

From: s. 22(1)(a)(ii)
To: s. 22(1)(a)(ii)
Cc: s. 22(1)(a)(ii)
Subject: FW: Starlink - request for high level information [SEC=OFFICIAL:Sensitive]
Date: Thursday, 15 May 2025 7:51:00 AM
Attachments: [image001.jpg](#)
[image002.png](#)
s. 33(a)(i), s. 47C(1)
Importance: High

OFFICIAL: Sensitive

Morning s. 22(1)(a)(i),

s. 22(1)(a)(i) and s. 22(1)(a)(i) edited the doc s. 22(1)(a)(ii) sent through yesterday a bit more, could you pls read through the attached this morning, and let me know if you have any additional thoughts to help with s. 22(1)(a)(ii) question:

s. 33(a)(i)

s. 33(a)(i)

They're hoping to get the next draft to s. 22(1)(a)(i) this arvo, so if you could pls put something together for me to review by lunch, that'd be amazing ☺

Happy to chat!

Cheers,

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

Assistant Director | Telecommunications Security Risk

Risk Assessment Branch

Cyber & Infrastructure Security Centre | Department of Home Affairs

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

OFFICIAL: Sensitive

From: s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>
Sent: Wednesday, 14 May 2025 4:43 PM
To: s. 22(1)(a)(ii) @homeaffairs.gov.au>; s. 22(1)(a)(ii)
s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>

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

Cc: s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>
Subject: FW: Starlink - request for high level information [SEC=OFFICIAL:Sensitive]

OFFICIAL: Sensitive

Hi team,

Following s. 22(1)(a)(ii) input, s. 22(1)(a)(ii) and I have updated the existing document to be more prescriptive regarding the s. 33(a)(i)

By no means finalised. The team will work on polishing the product off tomorrow (and potentially sending to DITRDCA for review if time allows).

s. 22(1)(a)(ii) feel free to provide input into the attached document as opposed to the former document ☺

Kind regards,

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

s. 22(1)(a)(ii) (he/him)
Telecommunications Security Risk
Risk Assessment Branch | Cyber & Infrastructure Security Centre
Department of Home Affairs
P: s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @homeaffairs.gov.au

Acknowledgement of Country Signature Block Graphic 2022 (1)



OFFICIAL: Sensitive

From: s. 22(1)(a)(ii) @homeaffairs.gov.au>
Sent: Wednesday, 14 May 2025 11:19 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) s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>; s. 22(1)(a)(ii) s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>
Subject: RE: Starlink - request for high level information [SEC=OFFICIAL]

OFFICIAL

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

I've had another look in detail, and I think we are close but we need to expand a bit further on what the framework in the Tel Act actually sets out for C/CSPs and what that means in practice for Starlink (noting DITRDCA leads on the Tel Act, we may need to get that info from them).

s. 33(a)(i)

If we need to engage CI Policy colleagues for assistance, we can do that too.

Could I have those updates by COB Thursday please? And also, could I please have a copy of the DITRDCA paper?

Thanks,

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

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

Director | Telecommunications Security Risk

Risk Assessment Branch | Cyber & Infrastructure Security Centre

Cyber & Infrastructure Security Group

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)

OFFICIAL

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



Australian Government
Department of Home Affairs



CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

OFFICIAL

Document 12
Page 1 of 8

Low Earth Orbit Satellite Communications – security considerations

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

Director
Telecommunications Security Risk
Cyber and Infrastructure Security Group

22 May 2025

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





- *Security of Critical Infrastructure Act 2018* – Administered by Dept of Home Affairs
 - Sets out obligations for critical infrastructure owners/operators/assets
- *Telecommunications Act 1997* – Administered by Dept of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)
 - Sets out obligations for telecommunications carriers and carriage service providers (CSPs)
- Starlink Australia Pty Ltd is a licenced telecommunications carrier, and a critical asset



- Any Low Earth Orbit Satellite (LEOSat) provider who offers public telecommunications services in Australia is considered in the same manner as other telecommunication providers under the Tel Act.
- Starlink Australia Pty Ltd (Starlink) is a licenced carrier under the Telecommunications Act 1997 (Tel Act).
- The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) has principal authority for the licencing of carriers.



Starlink's obligations under the Tel Act:

- Carriers and CSPs, including Starlink, may be subject to over 30 categories of obligations. Carrier and CSP obligations can be classified into four broad groups:
 - Competition;
 - Consumer Protection;
 - Telecommunications-specific levies; and
 - National Interest.



Starlink's obligations under the SOCI Act:

- Protect their asset 'so far as reasonably practicable to do so' from all-hazard security risks where there is a material risk that the occurrence of the hazard could impact their asset; and
- Notify the Home Affairs Secretary of changes and/or proposed changes to its telecommunications services or systems that are likely to have a material adverse effect on their capacity to meet their obligation to protect the asset.



Telecommunications Security Risk Management Program rules:

- Reporting ownership and operational information to the Register of Critical Infrastructure Assets;
- Implementing, maintaining and complying with a Risk Management Program to identify and mitigate against all-hazards to their critical telecommunication asset. This includes cyber, physical, supply chain and personnel risks;
- Mandatory reporting of cyber security incidents to the Australian Cyber Security Centre; and
- Complying with government assistance, directions and information gathering requests.



Nature and risk profile of LEOsSat providers

- Starlink plays an important role, along with other market players such as NBN Co. and AWS in providing satellite-based internet services in Australia, particularly in regional and remote areas.
- Availability risks due to the offshore nature of Starlink.
- DITRDCA notes there are a number of state and territory based departments who also use Starlink in remote areas of Australia.



Australian Government
Department of Home Affairs



CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

OFFICIAL

Document 12
Page 8 of 8

Discussion



****OFFICIAL****

MEDIA ENQUIRY

Subject: Australian telecommunications sector possible reliance on Starlink		
Deadline: 12.00pm, 31/10/2024		
Journalist: s. 47F(1)		Outlet: s. 47F(1)
Phone:	Mobile: s. 47F(1)	Email: s. 47F(1)
Enquiry Received (Time & Date): 10.44am, 30/10/2024		
Media Officer:		Media Ph:

QUESTION / ISSUE

Journalist asked:

The story is about the extent to which Australia's telecoms network – from civilian to emergency services – relies on Starlink and whether this reliance presents a vulnerability.

It's a written story for the s. 47F(1) website.

Questions:

- Starlink's fast, low-latency satellite internet service has proved useful and popular in Australia. State and federal governments have spent over \$50 million on contracts for Starlink internet services / hardware over the last three years, via registered Starlink resellers. More than 200,000 Australians now rely on Starlink for basic internet. Some national security experts are concerned this reliance could pose a threat to national security, since it gives a privately owned foreign company great leverage. Is the Department at all concerned about this reliance on Starlink posing a threat to national security?*
- What has the Department done to mitigate this potential threat?*

Happy to clarify anything over the phone or email.

OFFICIAL

RESPONSE OFFICIAL

Attributable to a Departmental spokesperson:

- The Australian Government is committed to protecting Australia's critical infrastructure to secure the essential services all Australians rely on.
- The Department of Home Affairs (the Department) recognises the critical importance of secure and resilient telecommunications infrastructure and services to Australia's national security.
- The Department actively assists Australian critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations for the shared benefit of all Australians. This includes conducting security regulation of Australia's communications sector.
- The Department acknowledges Starlink's role, along with other market players such as NBN Co. and Amazon Web Services in providing satellite-based internet services, particularly in regional and remote areas.
- The Department continually assesses the potential national security risks posed by potential disruptions to critical services and reliance on particular providers and ensures that frameworks are in place to manage these risks.
- To support regulated entities, to mitigate potential security risks, and to assist in shaping a more resilient communications sector, the Department administers the Telecommunications Sector Security Reforms (TSSR) framework, which imposes strict security obligations on telecommunications providers, including satellite-based internet service providers.
 - o Starlink Australia is a regulated entity under this framework, as a licenced telecommunications carrier.
- Throughout 2024, in partnership with industry, the Department has co-designed a package of legislative reform to the *Security of Critical Infrastructure Act 2018* to further strengthen and enhance the security framework for the communications sector.
 - o These reforms will include a Risk Management Program obligation for telecommunications providers, further strengthening security and resilience in the sector.
 - o These measures have been introduced to Parliament under the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill*.
- Questions related to market share or commercial arrangements should be directed to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA).

s. 47E(d)

OFFICIAL

s. 47E(d)

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

CLEARANCE

All clearances below must be completed before being returned to Media Operations.

Lead business area

The Media team will contact the area(s) should further clarification be required.

Telecommunications Security Risk Section, Risk Assessment Branch

OFFICIAL

OFFICIAL

Drafting officer		
s. 22(1)(a)(ii)	A/g Assistant Director, Telecommunications Security Risk	Date (31/10/2024)

International Division clearance	
	Yes ☐ N/A ☒

Other Government agency consultation/clearance		Yes ☐ N/A ☐
Agency	Branch/area	Date (DD/MM/YYYY)
Agency	Branch/area	Date (DD/MM/YYYY)

Final SES clearance (minimum SES Band 1) and approval for release		
SES of lead business area must verify that all appropriate consultation and clearances have been undertaken.		
Hamish Hansford	Deputy Secretary, Cyber and Infrastructure Security	Date (31/10/2024)

Media and Communication Branch		
s. 22(1)(a)(ii)	Director, National Security and Crisis Communications, Media and Communication Branch	Date (DD/MM/YYYY)

Review / Consultation		
s. 22(1)(a)(ii)	Critical Infrastructure Security Policy Branch	Date (31/10/2024)

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

OFFICIAL

From: s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>
Sent: Thursday, 31 October 2024 9:18 AM
To: s. 22(1)(a)(ii) @HOMEAFFAIRS.GOV.AU>
Cc: Telco security s. 22(1)(a)(ii) @homeaffairs.gov.au>
Subject: RE: media request - S. 47F(1) - Starlink [SEC=OFFICIAL]

OFFICIAL

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

Thanks for sending this through, it is incredibly thorough. I've slightly updated the wording (in track form) to make our points a little more specific in some areas, and broader in others. I also don't think we need to write our points out as an email to the s. 47F(1) as I think Media takes care of that? Although I could be wrong, so let me know if I am ☺

Feel free to consider as you wish, and flick off to s. 22(1)(a)(ii)

Happy to discuss.

Kind regards,

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

Telecommunications Security Risk Points:

s. 47C(1)

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

S. 47C(1)

OFFICIAL

From: S. 22(1)(a)(ii) <[REDACTED]@HOMEAFFAIRS.GOV.AU>
Sent: Thursday, 31 October 2024 8:14 AM
To: S. 22(1)(a)(ii) <[REDACTED]@HOMEAFFAIRS.GOV.AU>
Cc: S. 22(1)(a)(ii) <[REDACTED]@homeaffairs.gov.au>
Subject: RE: media request - S. 47F(1) - Starlink [SEC=OFFICIAL]

OFFICIAL

Hi [REDACTED]

Please find below a draft response to the questions outlined by S. 47F(1) from S. 47F(1).

Happy to make any amendments to add/delete sections, and for any further input you may have regarding the recent changes within the SOCI reforms that could be potentially included to strengthen these points.

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

Hi s. 47F(1)

Thank you for reaching out to the Department for comment on this matter.

S. 47C(1)

Kind regards,

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

Policy Officer | Telecommunications Security Risk Section
Risk Assessment Branch | Security Regulation Division
Cyber and Infrastructure Security Centre
Department of Home Affairs
E: s. 22(1)(a)(ii) @homeaffairs.gov.au



[CISC.gov.au](https://cisc.gov.au) | [Twitter](#) | [LinkedIn](#)

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

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

OFFICIAL

From: S. 47F(1)
Sent: Wednesday, 30 October 2024 10:44 AM
To: Home Affairs Media <media@homeaffairs.gov.au>
Subject: media request - S. 47F(1) - Starlink

Hi there,

S. 47F(1) from S. 47F(1) here. I'm seeking written comment by midday AEDT Thursday.

The story is about the extent to which Australia's telecoms network – from civilian to emergency services – relies on Starlink and whether this reliance presents a vulnerability.

It's a written story for the S. 47F(1) website.

Questions:

1. Starlink's fast, low-latency satellite internet service has proved useful and popular in Australia. State and federal governments have spent over \$50 million on contracts for Starlink internet services / hardware over the last three years, via registered Starlink resellers. More than 200,000 Australians now rely on Starlink for basic internet. Some national security experts are concerned this reliance could pose a threat to national security, since it gives a privately owned foreign company great leverage. Is the Department at all concerned about this reliance on Starlink posing a threat to national security?
2. What has the Department done to mitigate this potential threat?

Happy to clarify anything over the phone or email.

Kind Regards,

s. 47F(1)

s. 47F(1)

Technology reporter

s. 47F(1)

M: s. 47F(1)

Please consider the environment before printing this e-mail.

The information contained in this email and any attachment is confidential and may contain legally privileged or copyright material. It is intended only for the use of the addressee(s). If you are not the intended recipient of this email, you are not permitted to disseminate, distribute or copy this email or any attachments. If you have received this message in error, please notify the sender immediately and delete this email from your system. The s. 47F(1) does not represent or warrant that this transmission is secure or virus free. Before opening any attachment you should check for viruses. The s. 47F(1) liability is limited to resupplying any email and attachments.

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