witness. Judge noted that ed had taken appropriate steps to ensure he was not damaging nat sy. Was this the reason ed was acquitted?

Instances of Js publishing information against DSM advice.

Yes but very rarely. Tends to be extreme, non-msm organizations.

Eg: Declassified UK (online pub). Copy of ministerial brief inadvertently sent from MOD to ed in response to FOI request.

- In Feb, Ed published article incl SPI of a UKSF officer without seeking DSM advice. DSMA advised he remove SPI but he refused to do so (wasn't the main point of the article).
- In Aug, Ed published embarrassing details of HMG views on a developing country. No DSMA concern.

Eg: The Sun 2017? Details of planned UK training battalion deployment to Afghanistan. Relationship Ed/senior MOD official.

Process for Managing Approaches by Js seeking to reduce risk of prosecution.

None? Never happened?

Logistics and Operation

How Often? Peaks and troughs. System is reactive to domestic and international events. In last 10 years:

393 RFAs in 2011

106 RFAs in 2022

Process for Appointing Sec & deputies. Use MOD process (with media participation)
- all DSMA members are employed as civil servants.

- Chair (DG Sec Pol, MOD) and Vice-Chair (Media) jointly chair Secretary selection board.
- MoD member (D Nat Sy, MOD) and a senior media member jointly chair deputy secretary selection boards.

IT Systems.

In Office (MOD Main Building).

- Unclass Standalone (for comms with media, using DSMA O365 package)
- MODnet (Restricted). Mainly for admin
- MODnet (S). Rarely used. For sensitive MOD matters. Prefer to 'walk the corridor'.

WFH

Unclass laptop
MODnet iphone (OS)

Stored Information.

- Official Information (Registered). Emails, files
- DSMA Information (Unregistered). Sensitive secretariat/media comms info. Only accessed by secretariat members. No Government nor Police access.

Relationship DSMA System/Government Agencies.

- MOD: always very good – historical. 'D' since 1912.
- Relationship with agencies varies according to personalities involved and changing organizational policies. Can range from very good to poor.

Feedback from Agencies.

Rarely but during 2015 system review (post Snowden), all agencies went on the record as keen to maintain the system.



OFFICIAL:Sensitive

2 November 2022

Minutes

Briefing with UK Defence and Security Media Advisory (DSMA) System

With Brigadier Geoffrey Dodds, DSMA Secretary

Attendees

- Brigadier Geoffrey Dodds
DSMA Secretary
- s. 22(1)(a)(ii)
[Redacted]
- s. 22(1)(a)(ii)
Manager, Government and Executive Advice, Australian Federal Police (AFP)
- s. 22(1)(a)(ii)
Acting Coordinator, Legislative Reform, AFP
- s. 22(1)(a)(ii)
[Redacted]
- s. 22(1)(a)(ii)
[Redacted]
- Andrew Warnes
First Assistant Secretary, Criminal Justice Division, Attorney-General's Department (AGD)
- Susan McKeag
Assistant Secretary, Criminal Law Policy Branch, AGD
- s. 22(1)(a)(ii)
Director, Law Enforcement Powers Section, AGD
- s. 22(1)(a)(ii)
Assistant Director, Law Enforcement Powers Section, AGD
- s. 22(1)(a)(ii)
Policy Officer, Law Enforcement Powers Section, AGD
- s. 22(1)(a)(ii)
Policy Officer, Law Enforcement Powers Section, AGD

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL:Sensitive

Overview of briefing on DSMA System

Brigadier Dodds provided an overview of the DSMA system, including its history, purpose, structure and core functions.

The DSMA system is comprised of three elements:

- DSMA Notices
 - Guidance notices for media that describe agreed categories of information or topics which, if reported on, could harm the United Kingdom's (UK) national security and/or endanger lives.
- DSMA Committee
 - Board with joint membership from government agencies and the media industry to oversee the development of the DSMA Notices and operation of the DSMA system, including recommending improvements to the system as appropriate.
- DSMA Secretary
 - An eminent, non-Government person to provide media with expert, independent and confidential guidance on the potential impact certain stories or publications may have on national security. Brigadier Dodds has been the DSMA Secretary since November 2016.

Background and Purpose

- The DSMA system was established in 1912 and has served the UK well over the century that it has been in operation.
- The system serves as an agreement between the UK media and the UK Government, by reconciling the government's need to protect national security information with the media's need for freedom of information.
- The system has a different meaning for both government and media. It is the role of the DSMA Secretary to enmesh these two aims.
 - Government: to prevent the inadvertent disclosure and publication of national security information by the press.
 - Media: to ensure the media can publish what it wants without it affecting journalists/media organisations, or damaging national security.
- The system is voluntary and non-statutory, with the decision to publish resting with the news editor or publisher.
 - The Official Secrets Act remains a recourse of action for government if needed.
- The DSMA Secretary indicated that approximately 90% of the UK media view the DSMA System positively. Those in the media industry who are not supportive of the system are mostly the strongest proponents of media freedom.

DSMA Committee

- The Committee is comprised of five government and 17 media representatives. These representatives are senior officials or executives from their organisation or government department, which helps to facilitate widespread buy-in from both government and the media.
 - Each of the major broadcasting companies in the UK have a seat on the Committee.
 - Media companies select (a) member(s) to represent their industry. These associations include news media, periodical publishers and book publishers, among others.
 - Media members do not represent their specific broadcaster or publication on the Committee. Although they may be from a media organisation, the purpose of their being on the Committee is to represent the interests of free media as a whole. This is important because the media members may agree to something as part of the Committee but then have to sell the decision to the wider UK media.
- The Committee is chaired and resourced by government, meets formally twice annually, and holds additional meetings as required.
- The Committee delegates authority to the DSMA Secretary every six months to enact its policy.
- The main function of the DSMA Committee is to agree and approve the five standing notices.

Operation

- The DSMA Secretary provides advice and guidance to journalists within the framework of the five standing DSMA Notices. This may include verbal advice, written advice or suggested track changes on a document (e.g. draft article, book chapter). The DSMA Secretary's advice is focused on the agreed text in the standing DSMA Notices.
- The DSMA Secretary consults with agencies in almost every instance and there has never been a case where a journalist has refused to give permission for the DSMA Secretary to consult with an agency.
 - However, advice is often sought within very tight timeframes. Journalists are often under immense pressure to publish some information online immediately, especially during the daytime.
 - Journalists often expect the DSMA Secretary to consult with agencies, which Brigadier Dodds attributes to their need to publish accurate information, as the contrary would result in their journalistic reputation being significantly damaged.
- The number of enquiries that the DSMA System receives ebbs and flows, as the media is not always aware of national security activity taking place (e.g. during wartime).
 - Brigadier Dodds provided the following sample figures from different years:
 - 393 requests in 2011
 - 106 requests in 2022
- The main stakeholders in the system include the UK Government, public and media. Currently, government departments are seeking DSMA advice more frequently than the media.
- Conversations between the DSMA system and journalists/media organisations are confidential. The Secretary is not required to submit evidence from discussions with media as part of police

investigations or court proceedings, and the system is not subject to Freedom of Information (FOI) Act requests.

- The DSMA Secretary does not advise on information that is widely available in the public domain.
- Should the media publish information that may be harmful to national security, the Secretary can advise the journalist or media organisation to remove the article if it has been published online. However, there is no recourse if the information has been published in print media.

Challenges

- **Globalised media:** The DSMA system is a UK system operating in a globalised world. The prevalence of digital media means that UK information can be published in other countries, and there is no recourse for the DSMA to prevent this. However, in the main, overseas publication of UK national security information rarely happens.
- **Reluctance of digital industry:** Tech giants are resistant to communicating with the DSMA Secretary. Brigadier Dodds suspects that the reason for this is that tech giants are waiting to settle a bargain with government.
- **Difficult to keep pace and make updates to system:** The narrowness of the system means that it takes some time to update notices. Cyber has only recently been incorporated into the notices, and it took five years to accomplish it. Currently, the DSMA is trying to include counter-terrorism into the notices.

Logistics

- The DSMA Secretary has a separate, standalone computer in Ministry of Defence. The Secretary also has OFFICIAL:Sensitive phones and systems for communicating with government agencies and maintaining administrative records relating to the system and the DSMA Committee.
- If a sensitive conversation needs to occur, the DSMA Committee Secretary will generally go and speak to the relevant agency in person.

Questions and Answers

Advice to journalists

Under the UK DSMA system, are law enforcement agencies and transnational, serious and organised crime (TSOC) covered, or is there a focus only on military and national security agencies?

- Defence and national security (intelligence) agencies are the focus of the DSMA system, but there is a recognition that TSOC is related to national security, so TSOC and law enforcement are covered in some cases.
- The UK media sees policing as a civil operation unrelated to defence and security, so incorporating law enforcement activities and related crimes such as TSOC and counter-terrorism is a gradual process.

Does a journalist ever come to the DSMA Secretary seeking a different answer regarding publication than was provided by the agency that owns the information?

- Yes, a journalist might go to the agency in question regarding the article they wish to publish, either in parallel with or before seeking advice from the DSMA Secretary. However, Brigadier Dodds did not consider this to be an issue.
- The two types of advice may differ slightly. It may even be the case that something in the article contradicts the DSMA Notices but the media team in the agency in question may be relaxed about it. The DSMA Secretary can consult with the agency for background in this case.
- Brigadier Dodds noted that if a journalist chooses to seek advice in the first place, then it is most likely that their intention is to prevent harm and take on the best advice given to them. It is not in the journalist's interest to publish against the advice, as the system is only voluntary and does not grant the journalist immunity or protection if there is a breach of the Official Secrets Act.

If a government agency refuses to provide comment to a journalist, and the journalist then goes to the DSMA Secretary for comment, can the DSMA Secretary comment on the article or only provide technical advice?

- Yes, a journalist can go to an agency and receive 'no comment' then subsequently seek advice from the DSMA. In this case, the DSMA Secretary can contact the agency and ask for advice on what the concerns are. The agency may still provide no comment or it may provide background to assist the DSMA Secretary to interpret the standing DSMA Notice and provide advice to the journalist.

In how many instances has a journalist or media organisation not come to the DSMA for consultation before publishing, or published against DSMA advice?

- There are very few instances of this. Brigadier Dodds is aware of one article and two books in 2022 that have been published without DSMA consultation.
- Cases where information has been published against advice has generally come from fringe media organisations which are not part of the mainstream media.

Consultation with agencies

What is the relationship between the DSMA and government agencies like? Do agencies have views on the system and role of the DSMA Secretary?

- Agency views on the DSMA system vary from very good to poor. For the most part, this depends on individual personalities and changing policies around disclosures that new agency directors may bring in. In the last review of the DSMA system in 2015, all agencies came out in support of the system.
- The DSMA system has very deep roots in the Ministry of Defence, so the Ministry of Defence press office sees the DSMA Secretary as a 'brother-in-arms'.

Does the DSMA Secretary have to tell the journalist before contacting the government agency concerned?

- Yes, permission must be sought from the journalist/media organisation before consulting the government agency.
- Permission is reliably granted by the media – no journalist has ever refused permission for the DSMA Secretary to consult with the agency.

- Brigadier Dodds suspects this is related to the fact that journalists do not want to be caught out publishing inaccurate material.

How does the DSMA Secretary contact a government agency, taking into consideration the confidentiality that exists between the Secretary and the media organisation/journalist?

- Permission must be sought from the journalist/media organisation first to consult the agency.
- The DSMA Secretary has an unclassified email and phone line for communications with the media, and a Ministry of Defence phone, which is used to contact government agencies. If there is something particularly sensitive to discuss, the DSMA Secretary and the government agency will meet in person.

At what point would the DSMA Secretary consult a government agency without first asking permission from the journalist or media organisation, for example because the risk is so high (e.g. likely to cause loss of life or significant damage to national security)?

- This has never happened, but in such a situation it would be at the discretion of the Secretary.
- Such a decision must balance the Secretary's and the system's credibility and the breach of journalist confidentiality with the risk of exposure.

Do government agencies ever pre-brief the DSMA Secretary on operational activity that they know or suspect may become public?

- Generally, no. Brigadier Dodds estimates that agencies suffer by not doing so. Agencies run a risk by not engaging with the DSMA early, as it can become too late for the DSMA Secretary to prevent any harm.

Security considerations

How have journalists generally obtained the information brought to the DSMA for consultation?

- Usually, information in the possession of journalists is the result of their own investigation. However, an investigation is likely to have been prompted by something, for example a tip-off or leak from a government agency.
- Usually, a journalist will seek legal advice from their own in-house legal team before consulting with the DSMA Secretary.

Is there ever a risk that the DSMA Secretary could breach the Official Secrets Act?

- Brigadier Dodds has never had concerns that he would breach the Official Secrets Act.
- Advice provided to the journalist/media organisation is based on the five standing notices which have been jointly agreed by government and media representatives, and the notices are written in general terms.
- If there is sensitive information to be discussed, the Secretary would meet with the agency who owns the information.

Logistics and operation

What is the appointment process and term of tenure for the DSMA Secretary role?

- The DSMA Secretary is employed by government as a civil servant, but does not work ‘for government’, as the role requires impartiality from government. The DSMA Secretary is hired on a permanent contract but is granted authority by the DSMA Committee every six months.
- The Secretary and the two Deputy Secretaries are chosen by the DSMA Committee and there must be joint media–government agreement before hiring either role.

If the DSMA Secretary provides incorrect advice, the Secretary be fired from their role?

- As a government employee, the Secretary would have to break a government rule, and would likely be let go by the Ministry of Defence.

How does the DSMA avoid civil and/or legal liability? Are there any statutory or legislative protections in place?

- There are no protections in place to cover the DSMA or Secretary when incorrect advice is given.

From: Warnes, Andrew
To: s. 22(1)(a)(ii)@defence.gov.au; s. 22(1)(a)(ii)@defence.gov.au; s. 22(1)(a)(ii)@defence.gov.au;
s. 22(1)(a)(ii)@homeaffairs.gov.au; s. 22(1)(a)(ii)@dfat.gov.au;
s. 22(1)(a)(ii)@dfat.gov.au; s. 22(1)(a)(ii)@afp.gov.au;
s. 22(1)(a)(ii)@agd.gov.au;
Cc: s. 22(1)(a)(ii); McKeag, Susan; s. 22(1)(a)(ii); s. 22(1)(a)(ii)
Subject: Meeting summary - briefing with UK DSMA Secretary [SEC=OFFICIAL:Sensitive]
Date: Monday, 7 November 2022 5:58:09 PM
Attachments: Minutes from Briefing with UK DSMA Secretary.DOCX
Responses to AUS AGD.docx
DSMA Notice System Briefing.docx
s. 33(a)(iii)
image001.png

OFFICIAL: Sensitive

Good afternoon colleagues,

Thank you to those who attended the briefing with Brigadier Geoffrey Dodds on the UK's DSMA system on Wednesday evening. We at AGD found it to be a highly useful session and hope that you also found it informative.

Please find attached the following documents for your reference:

- Minutes from the meeting
- Brig Dodds' responses to questions submitted in advance of the meeting
- Brig Dodds' briefing notes on the DSMA system
- Two examples from Brig Dodds of formal supplementary DSMA notices issued to media organisations.

Please note that although the supplementary documents are unclassified, **we would be grateful if you did not distribute these documents further.**

If you have any questions, please feel free to contact me or s. 22(1)(a)(ii)@ag.gov.au, A/g Director, Law Enforcement Powers Section.

Kind regards
Andrew

OFFICIAL: Sensitive

Andrew Warnes | First Assistant Secretary
Criminal Justice Division
Attorney-General's Department
Tel s. 22(1)(a)(ii) s. 22(1)(a)(ii)@ag.gov.au

2586 Indigenous signature block NEW5 (2)



From: s. 22(1)(a)(iii)
To: s. 22(1)(a)(ii); s. 22(1)(a)(ii); s. 22(1)(a)(ii); s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @defence.gov.au"; s. 22(1)(a)(ii); s. 22(1)(a)(ii)
s. 22(1)(a)(ii); s. 22(1)(a)(ii) "DFAT"; s. 22(1)(a)(ii); s. 22(1)(a)(ii)
Cc: s. 22(1)(a)(iii); s. 22(1)(a)(ii)
Subject: Meeting summary - Press Freedom - Briefing with UK DSMA Secretary [SEC=OFFICIAL:Sensitive]
Date: Tuesday, 8 November 2022 9:28:00 AM
Attachments: [Minutes from Briefing with UK DSMA Secretary.DOCX](#)
[Responses to AUS AGD.docx](#)
[DSMA Notice System Briefing.docx](#)
s. 33(a)(iii)
[image001.png](#)
[image002.jpg](#)
[image003.png](#)

OFFICIAL: Sensitive

Good morning all,

For your awareness, please see below an email from our FAS Andrew Warnes to his counterparts following the briefing with Brigadier Geoffrey Dodds on the UK's Defence and Security Media Advisory (DSMA) system last week.

I would like to draw your attention to the attached documents which include the Minutes from the briefing, as well as some supplementary documents provided by Brig Dodds. While the supplementary documents are unclassified, grateful if you please did not distribute them further.

If you have any questions or would like to discuss, please don't hesitate to give me a call.

Kind regards,

s. 22(1)(a)(iii)

s. 22(1)(a)(ii)

A/g Director, Law Enforcement Powers Section
Criminal Law Policy Branch | Criminal Justice Division
National Security and Criminal Justice Policy Group
Attorney-General's Department

T: s. 22(1)(a)(ii) | E: s. 22(1)(a)(ii) @ag.gov.au

AGD Logo



From: [Warnes, Andrew](#)
To: s. 22(1)(a)(ii)
Cc: s. 22(1)(a)(ii) [McKeag, Susan](#); s. 22(1)(a)(ii); s. 22(1)(a)(ii); s. 22(1)(a)(ii); s. 22(1)(a)(ii); s. 22(1)(a)(ii)
Subject: RE: Meeting summary - briefing with UK DSMA Secretary [SEC=OFFICIAL:Sensitive]
Date: Thursday, 1 December 2022 11:58:18 AM
Attachments: [image002.png](#)
[image003.png](#)

OFFICIAL: Sensitive

Thanks s. 22(1)(a)(ii) s. 47C(1)

s. 47C(1)

s. 47C(1)

Cheers

Andrew

Andrew Warnes | First Assistant Secretary
Criminal Justice Division
Attorney-General's Department
Te s. 22(1)(a)(ii) s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au)

2586 Indigenous signature block NEW4 (2)



OFFICIAL: Sensitive

From: s. 22(1)(a)(ii) [@afp.gov.au](mailto:s.22(1)(a)(ii)@afp.gov.au)
Sent: Wednesday, 30 November 2022 4:25 PM
To: Warnes, Andrew s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au)
Cc: s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au); McKeag, Susan s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au); s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au); s. 22(1)(a)(ii) [@ag.gov.au](mailto:s.22(1)(a)(ii)@ag.gov.au); s. 22(1)(a)(ii) [@afp.gov.au](mailto:s.22(1)(a)(ii)@afp.gov.au); s. 22(1)(a)(ii) [@afp.gov.au](mailto:s.22(1)(a)(ii)@afp.gov.au); s. 22(1)(a)(ii) [@afp.gov.au](mailto:s.22(1)(a)(ii)@afp.gov.au)
Subject: RE: Meeting summary - briefing with UK DSMA Secretary [SEC=OFFICIAL:Sensitive]

CAUTION: This email originated from outside of the organisation. Do not follow guidance, click links, or open attachments unless you recognise the sender and know the content is safe.

Good afternoon Andrew and colleagues,

Thanks again for organising the briefing with Brigadier Geoffrey Dodds, DSMA Secretary. It was very useful to hear firsthand how the UK system operates and how it may be applied to Australia.

While the Brigadier was quite positive in his estimation of the system and how it could be applied to law enforcement matters, he did note that the UK media did not agree with law enforcement being included under the UK DSMA system. s. 47C(1)

s. 47C(1)

We also note that much of the UK system's efficacy is because of the relationship with media that has been built over decades.

s. 47C(1)

s. 47C(1)

Regards, s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

Writing to you from Ngunnawal Country
MANAGER GOVERNMENT AND EXECUTIVE ADVICE
STRATEGY & PERFORMANCE OFFICE

AUSTRALIAN FEDERAL POLICE

Tel: s. 22(1)(a)(ii) Ext: s. 22(1)(a)(ii) Mob: s. 22(1)(a)(ii)

www.afp.gov.au

AFP Acknowledgement

The Australian Federal Police acknowledges the traditional owners and custodians of country throughout Australia and their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.