SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

QoN	Senator	Broad topic	Hansard Page	Hansard Reference
1	Kitching	Slack	94-95	**Senator KITCHING:** I'm just looking up Slack in Wikipedia. It doesn't say that it's encrypted. Certainly if you go to their platform—which I'm not sure I'll be able to download, because this is a DPS machine and I don't think they let us download it, otherwise there would be many random applications on these computers—I think you just put in your work email and it says to try it for free. Are you able to take it on notice and see if— **Ms Noble:** I certainly can get you more details on how it works. **Senator KITCHING:** If the Slack channel is not encrypted, have any of the threats of compromise or the indicators of compromise been shared on that channel? **Ms Noble:** Yes, they would have been—they have been. **Senator KITCHING:** If it's not encrypted, is that problematic? **Ms Noble:** I think my colleague was just describing to me that there is a level of protection by Slack, but I would like to get you the exact detail on notice.
2	Kitching	Online Advice	95	**Senator KITCHING:** Thank you. Your cyber.gov.au website also says that you can share cyber threats through the news pages. I think those headings are for news, latest advice and latest threat advice. There have been two reports of latest advice since August 2018—is that correct? **Ms Noble:** I'm not sure; I'd have to check the website myself. **Senator KITCHING:** I might put some questions on notice about that. **Ms Noble:** Sure.
3	Kitching	2018 ANU Spear Phishing Attack		In November 2018, a sophisticated actor gained unauthorised access to the Australian National University (ANU) network through a spear phishing attack which resulted in the actor dwelling on the ANU network, accessing information from the human resources, financial management and student administration systems for approximately 6 weeks. (a) Prior to the data breach, was ANU or any other university in Australia warned by the ASD of the cyber threat? (b) Prior to the November 2018 ANU data breach, did the ASD brief ANU or any other university in Australia? If yes, how many times? (c) Prior to the November 2018 ANU data breach, did the ASD send ANU or any other university written communications warning ANU of this cyber threat? (d) Prior to the November 2018 ANU data breach, did ASD provide threat warning to ANU or any other university through an online sharing portal? (e) Did ASD provide any cyber security guidance to ANU prior to the November 2018 data breach? (f) Since the November 2018 data breach, what guidance has ASD provided to ANU to prevent future data breaches and mitigate against other cyber threats? (g) Since the November 2018 data breach, have there been any independent assessments of the cyber resilience

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				of Australian universities? (h) In a media release from Minister Tehan on 7 August 2019, the Minister announced that "the vice-chancellors of Australia's universities will receive a high-level cyber security briefing from the Australian Government's lead agency on cyber security. Minister for Education Dan Tehan has invited an expert from the Australian Signals Directorate (ASD) to update universities on the latest cyber security risks and to provide advice on strengthening their cyber security." Apart from the advice provided to the vice chancellors, have ASD sprint teams been deployed to any universities to give proactive assistance in securing research and student data in Australian universities after the November 2019 data breach? (i) Will ASD be following up with the Vice Chancellors to see if its advice and guidance is implemented by Australian universities?
4	Kitching	Fraud Attacks - rogue mobile applications		The latest RSA Quarterly Fraud Report (Q2 2019) highlighted that fraud attacks from rogue mobile applications increased 300 percent in the quarter. (a) What actions is the ACSC taking to action this threat intelligence for Australian businesses? (b) What actions is the ACSC taking to action this threat intelligence for Australian small businesses? (c) What actions is the ACSC taking to action this threat intelligence for Australian consumers?
5	Kitching	Fraud Attacks – financial malware		The latest RSA Quarterly Fraud Report (Q2 2019) highlighted that fraud attacks introducing financial malware increased 56 percent in the quarter. (a) What actions is the ACSC taking to action this threat intelligence for Australian businesses? (b) What actions is the ACSC taking to action this threat intelligence for Australian small businesses? (c) What actions is the ACSC taking to action this threat intelligence for Australian consumers?
6	Kitching	Malicious code identification		In the last year, the UK's NCSC used automated scanning to identify '*over 1,200 sites which were serving malicious code to illicitly copy credit card transactions*' and helped those small businesses to address these issues to 'protect their customers and their reputation'. Has the ACSC undertaken similar proactive initiatives to assist Australian small businesses address malware infections that jeopardise their customers?
7	Kitching	UK Information sharing		In a speech at CYBERUK 2019, the Director of GCHQ, Jeremy Fleming stated that: *"knowledge sharing must go two ways. A fundamental principle of the NCSC has always been to be more open, more transparent with the information we obtain. We're already doing that and are committed to share even more in real time, to help business and Government defend themselves and the UK.* *So specifically, in the last year we have made it simple for our analysts to share time- critical, secret information in a matter of seconds. With just one click, this information is being shared and action is being taken. In the coming year, we will continue to scale this capability so - whether it's indicators of a nation state cyber actor, details of malware used by cyber criminals or credit cards being sold on the Dark Web - we will declassify this information and get it back to those who can act on it."* (a) Is sharing more cyber threat intelligence information with Australian business in real time a priority for

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				government? (b) If so, what practical steps has the government taken to enable this in the last year? (c) What practical steps is the government planning to enable this in the next year? (d) Is sharing time critical, secret information with Australian business a priority for government? If so, what steps are being taken to enable this?
8	Kitching	UK Cyber Security Information Sharing Partnership		The UK NCSC has established the Cyber Security Information Sharing Partnership (CiSP*), "a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business."* The CiSP offers members *"engagement with industry and government counterparts in a secure environment, early warning of cyber threats, the ability to learn from experiences, mistakes, successes of other users and seek advice an improved ability to protect their company network and access to free network monitoring reports tailored to your organisations' requirements".* Why does the ACSC not offer a similar platform to Australian businesses and organisations?
9	Kitching	Unencrypted Government Websites		One of Australia's most visited government websites the Bureau of Meteorology, which receives approximately 3.5 billion page views each year, is still using unencrypted web connections more than a year after Google began labelling them insecure because they do not "protect the integrity and confidentiality of data". According to the Why No HTTPS? website, at least 12 other agencies, including the Department of Defence, Department of Health, Australian Bureau of Statistics, Environment and Energy, Department of Agriculture, Geoscience Australia, Clean Energy Regulator, National Archives of Australia, Australian Institute of Criminology, Inspector-General of Taxation, Taxation Ombudsman and the Commonwealth Ombudsman are also using unencrypted web connections. (a) In ASD's view, is it appropriate for government websites to be on unencrypted connections? (b) Does training the public to ignore insecure warnings while using government websites undermine the government's efforts to ensure a healthy cyber security ecosystem? (c) According to the Why No HTTPS? website, at least 12 other agencies, including the Department of Defence, Department of Health, Australian Bureau of Statistics, Environment and Energy, Department of Agriculture, Geoscience Australia, Clean Energy Regulator, National Archives of Australia, Australian Institute of Criminology, Inspector-General of Taxation, Taxation Ombudsman and the Commonwealth Ombudsman are also using unencrypted web connections. Have all of the listed Departments committed to timelines for ensuring their websites are using encrypted web connections? Has ASD discussed this issue with any of these agencies? If yes, which agencies has ASD had discussions with and what have been the outcomes for each agency? If no, why not? (d) Has the Government set a target date for when all government websites will be on encrypted web connections? (e) If the Government has set a target date for when all government websites will be on encrypted web connections, what is the target date?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

10	Kitching	Information Sharing		The ACSC's remit is to provide 'advice and information…to help protect Australians'. (a) What is the ACSC's primary channel for sharing cyber threat intelligence to businesses? (b) What is the ACSC's primary channel for sharing cyber threat intelligence to small businesses? (c) What is the ACSC's primary channel for sharing cyber threat intelligence to individuals?
11	Kitching	Slack		In response to a question from Senator Kitching at the Foreign Affairs, Defence and Trade Senate Estimates hearings on 23 October 2019, the Head of the ACSC, Ms Rachel Noble said that one of the interim public-private communications platform it uses to share cyber threats is a Slack channel. (a) Was this a reference to the slack workspace/channels used by the JCSCs to collaborate with its members? (b) How many slack channels does the government use to share threat intel? (c) Ms Noble told Senator Kitching at the Senate estimates hearing on 23 October 2019 that she did not know whether Slack was encrypted. Is Slack an encrypted communications platform? (d) How much does the Slack channel cost ACSC? (e) Is it true that the JCSCs currently use a 'free' version of the Slack platform? (f) Does the JCSCs use of a free slack plan mean that only the last 10,000 messages on these channels can be searched by members? (g) Has the Government undertaken any analysis of the security of sharing threat intelligence including indicators of compromise via Slack? (h) Does the security of Slack impede commonwealth entities from sharing threat intelligence on the platform? (i) What is the average number of interactions from ACSC staff per day on these Slack channels? (j) Has the Government undertaken any analysis of the security of sharing threat intelligence via Slack? (k) Does the security of Slack impede Commonwealth entities from sharing threat intelligence on the platform? (l) What is the average number of interactions per day on Slack? (m) On the Slack channel, on average, how many of the interactions come from ASD/ACSC? (n) On the Slack channel, on average, how many of these interactions come from the federal government? (o) In the view of ASD, is the current level of Commonwealth engagement in this Slack channel optimal? (p) Does the current level of Commonwealth engagement on Slack adequately meet the ACSC's obligation to provide 'advice and information…to help protect Australians'?
12	Kitching	Online Information Sharing Portal		Appendix A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that "ASD continues to develop co-designed online information sharing portals within the cyber.gov.au platform." (a) Has ASD completed any co-designed online information sharing portals? If yes: i. Who was consulted in the design of this portal? ii. What feedback was given to ASD by those consulted about industry needs? iii. How many users registered to the portal? iv. How many messages are posted per day on this portal?

				v. Can the portal share classified information? vi. How much does the platform cost? vii. Has the government undertaken any analysis of the security of sharing threat intelligence via this portal? viii. Has ASD commenced the co-design of any information sharing portals but has not yet completed? (b) Has ASD commenced co-designing portal(s) but not yet completed? i. When did the co-design process start? ii. When will this co-design process be concluded? iii. Who was consulted in the design of this incomplete portal?
13	Kitching	Online Advice		In response to a question from Senator Kitching at Foreign Affairs, Defence and Trade Senate Estimates hearings, the Head of the ACSC, Ms Rachel Noble said that another cyber threat sharing platform is the cyber.gov.au website. (a) Is Commonwealth cyber threat intelligence shared with Australians through the "News", "Latest Advice" or "Latest Threat Advice" pages on the ACSC website cyber.gov.au? (b) What is the average number of visitors per day to the cyber.gov.au/news webpage over the past 12 months? (c) What is the average number of visitors per day to the https://www.cyber.gov.au/threats webpage over the past 12 months? (d) Why was there no "Latest Threat Advice" posted on https://www.cyber.gov.au/threats on during an 11-month period between 15 August 2018 and 29 July 2019? (e) Seven "Latest Threat Advice" posted on https://www.cyber.gov.au/threats at 12 October 2018, 21 December 2018, 29 January 2019, 16 May 2019, 6 June 2019, 3 July 2019, 24 July 2019 appear to have been added after 30 July 2019. The Wayback Machine archived "Latest Threat Advice" site on 10 June 2019, shows that the 12 October 2018, 21 December 2018, 29 January 2019, 16 May 2019 and 6 June 2019 posts do not appear on the archived page. Did ACSC backdate these seven threat advices? If not, on what date was each of these advices posted and why have they not been captured by the Wayback Machine archive of the site on 10 June 2019. (f) What is the average number of visitors per day to the ACSC's https://www.cyber.gov.au/advice webpage over the past 12 months? (g) Why were there only two reports of "Latest Advice" on https://www.cyber.gov.au/advice webpage since August 2018?
14	Kitching	Stay Smart Online Website		The ACSC also runs the "Stay Smart Online" website, which provides general cyber security advice to the public. (a) What is the average number of visitors per day to Stay Smart Online webpage over the past 12 months? (b) On average, how many alerts does the Stay Smart Online website issue per month? (c) How does the number of alerts issued by Stay Smart Online website compare with equivalent public awareness pages in the United Kingdom and the United States?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

15	Kitching	Establishment of Joint Cyber Security Centres		Appendix A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that ASD has established Joint Cyber Security Centres (JCSCs) Sydney, Melbourne, Adelaide, Perth and Brisbane. (a) How many individuals have signed the ACSC deed for each centre? (b) How many ASX 200 firms have signed the ACSC deed for each centre? (c) How many SMEs have signed the ACSC deed for each centre? (d) How many local government or local government representative organisations have signed the ACSC deed for each centre? (e) How many state or territory government departments or entities have signed the ACSC deed for each centre? (f) For each financial year of the 2016 Australian Cyber Security Strategy since the establishment of each JCSC, what is the average number of people who visit each centre per day? Per month? (g) For each financial year of the 2016 Australian Cyber Security Strategy since the establishment of each Joint Cyber Security Centre, what is the median number of people who visit each centre per day? Per month? (h) How many events have been held at each Joint Cyber Security Centre in Sydney, Melbourne, Adelaide, Perth and Brisbane? (i) For each Joint Cyber Security Centre in Sydney, Melbourne, Adelaide, Perth and Brisbane, what is the average number of people who attend JCSC events? (j) For each Joint Cyber Security Centre in Sydney, Melbourne, Adelaide, Perth and Brisbane, what is the median number of people who attend JCSC events?
16	Kitching	Joint Cyber Security Centres Collaborative Programs		Appendix A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that "JCSCs have established strong collaborative programs with state and territory governments, academic institutions, and a wide range of key industry and small business associations." (a) How many collaborative programs have JCSC established with state and territory governments? Please provide details of these collaborative programs. (b) How many collaborative programs have JCSC established with academic institutions? Please provide details of these collaborative programs. (c) How many collaborative programs have JCSC established with industry associations? Please provide details of these collaborative programs. (d) How many collaborative programs have Joint Cyber Security Centres established with small business associations? Please provide details of these collaborative programs.
17	Kitching	Funding Joint Cyber Security Centres		The Commonwealth provided $47m over four years to fund the establishment of the Joint Cyber Security Centres. This funding finishes in 2019-20 when the 2016 Cyber Security Strategy ends. (a) How is the government planning to fund the JCSCs beyond this financial year? (b) Will the JCSC's Commonwealth funding be extended?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

18	Kitching	Cyber threats to Healthcare Providers		In October 2019, several hospitals in Victoria were victims of ransomware attacks disrupting clinical services, including outpatient appointments and elective surgery. (a) Who in the Commonwealth government is primarily responsible for providing cyber threat intelligence to health service providers in Australia? (b) Has the ACSC provided targeted cyber threat intelligence to health service providers about the risk of ransomware attacks? (c) How many health care providers are ACSC Partners? (d) How many times have health care providers have been to events held at Joint Cyber Security Centres? (e) Is the ACSC's assessment that health care providers are well prepared to protect themselves against threats of ransomware attacks? (f) Is the ACSC's assessment that health care providers are well prepared to mitigate the impact of ransomware attacks? (g) Is the ACSC's assessment that no further steps need to be taken by the Commonwealth to help health care providers prepare themselves from this threat of ransomware attacks? (h) Has the ACSC assessed the potential impact to Australian citizens of ransomware campaigns that target health care providers? (i) Has the ACSC assessed the potential impact to Australian health care providers if they were targeted by a ransomware campaign? (j) Who is responsible for providing guidance to health care providers on managing these threats? (k) Have there been any independent assessments of the cyber resilience of Australian health care providers?
19	Kitching	Advice to Local, State and Territory Governments		According to 11 May 2019 article by Kevin Collier of CNN, since 2013 over 170 local and state governments in the US have been victims of ransomware attacks. (a) Who in the Commonwealth government is primarily responsible for providing cyber threat intelligence to local governments in Australia? (b) Who in the Commonwealth government is primarily responsible for providing cyber threat intelligence to state governments in Australia? (c) Has the ACSC provided targeted cyber threat intelligence to state or local governments about these risks? (d) Has the ACSC provided targeted cyber threat intelligence to representative bodies such as the Australian Local Government Association? (e) How many local governments or local government representative bodies are ACSC Partners? (f) How many times have local governments or local government representative bodies been to events held at Joint Cyber Security Centres? (g) Is the ACSC's assessment that local government is well prepared to protect themselves against threats of ransomware attacks? (h) Is the ACSC's assessment that local government is well prepared to mitigate the impact of ransomware

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				attacks? (i) Has the ACSC assessed the potential impact to Australian citizens if a ransomware campaign like that targeting US local governments were to target Australian local governments? (j) Has the ACSC assessed the potential impact to Australian businesses if a ransomware campaign like that targeting US local governments were to target Australian local governments? (k) Who is responsible for providing guidance to local governments and state governments on managing threats of ransomware attacks? (l) Has there been any independent assessments of the cyber resilience of Australian local governments? (m) Is ACSC aware of any Australian local governments being subject of ransomware attacks?
20	Kitching	Advice to schools		According to the (a) Who in the Commonwealth government is primarily responsible for providing cyber threat intelligence to schools in Australia? (b) Has the ACSC provided targeted cyber threat intelligence to schools about risks of ransomware attacks? (c) Has the ACSC provided targeted cyber threat intelligence to representative bodies such as the Catholic Schools NSW about the risks of ransomware attacks? (d) How many schools or schools representative bodies are ACSC Partners? (e) How many times have schools or schools representative bodies been to events held at Joint Cyber Security Centres (f) Is the ACSC's assessment that schools are well prepared to protect themselves against threats of ransomware attacks? (g) Is the ACSC's assessment that schools are well prepared to mitigate the impact of ransomware attacks? (h) Who is responsible for providing guidance to schools on managing the threats of ransomware attacks? (i) Has there been any independent assessments of the cyber resilience of Australian schools? (j) Is ACSC aware of any Australian schools being subject of ransomware attacks?
21	Kitching	Advice to healthcare researchers		In its report "Beyond Compliance: Cyber Threats and Healthcare," cybersecurity company FireEye reported that foreign government-linked hackers have targeted organizations involved health research such as cancer research and medical devices. These attacks include incidents in 2019, but also date back as far as 2013. (a) Who in the Commonwealth government is primarily responsible for providing cyber threat intelligence to medical and health research institutes in Australia? (b) Has the ACSC provided targeted cyber threat intelligence to National Health and Medical Research Council about risks of cyber-attacks from foreign government linked hackers? (c) Has the ACSC provided targeted cyber threat intelligence to the Australian Research Council about risks of cyber-attacks from foreign government linked hackers? (d) Has the ACSC provided targeted cyber threat intelligence to Medical Research Future Fund about risks of cyber-attacks from foreign government linked hackers?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				(e) Has the ACSC provided targeted cyber threat intelligence to institutes within Australian universities that conduct medical research such as ANU's John Curtain School of Medical Research about risks of cyber-attacks from foreign government linked hackers? (f) Are the National Health and Medical Research Council, Australian Research Council, Medical Research Future Fund, or any of the medical research institutes within Australian universities ACSC Members? (g) How many times have National Health and Medical Research Council, Australian Research Council, Medical Research Future Fund, or any of the medical research institutes within Australian universities been to events held at JCSCs? (h) Is the ACSC's assessment that the National Health and Medical Research Council, Australian Research Council, Medical Research Future Fund, or any of the medical research institutes within Australian universities are well prepared to protect themselves against these threats? (i) Is the ACSC's assessment that the NHMRC, ARC, Medical Research Future Fund, or any of the medical research institutes within Australian universities are well prepared to mitigate the impact of such attacks? (j) Who is responsible for providing guidance to the National Health and Medical Research Council, Australian Research Council, Medical Research Future Fund, or any of the medical research institutes within Australian universities on managing these threats? (k) Have there been any independent assessments of the cyber resilience of the National Health and Medical Research Council or the Australian Research Council? (l) Is ACSC aware of any Australian medical research organisation being the subject of a cyber-enabled attack.
22	Kitching	Cyber Threat Reports		The UK's National Cyber Security Centre issues weekly cyber threat reports. (a) Does the ACSC publish an equivalent report? (b) If ACSC does not publish an equivalent report, does the government suggest that Australian CISOs subscribe to the UK or US threat reporting? (c) In September 2019, the UK's National Cyber Security Centre issued 9 threat reports. How many did ACSC issue during that period?
23	Kitching	Phishing Attacks		The "ANU Incident Report on the Breach of the Australian National University's Administrative Systems" concluded that the ANU's administrative systems were breached using a targeted spearphishing email and recommended that more effort is required to help drive awareness and safe user behaviours to safeguard from phishing attacks. According to the latest RSA Quarterly Fraud Report (Q2 2019), Australia became the 7th largest hosting location for phishing attacks in the world, hosting more than 3 per cent of global phishing attacks. Australia is ranked three spots higher than the UK on this index. Beyond the "Stay Smart Online" website, is the government developing any proactive outreach activities to drive awareness and user behaviours to protect Australians from phishing attacks?
24	Kitching	Cyber Defence Programs		The UK government's Active Cyber Defence program also works in partnership with UK Government Departments. Using a range of interventions these partnerships have been able to improve the UK's Revenue and Customs (HMRC)'s performance as the 16th most phished brand globally to the 146th most phished brand. Has the ACSC

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				undertaken any similar partnerships to reduce the use of Australian government department's brands, such as the ATO, in phishing campaigns?
25	Kitching	Malicious Code Identification		In the last year, the NCSC used automated scanning to identify 'over 1,200 sites which were serving malicious code to illicitly copy credit card transactions' and helped those small businesses to address these issues to 'protect their customers and their reputation'. Has the ACSC undertaken similar proactive initiatives to assist Australian small businesses address malware infections that jeopardise their customers?
26	Kitching	ASPI Foreign Interference recommendations – detection capabilities		In May 2019, the Australian Strategic Policy Institute made recommendations on how the Australian government could protect Australian democracy from foreign interference information operations. This included increasing the government's detection capabilities by supporting non-profit and independent media. Has the ASD provided advice on how the government can build up capabilities in information operation detection? To whom was this advice provided?
27	Kitching	ASPI Foreign Interference recommendations – impact measurement		In May 2019, the Australian Strategic Policy Institute made recommendations on how the Australian government could protect Australian democracy from foreign interference information operations. This included funding research to measure the impact of foreign interference. Has ASD provided advice on funding research in Australia to develop ways to measure the impact of foreign interference? To whom was this advice provided to?
28	Kitching	ASPI Foreign Interference recommendations – public funding		In May 2019, the Australian Strategic Policy Institute made recommendations on how the Australian government could protect Australian democracy from foreign interference information operations. This included publicly funding the defence of political parties. Has the ASD provided advice on providing public funding to better protect all major political parties from cyber threats? To whom was this advice provided?
29	Kitching	ASPI Foreign Interference recommendations – retaliatory sanctions		In May 2019, the Australian Strategic Policy Institute made recommendations on how the Australian government could protect Australian democracy from foreign interference information operations. This included considering concerted joint global or regional action to impose retaliatory sanctions. Has the Government worked with foreign governments to develop an approach to imposing retaliatory sanctions on state actors that commit cyber-attacks or foreign information operations?
30	Kitching	APH Hack		At the Foreign Affairs, Defence and Trade Senate Estimates Hearing on 23 October 2019, the following exchange took place between Senator Kitching, Ms Rachel Noble the head of ACSC and the Acting Head of ASD, Lt General Frewen: **Senator KITCHING:** There was certainly attribution in a Reuters report that it was a state actor in the breach in Parliament House. Are you investigating how Reuters received that information? Ms Noble**:** No. Lt Gen. Frewen**:** We are not investigating that, no. **Senator KITCHING:** Is anyone investigating that? Lt Gen. Frewen**:** I'm not aware, Senator.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				Is the reason that neither ASD nor the Australian Federal Police is conducting an investigation because the Government authorised the provision of this information to Reuters ? If no, why is no investigation being conducted?
31	Kitching	ACSC Annual Threat Reports		Action 4 of the 2016 Australia's Cyber Security Strategy is "Sponsor research to better understand the cost of malicious cyber activity to the Australian economy". Outcome 3 of Action 4 was "robust data is published that improves the ability of organisations to consider the effectiveness of their investment in cyber security." The Australian Strategic Policy Institute's review of the first year of the Cyber Security Strategy identified two Government reports as providing "some useful information for business" to consider the effectiveness of their investment in cyber (outcome 3) – the ACSC Threat report and the 2015 Cyber Security Survey. The ACSC Threat report was an annual report published in 2015, 2016 and 2017, around October. Why has no report been published since 2017?
32	Kitching	ACSC Cyber Security Survey		Action 4 of the 2016 Australia's Cyber Security Strategy is "Sponsor research to better understand the cost of malicious cyber activity to the Australian economy". Outcome 3 of Action 4 was "robust data is published that improves the ability of organisations to consider the effectiveness of their investment in cyber security." The Australian Strategic Policy Institute's review of the first year of the Cyber Security Strategy identified two Government reports as providing "some useful information for business" to consider the effectiveness of their investment in cyber (outcome 3) – the ACSC Threat report and the 2015 Cyber Security Survey. Since the 2015 Cyber Security Survey, ACSC also published a 2016 Cyber Security Survey. Has ACSC published a Cyber Security survey since the 2016 report? If no, why not?
33	Kitching	ACSC Partnerships measurement		Action 5 of the 2016 *Australia's Cyber Security Strategy* is "In partnership with the private sector, establish a layered approach to cyber threat information sharing through 1) partnerships between businesses and the Government within the Australian Cyber Security Centre; 2) co-designed joint cyber threat sharing centres (initially as a pilot) in key capital cities; and 3) a co-designed online information sharing portal". Outcome 1 of Action 5 is "Partnerships between the Australian Cyber Security Centre and the private sector are increased and proven valuable for both parties". How does the Government measure whether a partnership is "valuable"?
34	Kitching	ACSC number of Partnerships		Action 5 of the 2016 *Australia's Cyber Security Strategy* is "In partnership with the private sector, establish a layered approach to cyber threat information sharing through 1) partnerships between businesses and the Government within the Australian Cyber Security Centre; 2) co-designed joint cyber threat sharing centres (initially as a pilot) in key capital cities; and 3) a co-designed online information sharing portal". Outcome 1 of Action 5 is "Partnerships between the Australian Cyber Security Centre and the private sector are increased and proven valuable for both parties". (a) In Year 1 of the Strategy, how many partnerships between ACSC and the private sector were established?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				(b) In Year 2 of the Strategy, how many partnerships between ACSC and the private sector were established? (c) In Year 3 of the Strategy, how many partnerships between ACSC and the private sector were established?
35	Kitching	CERT Australia		Action 6 of the 2016 Australia's Cyber Security Strategy is "Increase the Computer Emergency Response Team (CERT) Australia's capacity". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper assessed Action 6 as complete because CERT was absorbed into ASD and a 24/7 incident response capability has been established within ASD, expanding the services that CERT and ASD previous provided to businesses and government. (a) How many businesses were served by CERT/ASD in year 1 of the Strategy? (b) How many businesses were served by CERT/ASD in year 2 of the Strategy? (c) How many businesses were served by CERT/ASD in year 1 of the Strategy?
36	Kitching	CERT Australia Number of International Partnerships		Outcome 2 of Action 6 of the 2016 Australia's Cyber Security Strategy is "CERT Australia increases its international partnerships, focusing on prevention and shutting down malicious cyber activity." Before CERT was absorbed into ASD, how many international partnerships did it have?
37	Kitching	CERT Australia mandate - International Partnerships		Outcome 2 of Action 6 of the 2016 Australia's Cyber Security Strategy is "CERT Australia increases its international partnerships, focusing on prevention and shutting down malicious cyber activity." After CERT was absorbed into ASD, does CERT still have a mandate to increase its international partnerships? If not, who was the responsibility transferred to?
38	Kitching	Provision of cyber security services baseline		Action 10 of 2016 Australia's Cyber Security Strategy is "Increase the Australian Signals Directorate's capacity to identify new and emerging cyber threats to our security and improve intrusion analysis capabilities". Outcome 2 of Action 10 is "the Australian Signals Directorate expands the number of cyber security services it offers to a wider range of organisations". What is the baseline number of organisations that ASD provided cyber security services to the year prior to the commencement of the Strategy?
39	Kitching	Provision of cyber security services – expansion of services progress		Action 10 of 2016 Australia's Cyber Security Strategy is "Increase the Australian Signals Directorate's capacity to identify new and emerging cyber threats to our security and improve intrusion analysis capabilities". Outcome 2 of Action 10 is "the Australian Signals Directorate expands the number of cyber security services it offers to a wider range of organisations". (a) In Year 1 of the Strategy, how many organisations did ASD provides services to? (b) In Year 2 of the Strategy, how many organisations did ASD provides services to? (c) In Year 3 of the Strategy, how many organisations did ASD provides services to?
40	Kitching	National Cyber Incident Management		Action 12 of 2016 Australia's Cyber Security Strategy is "Expand the nation's cyber incident management arrangements and exercises program". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that Action 12 was completed because a National Cyber Incident Management Arrangements were agreed

		Arrangements		by the Council of Australian Governments in December 2018; and the ACSC National Exercise Program has supported 55 cyber security exercise activities with Federal, state and territory governments, international governments and owners and operators of Australia's critical infrastructure. Who was consulted in the development of the National Cyber Incident Management Arrangements?
41	Kitching	Cyber Security Exercises Breakdown		Action 12 of 2016 Australia's Cyber Security Strategy is "Expand the nation's cyber incident management arrangements and exercises program". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that Action 12 was completed because a National Cyber Incident Management Arrangements were agreed by the Council of Australian Governments in December 2018; and the ACSC National Exercise Program has supported 55 cyber security exercise activities with Federal, state and territory governments, international governments and owners and operators of Australia's critical infrastructure. (a) Of the 55 cyber security exercise activities, how many were with federal government? Which government entities attended the exercises? (b) Of the 55 cyber security exercise activities, how many were with state or territory governments? a. Which state government entities attended the exercises? (c) Of the 55 cyber security exercise activities, how many were with owners and operators of Australia's critical infrastructure? a. Which owners and operators attended the exercises? (d) Did any private sector entities participate in any of the 55 cyber security exercises?
42	Kitching	Cyber Security Exercises Total Numbers		Action 12 of 2016 Australia's Cyber Security Strategy is "Expand the nation's cyber incident management arrangements and exercises program". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that Action 12 was completed because a National Cyber Incident Management Arrangements were agreed by the Council of Australian Governments in December 2018; and the ACSC National Exercise Program has supported 55 cyber security exercise activities with Federal, state and territory governments, international governments and owners and operators of Australia's critical infrastructure. (a) In Year 1 of the Strategy, how many exercises were conducted? (b) In Year 2 of the Strategy, how many exercises were conducted? (c) In Year 3 of the Strategy, how many exercises were conducted?
43	Kitching	Incident Management		Action 12 of 2016 Australia's Cyber Security Strategy is "Expand the nation's cyber incident management arrangements and exercises program". Outcome 1 of Action 12 is "The Government's cyber incident management arrangements respond to the evolving cyber threat landscape." (a) How does the Government measure progress and achievement of this outcome? (b) In Year 1 of the Strategy, what was the progress made toward this outcome?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				(c) In Year 2 of the Strategy, what was the progress made toward this outcome? (d) In Year 3 of the Strategy, what was the progress made toward this outcome?
44	Kitching	Joint Cyber Exercises Breakdown		Action 12 of 2016 Australia's Cyber Security Strategy is "Expand the nation's cyber incident management arrangements and exercises program". Outcome 3 of Action 12 is "The Government and private sector establish a program of joint cyber exercises." (a) In Year 1 of the Strategy, how many joint cyber exercises between Government and private sector took place? i. What were they? (b) In Year 2 of the Strategy, how many joint cyber exercises between Government and private sector took place? i. What were they? (c) In Year 3 of the Strategy, how many joint cyber exercises between Government and private sector took place? **i.** What were they?
45	Kitching	Joint Cyber Exercises – Progress and International Partners		Action 12 of 2016 Australia's Cyber Security Strategy is "Expand the nation's cyber incident management arrangements and exercises program". Outcome 4 of Action 12 is "Australia works with international partners on developing policies for incident response as a confidence building measure." (a) How does the Government measure progress and achievement of outcome 4? (b) How many international partners has the government worked with to develop incident response policies? (c) Who were these international partners? (d) In Year 1 of the Strategy, what was the progress made toward this outcome? (e) In Year 2 of the Strategy, what was the progress made toward this outcome? (f) In Year 3 of the Strategy, what was the progress made toward this outcome?
46	Kitching	Guidance Products		Action 13 of the 2016 Australia's Cyber Security Strategy is "Co-design voluntary guidelines on good cyber security practice". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that Action 13 was completed because ACSC provides a range of voluntary guidance products. The example cited was the best practices for Managed Service Providers developed as part of the Cloud Hopper operation. (a) Apart from the example of the best practice for MSPs, how many other guidance products did ACSC provide? **i.** What were they?
47	Kitching	Good cyber practice voluntary guidelines – Co-		Action 13 of the 2016 Australia's Cyber Security Strategy is "Co-design voluntary guidelines on good cyber security practice". Outcome 1 of Action 13 is "The Government and private sector co-design and publish baseline guidance for Australian

		design partners		cyber security that provides a benchmark for good practice, informs cyber security insurance and meets corporate obligations." (a) How many private sector partners has the government worked with in this co-design process? (b) Who were these private sector partners? (c) How were these private sector partners selected?
48	Kitching	Good cyber practice voluntary guidelines – Baseline Guidance		Action 13 of the 2016 Australia's Cyber Security Strategy is "Co-design voluntary guidelines on good cyber security practice". Outcome 1 of Action 13 is "The Government and private sector co-design and publish baseline guidance for Australian cyber security that provides a benchmark for good practice, informs cyber security insurance and meets corporate obligations." (a) In Year 1 of the Strategy, what "baseline guidance" was published? (b) In Year 2 of the Strategy, what "baseline guidance" was published? (c) In Year 3 of the Strategy, what "baseline guidance" was published?
49	Kitching	Good cyber practice voluntary guidelines – benchmarking		Action 13 of the 2016 Australia's Cyber Security Strategy is "Co-design voluntary guidelines on good cyber security practice". Outcome 2 of Action 13 is "Australia's good practice guidelines are an economic and security asset—they provide a commercial advantage and ensure cyber risks to critical services are risk assessed and managed." (a) How does the Government measure progress towards outcome 2? (b) Has the government undertaken any international benchmarking of Australia's good practice guidelines to assess their relative strength compared to peer nations? (c) In Year 1 of the Strategy, what was the progress made toward this outcome? (d) In Year 2 of the Strategy, what was the progress made toward this outcome? (e) In Year 3 of the Strategy, what was the progress made toward this outcome?
50	Kitching	Australian Cyber Security Strategy – Outcome 3		Action 13 of the 2016 Australia's Cyber Security Strategy is "Co-design voluntary guidelines on good cyber security practice". Outcome 3 of Action 13 is "Australian businesses, small and large, have improved understanding of good cyber security practices." (a) How does the Government measure progress and achievement of this outcome? (b) What work did the government do to benchmark the level of understanding of large Australian businesses of good cyber security practices at the beginning of the cyber security strategy? (c) What work did the government do to benchmark the level of understanding of Australian small businesses of good cyber security practices at the beginning of the cyber security strategy? (d) What ongoing survey work has the government undertaken to measure levels of understanding of good cyber security practices in large Australian businesses during the life of the cyber security strategy? (e) What ongoing survey work has the government undertaken to measure levels of understanding of good cyber

				security practices in Australian small businesses during the life of the cyber security strategy? (f) In Year 1 of the Strategy, what progress made toward this outcome? (g) In Year 2 of the Strategy, what progress made toward this outcome? (h) In Year 3 of the Strategy, what progress made toward this outcome?
51	Kitching	Australian Cyber Security Strategy – Outcome 4		Action 13 of the 2016 Australia's Cyber Security Strategy is "Co-design voluntary guidelines on good cyber security practice". Outcome 4 is "Governments, critical services and high-risk sectors demonstrate good cyber security practices." (a) How does the Government measure progress and achievement of this outcome? (b) In Year 1 of the Strategy, what was the progress made toward this outcome? (c) In Year 2 of the Strategy, what was the progress made toward this outcome? (d) In Year 3 of the Strategy, what was the progress made toward this outcome?
52	Kitching	Strategies to Mitigate Targeted Cyber Intrusions – Independent Assessments		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Has the ASD conducted independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions?
53	Kitching	Strategies to Mitigate Targeted Cyber Intrusions – Public Availability of Tools		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reported that ASD are using new technology solutions to improve agency cyber hygiene at scale, including automated scanning tools to identify vulnerabilities. The UK government makes these tools publicly available. Why does the ASD not do the same in Australia?
54	Kitching	Strategies to Mitigate Targeted Cyber Intrusions – Sprint Teams		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". The "2020 Cyber Security Strategy: A Call for Views" paper also reports that dedicated 'Sprint Teams' have been created to uplift cyber security for select Australian Government agencies. (a) Which agencies have these sprint teams been deployed to? (b) How were agencies identified as requiring these 'sprint team' intervention?
55	Kitching	Mitigation of Targeted Cyber Intrusions		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Outcome 1 of Action 18 is: "Government agency cyber security practices are the exemplar for public and private

				sector organisations in Australia." (a) How does the Government measure progress and achievement of outcome 1? (b) In Year 1 of the Strategy, what was the progress made toward this outcome? (c) In Year 2 of the Strategy, what was the progress made toward this outcome? (d) In Year 3 of the Strategy, what was the progress made toward this outcome? (e) Does the ASD consider self-assessments of compliance with the strategies to Mitigate Targeted Cyber Intrusions effective considering five years of ANAO cyber security audits have found only 29% of agencies were compliant at the time but in self-reporting to AGD about 60% claim to have implemented the Top Four mitigation strategies? (f) Does ASD consider that sufficient progress has been made toward this outcome, given five years of ANAO cyber security audits have found only four of 14 agencies or 29% were compliant at the time of auditing?
56	Kitching	Cyber Security Capability		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Outcome 2 of Action 18 is "Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability." (a) How does the Government measure progress and achievement of this outcome? (b) In Year 1 of the Strategy, what was the progress made toward this outcome? (c) In Year 2 of the Strategy, what was the progress made toward this outcome? (d) In Year 3 of the Strategy, what was the progress made toward this outcome? (e) Is the fact that five years of Australian National Audit Office cyber security audits have found only 29% were compliant at the time of auditing, while self-reporting to AGD suggests about 60% claim to have implemented the Top Four mitigation strategies an indication that agencies are not equipped to understand, assess or improve their cyber security capability? (f) The PSPF 2017-18 consolidated compliance report shows that only 60.2 percent of the 93 reporting agencies are fully compliant with the top four controls. This is an improvement of only 1.1 percent on the 2015-16 figure of 59.1 precent. In 2014-15, the figure was 48.4 per cent. Does the lack of substantial improvement in these figures indicate slow progress toward Outcome 2?
57	Kitching	Cyber resilience		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Outcome 3 of Action 18 is "Non Government information stored on Government networks is resilient to malicious cyber activity." (a) How does the Government measure progress and achievement of this outcome? (b) In Year 1 of the Strategy, what was the progress made toward this outcome?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				(c) In Year 2 of the Strategy, what was the progress made toward this outcome? (d) In Year 3 of the Strategy, what was the progress made toward this outcome?
58	Kitching	Targeted Independent Assessments		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Outcome 3 of Action 18 is "Non Government information stored on Government networks is resilient to malicious cyber activity." The Australian Signals Directorate revealed that over the 2016, 2017 and 2018 financial years, it responded to 1097 "cyber incidents" affecting both unclassified and classified government networks. Has the government conducted independent assessments across the agencies where these attacks occurred?
59	Kitching	Independent Assessments – ANAO Audits		Action 18 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of the Australian Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions". Outcome 3 of Action 18 is "Non Government information stored on Government networks is resilient to malicious cyber activity." Five years of ANAO cyber security audits have found only 29% of agencies or 4 agencies are cyber resilient. Most government agencies audited as not being cyber resilient have committed to applying the recommendations of the ANAO reports. Has the ASD been doing independent assessments or monitoring to ensure that the ANAO's recommendations are implemented by the agencies that were not found to be cyber resilient?
60	Kitching	Vulnerability Assessments - Progress		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reports that for Action 19, ASD has conducted active vulnerability assessments of a number of key government agencies. How many agencies received these independent security assessments? Which agencies are they?
61	Kitching	Vulnerability Assessments - Outcomes		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reports that for Action 19, ASD has conducted active vulnerability assessments of a number of key government agencies. What were the outcomes of these independent security assessments?
62	Kitching	Migration and Network		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those

		Improvement		agencies address the findings". Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reports that for Action 19, ASD provided clear guidance on mitigation and network improvement. (a) Does ASD follow up to determine whether the guidance has been followed? (b) Does any other independent agency audit compliance with this guidance? (c) What proportion of agencies implement ASD's guidance? (d) What was the consequence of non-compliance with recommendations arising out of the active vulnerability assessments? (e) Were the results of the active vulnerability assessments shared with the Minister? (f) Was the methodology of the active vulnerability assessments different to the ANAO audits? **i.** If so how and why?
63	Kitching	Government Agencies' Cyber Security - Progress		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Outcome 1 of Action 19 is "Government agency cyber security practices are the exemplar for public and private sector organisations in Australia." Does ASD consider that sufficient progress has been made toward this outcome, given five years of ANAO cyber security audits have found only four of 14 agencies or 29% were compliant at the time of auditing?
64	Kitching	Government Agencies Cyber Security - Indications		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Outcome 2 of Action 19 is "Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability." The PSPF 2017-18 consolidated compliance report shows that only 60.2 percent of the 93 reporting agencies are fully compliant with the top four controls. This is an improvement of only 1.1 percent on the 2015-16 figure of 59.1 precent. In 2014-15, the figure was 48.4 percent. What does the lack of substantial improvement in these figures indicate about progress toward Outcome 2?
65	Kitching	Compliance with cyber security controls - Timeframes		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Outcome 2 of Action 19 is "Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability." The PSPF 2017-18 consolidated compliance report shows that only 60.2 percent of the 93 reporting agencies are fully compliant with the top four controls. This is an improvement of only 1.1 percent on the 2015-16 figure of 59.1 precent. In 2014-15, the figure was 48.4 percent. When does the government expect to reach 100% compliance?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

66	Kitching	Compliance with cyber security controls – Steps Taken		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Outcome 2 of Action 19 is "Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability." The PSPF 2017-18 consolidated compliance report shows that only 60.2 percent of the 93 reporting agencies are fully compliant with the top four controls. This is an improvement of only 1.1 percent on the 2015-16 figure of 59.1 precent. In 2014-15, the figure was 48.4 percent. What steps is it taking in order for the Government to reach 100% compliance?
67	Kitching	Active Vulnerability Assessments		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Outcome 3 of Action 19 is "non government information stored on Government networks is resilient to malicious cyber activity." Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reports that for Action 19, ASD provided clear guidance on mitigation and network improvement. The Australian Signals Directorate revealed that over the 2016, 2017 and 2018 financial years it responded to 1097 "cyber incidents" affecting both unclassified and classified government networks. Did the government conduct active vulnerability assessments across the agencies where these attacks occurred?
68	Kitching	Active Vulnerability Assessments - Frequency		Action 19 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings". Outcome 3 of Action 19 is "non government information stored on Government networks is resilient to malicious cyber activity." Annex A of the "2020 Cyber Security Strategy: A Call for Views" paper reports that for Action 19, ASD provided clear guidance on mitigation and network improvement. Five years of ANAO cyber security audits have found only 29% of agencies or 4 agencies are cyber resilient. Most government agencies audited as not being cyber resilient have committed to applying the recommendations of the ANAO reports. How regularly have active vulnerability assessments been undertaken by the agencies that were not found to be cyber resilient by the ANAO?
69	Kitching	Requests for ASD Service		Action 20 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies". Annex A of the "2020 Cyber Security Strategy: A Call for Views" reported that for Action 10, ASD acted on 600 individual service requests across Government since July 2017.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				(a) Which agencies requested ASD service? (b) For each financial year, how many times did each Department request service? (c) What proportion of the services were vulnerability assessments? (d) What proportion of the services were technical security advice? (e) What proportion of the services were advice on emerging technologies?
70	Kitching	Prototype Security Validation Tools		Action 20 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies". Annex A of the "2020 Cyber Security Strategy: A Call for Views" reported that for Action 20, ASD provided a number of Government agencies with a range of prototype security validation tools. (a) Which agencies were provided with these tools? (b) What security validation tools were provided to agencies?
71	Kitching	Compliance with Vulnerability Assessments		Action 20 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies". Outcome 1 of Action 20 is "Government agency cyber security practices are the exemplar for public and private sector organisations in Australia." (a) What proportion of agencies comply with the recommendations of vulnerability assessments? (b) Does ASD conduct assessments on whether security advice/guidance has been followed by agencies? (c) What proportion of security advice/guidance has been followed by agencies?
72	Kitching	PSPF 2017-18 Compliance		Action 20 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies". Outcome 2 of Action 19 is "Government agencies are empowered to maintain a high level of cyber security and are equipped to improve their cyber security capability." The PSPF 2017-18 consolidated compliance report shows that only 60.2 percent of the 93 reporting agencies are fully compliant with the top four controls. This is an improvement of only 1.1 percent on the 2015-16 figure of 59.1 precent. In 2014-15, the figure was 48.4 percent. Does the lack of substantial improvement in these figures indicate slow progress toward Outcome 2?
73	Kitching	Vulnerability Assessments		Action 20 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies". Outcome 3 of Action 19 is "Non Government information stored on Government networks is resilient to malicious cyber activity." The Australian Signals Directorate revealed that over the 2016, 2017 and 2018 financial years it

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				responded to 1097 "cyber incidents" affecting both unclassified and classified government networks. Did ASD conduct vulnerability assessments in agencies where these attacks occurred?
74	Kitching	Vulnerability Assessments - Frequency		Action 20 of the 2016 Australia's Cyber Security Strategy is "Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies". Outcome 3 of Action 19 is "Non Government information stored on Government networks is resilient to malicious cyber activity." Five years of ANAO cyber security audits have found only 29% of agencies or 4 agencies are cyber resilient. Most government agencies audited as not being cyber resilient have committed to applying the recommendations of the ANAO reports. How regularly has vulnerability assessments been undertaken by the agencies that were not found to be cyber resilient by the ANAO?
75	Kitching	Guidance Reports		Action 21 of the 2016 Australia's Cyber Security Strategy is "Develop guidance for Government agencies to consistently manage supply chain security risks for ICT equipment and services" so that "Government agencies have clear guidance on identifying and managing cyber security risks when procuring ICT equipment and services." Annex A of the "2020 Cyber Security Strategy: A Call for Views" reported that Action 21 was complete because "ASD developed, in consultation with industry and government stakeholders, a technical guidance on cyber supply chain risk management for practitioners and executives. This guidance was published on cyber.gov.au on 25 June 2019.The Government-issued guidance provided in August 2018 to network providers highlighted the security risks that arise in 5G networks." (a) How many "Guidance" reports has the Government issued in Year 1 of the Strategy? (b) How many "Guidance" documents has the Government issue in Year 2 of the Strategy? (c) How many "Guidance" documents has the Government issue in Year 3 of the Strategy?
76	Kitching	Small Business Cyber Security Survey		In June 2019, the ACSC launched the Small Business Cyber Security Survey. (a) When will the results of the survey be published? (b) Why was this survey only launched at the end of Year 3 of the strategy?
77	Kitching	2018 PSPF		The October 2018 PSPF moved cyber security controls, including the Essential 8, away from a compliance-based approach toward a principles-based cyber security framework. The rationale behind this change was to allow entities to apply the PSPF in a way that best suits their individual security goals and objectives. The ASD and ACSC has also released updates to the Australian Government Information Security Manual (ISM) to align it with the new risk-based approach in the PSPF giving organisations "greater flexibility to manage their own cyber security". Five years of ANAO cyber security audits on entities have found only 29% were compliant with the mandatory four, while self-reporting to AGD suggests about 60% claim to have implemented the Top Four mitigation strategies. (a) Given this, are you concerned that entities do not have the necessary cyber security maturity to be given lee

				way to "apply the PSPF in a way that best suits their individual needs"? (b) Given the November 2018 release of the ISM replaced compliance concepts with risk management concepts. Will the ASD continue to report on whether government departments are compliant with the Essential 8? (c) The move toward a risk-based approach for the PSPF was recommended by a 2015 Belcher Red tape review. Did the ASD provide advice to the government on the potential impacts "cutting red tape" could have on the transparency and effectiveness of cyber security in government? (d) The new PSPF adopts a life cycle approach to security management (including cyber security) made up of Planning, Monitoring and Reporting. Why is evaluation missing from this cycle? (e) Whose responsibility is it to evaluate the success of the risk-based approach in the PSPF of improving the governments overall cyber security posture?
78	Kitching	Upgrades to facilities / offices		1. Have any furniture, fixtures or fittings of the Secretary's office, or the offices of any Deputy Secretaries been upgraded since 1 July 2018. If so, can an itemised list of costs please be provided (GST inclusive). 2. Were there any upgrades to facility premises at any of the Departments or agencies since 1 July 2018. This includes but is not limited to: staff room refurbishments, kitchen refurbishments, bathroom refurbishments, the purchase of any new fridges, coffee machines, or other kitchen equipment. 3. If so, can a detailed description of the relevant facilities upgrades be provided together with an itemised list of costs (GST inclusive). 4. If so, can any photographs of the upgraded facilities be provided.
79	Kitching	FOI requests		1. Please list the number of Freedom of Information Act requests ('FOI requests') received by the Department for the following years: a. 2013-14; b. 2014-15; c. 2015-16; d. 2016-17; e. 2018-19; and f. 2019-20 to date. 2. For each year above, please provide: a. The number of FOI requests the Department granted in full; b. The number of FOI requests the Department granted in part; c. The number of FOI requests the Department refused in full; and d. The number of FOI requests the Department refused for practical reasons under the Freedom of Information Act. 3. For each year above, please also provide: a. The number of times the Department failed to make any decision on a FOI request within the 30 day statutory period; and

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				b. The number of times a request to the Department resulted in a practical refusal (i.e. no decision was made on the request). 4. For each year above, please also provide: a. The number of times the Department's FOI decisions have been appealed to the OAIC; and
80	Kitching	FOI Resourcing		1. Please provide the staffing (both ASL and headcount) of staff at the Department who work exclusively on FOI requests, broken down by APS level (e.g. three EL1s, four APS6s, one SES) for each of the following years: a. 2013-14; b. 2014-15; c. 2015-16; d. 2016-17; e. 2018-19; and f. 2019-20 to date. 2. For each of the years above, please also list the number of officers who are designated decision makers under the Freedom of Information Act 1982 within the Department. 3. In the past 12 months, has the Department seconded additional resources to processing Freedom of Information requests? If so, please detail those resources by APS level. 4. Please provide the number of officers who are currently designated decision makers under the Freedom of Information Act 1982 within the Minister's office. 5. Please provide the number of FOI requests currently under consideration by the Department. Please also provide the number of these requests that are currently overdue in response. 6. Does the department consult or inform the Minister when it receives Freedom of Information requests? If so: a. How many times has this occurred in the past twelve months; and b. Please outline the process by which the Department consults the Minister. 7. Has the Department consulted or informed another Department or agency about any FOI request in the past twelve months. If so, please provide the legal basis on which that consultation occurred (e.g. third party consultation, transfer of request).
81	Kitching	Briefings		1. Has the Department/agency or the Minister's office provided briefings to independents/minor parties in the Senate or House of Representatives. If so, can the following be provided: a. The subject matter of the briefing. b. The location and date of the briefing. c. Who proposed the briefing. d. Attendees of the briefing by level/position
82	Kitching	Promotional material		1. What was the Department/agency's total expenditure on promotional merchandise for FY 2018-19. 2. Can an itemised list of all Austender Contract Notice numbers for all promotional merchandise contracts in that period please be provided.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				3. Can photographs or samples of relevant promotional merchandise please be provided.
83	Kitching	Commissioned reports		1. Since 24 August 2018, how many Reports or Reviews have been commissioned. Please provide details of each report including: a. Date commissioned. b. Date report handed to Government. c. Date of public release. d. Terms of Reference. e. Committee members and/or Reviewers. 2. How much did each report cost/or is estimated to cost. 3. The background and credentials of the Review personnel. 4. The remuneration arrangements applicable to the Review personnel, including fees, disbursements and travel 5. The cost of any travel attached to the conduct of the Review. 6. How many departmental staff were involved in each report and at what level. 7. What is the current status of each report. When is the Government intending to respond to each report if it has not already done so.
84	Kitching	Market research		1. Does the Department/agency undertake any polling or market research in relation to government policies or proposed policies. 2. If so, can the Department provide an itemised list of: a. Subject matter b. Company c. Costs d. Contract date period 3. Can the Department/agency advise what, if any, research was shared with the Minister or their office and the date and format in which this occurred.
85	Kitching	Advertising and Information Campaign		1. What was the Department/agency's total expenditure on advertising and information campaigns for FY 2018-19 and for the current financial year to date. 2. What advertising and information campaigns did the Department/agency run in each relevant period. For each campaign, please provide: a. When approval was first sought. b. The date of approval, including whether the advertising went through the Independent Campaign Committee process. c. the timeline for each campaign, including any variation to the original proposed timeline. 3. Can an itemised list of all Austender Contract Notice numbers for all advertising and information campaign

				contracts in each period be provided.
86	Kitching	Social media influencers		1. What was the Department/agency's total expenditure on social media influencers for FY 2018-19 and 2019-20 to date. 2. What advertising or information campaigns did the Department/agency use social media influencers to promote. 3. Can a copy of all relevant social media influencer posts please be provided. 4. Can an itemised list of all Austender Contract Notice numbers for all relevant social media influencer contracts please be provided.
87	Kitching	Congestion busting		1. Can the Department/agency advise how it is "congestion busting" in relation to bureaucratic bottlenecks and regulatory bottlenecks. 2. Have any additional resources been allocated within the Department to achieve "congestion busting" within the department.
88	Kitching	Media monitoring		1. What is the total cost of media monitoring services, including press clippings, electronic media transcripts etcetera, provided to the each Minister's office for FY 2018-19 and FY 2019-20 to date. a. Which agency or agencies provided these services. b. Can an itemised list of Austender Contract notice numbers for any media monitoring contracts in each period please be provided c. What is the estimated budget to provide these services for the year FY 2019-20. 2. What was the total cost of media monitoring services, including press clippings, electronic media transcripts etcetera, provided to the department/agency for FY 2018-19 and FY 2019-20 to date. a. Which agency or agencies provided these services. b. Can an itemised list of Austender Contract Notice numbers for any media monitoring contracts in each period please be provided c. What is the estimated budget to provide these services for the year FY 2019-20.
89	Kitching	Comms staff		1. For all departments and agencies, please provide – in relation to all public relations, communications and media staff – the following: 2. By Department or agency: a. How many ongoing staff, the classification, the type of work they undertake and their location. b. How many non-ongoing staff, their classification, type of work they undertake and their location. c. How many contractors, their classification, type of work they undertake and their location. d. How many are graphic designers. e. How many are media managers. f. How many organise events.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				3. Do any departments/agencies have independent media studios. a. If yes, why. b. When was it established. c. What is the set up cost. d. What is the ongoing cost. e. How many staff work there and what are their classifications.
90	Kitching	Executive Management		In relation to executive management for the Department and its agencies, can the following be provided for FY 2018-19 and 2019-20 to date: a. The total number of executive management positions b. The aggregate total remuneration payable for all executive management positions. c. The change in the number of executive manager positions. d. The change in aggregate total remuneration payable for all executive management positions.
91	Kitching	Ministerial functions		In relation to any functions or official receptions hosted by Ministers or Assistant Ministers in the portfolio since 1 July 2018, can the following be provided: a. List of functions. b. List of all attendees. c. Function venue. d. Itemised list of costs (GST inclusive). e. Details of any food served. f. Details of any wines or champagnes served including brand and vintage. g. Any available photographs of the function. h. Details of any entertainment provided.
92	Kitching	Departmental functions		In relation to expenditure on any functions or official receptions etc hosted by the Department or agencies within the portfolio since 1 July 2018, can the following be provided: a. List of functions. b. List of all attendees. c. Function venue. d. Itemised list of costs (GST inclusive). e. Details of any food served. f. Details of any wines or champagnes served including brand and vintage. g. Any available photographs of the function. h. Details of any entertainment provided.
93	Kitching	Staff travel		What is the total cost of staff travel for departmental/agency employees for FY 2018-19 and FY 2019-20 to date.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

94	Kitching	Legal costs		What are the total legal costs for the Department/agency for FY 2018-19 and FY 2019-20 to date.
95	Kitching	Secretarial travel		Can an itemised list of the costs of all domestic and international travel undertaken by the Secretary of the Department since 1 July 2018 be provided including: a. Flights for the Secretary as well as any accompanying departmental officials, and identify the airline and class of travel. b. Ground transport for the Secretary as well as any accompanying departmental officials. c. Accommodation for the Secretary as well as any accompanying departmental officials, and identify the hotels the party stayed at and the room category in which the party stayed. d. Meals and other incidentals for the Secretary as well as any accompanying departmental officials. Any available menus, receipts for meals at restaurants and the like should also be provided. e. Any available photographs documenting the Secretary's travel should also be provided.
96	Kitching	Acting Minister arrangements		Can the Department provide all leave periods of the portfolio Minister from 24 August 2018 to date. Can the Department further provide acting Minister arrangements for each leave period.
97	Kitching	Departmental staff allowances		Can a list of Departmental/agency allowances and reimbursements available to employees be provided.
98	Kitching	Ministerial overseas travel		1. Can an itemised list of the costs met by the department or agency for all international travel undertaken by Ministers or Assistant Ministers in the portfolio since 1 July 2018 please be provided including: a. Flights for the Minister and any accompanying members of the Minister's personal staff or family members, as well as any accompanying departmental officials, together with the airline and class of travel. b. Ground transport for the Minister and any accompanying members of the Minister's personal staff or family members, as well as any accompanying departmental officials. c. Accommodation for the Minister and any accompanying members of the Minister's personal staff or family members, as well as any accompanying departmental officials, and identify the hotels the party stayed at and the room category in which the party stayed. d. Meals and other incidentals for the Minister and any accompanying members of the Minister's personal staff or family members, as well as any accompanying departmental officials. Any available menus, receipts for meals at restaurants and the like should also be provided. e. Any available photographs documenting the Minister's travel should also be provided.
99	Kitching	Board Appointments		1. Provide an update of portfolio boards, including board title, terms of appointment, tenure of appointment and members. 2. What is the gender ratio on each board and across the portfolio 3. Please detail any board appointments made from 1 July 2018 to date.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				4. What has been the total value of all Board Director fees and disbursements paid. 5. What is the value of all domestic travel by Board Directors. 6. What is the value of all international travel by Board Directors.
100	Kitching	Appointments – briefs prepared		1. How many times has the Department prepared a brief for statutory authorities, executive agencies, advisory boards, government business enterprises or any other Commonwealth body which includes a reference to a former Liberal or National member of parliament at a state, territory or federal level. 2. For each brief prepared, can the Department advise: a. The former member. b. The board or entity. c. Whether the request originated from the Minister's office. d. Whether the appointment was made.
101	Kitching	Stationery		How much has been spent on ministerial stationery requirements in FY 2019-19 and FY 2019-20 to date.
102	Kitching	Departmental staff in Minister's office		1. Can the Department provide an update on the total number of departmental staff seconded to ministerial offices, including: a. Duration of secondment. b. APS level. 2. Can the Department provide an update on the total number of DLOs/CLOs for ministerial offices including APS level.
103	Kitching	CDDA Payments		1. How many claims have been received under the Compensation for Detriment caused by Defective Administration scheme (CDDA) by the Department for FY 2018-19? 2. How many claims were: a. Accepted. b. Rejected. c. Under consideration. 3. Of the accepted claims, can the Department provide: a. Details of the claim, subject to relevant privacy considerations b. The date payment was made c. The decision maker.
104	Kitching	Recruitment		1. What amount has been expended by the department/agency on external recruitment or executive search services in FY 2018-19 and FY 2019-20 to date. 2. Which services were utilised. Can an itemised list be provided
105	Kitching	Staffing		1. How many full-time equivalent staff are engaged at 21 October 2019. How does this differ from the figures presented in Budget Paper 4 in the 2019-20 Budget.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				2. How many of these positions are (a) on-going and (b) non-ongoing. 3. How many redundancies have occurred in FY 2018-19 and FY 2019-20 to date. How many were: a. voluntary b. involuntary. 4. How many of those redundancies occurred as a result of departmental restructuring. What is the total cost of those redundancies. 5. What was the total value in dollar terms of all termination payments paid to exiting staff. 6. How much overtime or equivalent has been paid to staff in FY 2018-19 and FY 2019-20 to date. 7. How many section 37 notices under the Public Service Act 1999 have been offered in FY 2018-19 and FY 2019-20 to date.
106	Kitching	Comcare		1. For FY 2018-19 and FY2019-20 to date, can the Department advise whether it has been the subject of any investigations involving Comcare. If yes, please provide details of the circumstances and the status. 2. Can the Department advise the number of sanctions it has received from Comcare in the FY2019-20 to date.
107	Kitching	Fair Work Commission		For FY 2018-19 and FY2019-20 to date, how many references have been made to the Fair Work Commission within the Department or agency.
108	Kitching	Fair Work Ombudsman		For FY 2018-19 and FY2019-20 to date, how many references have been made to the Fair Work Ombudsman within the Department or agency.
109	Kitching	Office of the Merit Protection Commissioner		For FY 2018-19 and FY2019-20 to date, how many references have been made to the Office of the Merit Protection Commissioner within the Department or agency.
110	Kitching	Public Interest Disclosures		For FY 2018-19 and FY2019-20 to date, how many public interest disclosures have been received.
111	Gallagher	External Consultants		In relation to the use of all external consultants in the Department or agencies within the portfolio, can the following be provided. a. For each of the last six financial years from 2013-14 to 2018-19, the total amount spent on external consultants, including: i. contracts tagged as a “consultancy”. ii. contracts not defined as a “consultancy”, but tagged as ‘‘business intelligence consulting services’’, ‘‘information technology consultation services’’, ‘‘management advisory services’’, ‘‘management support services’’, ‘‘organisational structure consultation’’, ‘‘risk management consultation services’’ or ‘‘strategic planning consultation services’’ b. The total amount of full time equivalent hours (FTE’s) provided by external consultants in 2018-19. c. The total amount of variances granted to external consultant contracts (including those specified in 1(a)(i) above) in 2018-19.

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

				d. A breakdown by consultant, specifications and project completion for 2018-19.
112	Gallagher	External IT Consultants		In relation to expenditure on information technology in the Department or agencies within the portfolio, can the following be provided. a. For each of the last six financial years from 2013-14 to 2018-19, the total amount spent on information technology consultation services b. The total amount of full time equivalent hours (FTE's) provided by information technology consultation services in 2018-19. c. The total amount contracted to information technology consultation services in 2018-19. d. The total amount of variances granted to information technology consultation services contracts in 2018-19. e. A breakdown by consultant, specifications and project completion for 2018-19.
113	Gallagher	External Contractors		In relation to the use of all external contractors in the Department or agencies within the portfolio, can the following be provided: 1. The total amount spent on all contracts for Management and Business Professionals and Administrative Services for each of the last six financial years from 2013-14 to 2018-19. 2. The total amount spent on all contracts tagged as "Temporary Personnel Services" for each of the last six financial years from 2013-14 to 2018-19. 3. The total number of external contractors employed in 2018-19. 4. The aggregate total remuneration payable for all external contractors employed in 2018-19. 5. The total number of FTE hours provided by external contractors in 2018-19.
114	Gallagher	External IT Contractors		In relation to the use of external information technology contractors in the Department or agencies within the portfolio, can the following be provided: 1. The total amount spent on external contractors for each of the last six financial years from 2013-14 to 2018-19. 2. The total number of external contractors employed in 2018-19. 3. The aggregate total remuneration payable for all external contractors employed in 2018-19. 4. The total number of FTE hours provided by external contractors in 2018-19.
115	Gallagher	Grants		Please provide, for all administered and discretionary grant programs administered by each department and agency within the portfolio: 1. Name of the administered or discretionary grant program. 2. The recipient of the grant. 3. The ABN or ACN of the grant recipient. 4. The charitable status of the grant recipient. 5. Who authorised the grant payment. 6. For each year of the budget and forward estimates:

				a. What is the total funding budgeted for the program; b. How much funding has been contracted and allocated; c. How much funding has been contracted but not allocated; d. How much funding has been committed but not contracted; e. How much funding is uncommitted, uncontracted and unallocated.
116	Gallagher	Cost of APS staff		The total cost of all staff employed under the Public Service Act for each of the last six financial years from 2013/14 to 2018/19.
117	Gallagher	*Overall compliance and reporting*		The Australian Government set a target date for government entities to achieve compliance with the Australian Signals Directorate's Top Four mitigation strategies as detailed in the Protected Security Policy Framework (PSPF), INFOSEC 10 core requirements[1] by 30 June 2014[2]. Non-corporate Commonwealth entities are required to apply the Mandatory 4 whereas it is only considered best practice for corporate Commonwealth entities and wholly-owned Commonwealth companies. ASD had stated that implementing the top 4 mitigation strategies will be able to prevent over 85% of unauthorised intrusions. *Overall compliance and reporting* 1. Is the Department compliant with the core requirements in the Protected Security Policy Framework, *INFOSEC 10: Safeguarding information from cyber threats* policy? 2. Under the Public Governance, Performance and Accountability Act 2013, all non-corporate Commonwealth entities are required to report annually to the Attorney-General on the implementation of the Protected Security Policy Framework (PSPF). Has the Department provided an annual report to the Attorney general in 2015, 2016, 2017, 2018 and 2019 on compliance with the INFOSEC 10 core requirements?
118	Gallagher	Mandatory 4 implementation		The Australian Government set a target date for government entities to achieve compliance with the Australian Signals Directorate's Top Four mitigation strategies as detailed in the Protected Security Policy Framework (PSPF), INFOSEC 10 core requirements by 30 June 2014 . Non-corporate Commonwealth entities are required to apply the Mandatory 4 whereas it is only considered best practice for corporate Commonwealth entities and wholly-owned Commonwealth companies. ASD had stated that implementing the top 4 mitigation strategies will be able to prevent over 85% of unauthorised intrusions. Mandatory 4 implementation 3. Has the Department implemented Protected Security Policy Framework INFOSEC 10, requirement 1:

[1] https://www.protectivesecurity.gov.au/information/safeguarding-information-from-cyber-threats/Documents/pspf-infosec-10-safeguarding-information-cyber-threats.pdf
[2] ANAO, Audit Report No. 42 (2016–17), p. 7.

				application whitelisting? a. According to the Essential Eight Maturity Model what is the maturity of application whitelisting implementation? 4. Has the Department implemented Protected Security Policy Framework INFOSEC 10, requirement 2: patching applications? a. According to the Essential Eight Maturity Model, what is the maturity of patching applications implementation? 5. Has the Department implemented Protected Security Policy Framework INFOSEC 10, requirement 3: restriction of administrative privileges? a. According to the Essential Eight Maturity Model, what is the maturity of 'restrict administrative privileges' implementation? 6. Has the Department implemented Protected Security Policy Framework INFOSEC 10, requirement 4: patching operating systems? a. According to the Essential Eight Maturity Model, what is the maturity of 'Patching operating systems' implementation? https://www.protectivesecurity.gov.au/information/safeguarding-information-from-cyber-threats/Documents/pspf-infosec-10-safeguarding-information-cyber-threats.pdf ANAO, Audit Report No. 42 (2016–17), p. 7. https://www.cyber.gov.au/publications/essential-eight-maturity-model
119	Gallagher	Essential 8 implementation		Essential 8 implementation 7. Has the Department implemented Protected Security Policy Framework INFOSEC 10, C.4, 27 (a): configuring Microsoft Office macro settings? a. According to the Essential Eight Maturity Model what is the maturity of 'configuring Microsoft Office macro settings' implementation? 8. Has the Department implemented Protected Security Policy Framework INFOSEC 10, C.4, 27 (b): user application hardening? a. According to the Essential Eight Maturity Model what is the maturity of 'configuring Microsoft Office macro settings' implementation? 9. Has the Department implemented Protected Security Policy Framework INFOSEC 10, C.4, 27 (c): multi-factor authentication? a. According to the Essential Eight Maturity Model what is the maturity of 'multi-factor authentication' implementation? 10. Has the Department implemented Protected Security Policy Framework INFOSEC 10, C.4, 27 (d): daily backups? a. According to the Essential Eight Maturity Model what is the maturity of 'daily backups' implementation?

SSCFADT QUESTIONS ON NOTICE INDEX

Supplementary Estimates Hearings 23 October 2019

Australian Signals Directorate

120	Gallagher	Accountability and funding		11. How many times has the Department conducted a self assessment of its compliance with the Protected Security Policy Framework Essential Eight mitigation strategies and cyber resilience since 1 July 2013? 12. How many independent assessments of its cyber resilience has the Department conducted since 1 July 2013? 13. Has the Minister responsible been briefed on cyber security vulnerabilities in the Department networks since 1 July 2013? 14. Has an Australian Signals Directorate cyber security sprint team been deployed to the Department since 1 July 2013? 15. How much funding has the Department allocated to cyber security each year during 2015, 2016, 2017, 2018 and 2019? 16. How many times has there been a physical or cyber intrusion attempt made on the Department's networks that were considered serious enough to warrant an operational response in 2015, 2016, 2017, 2018 and 2019?