Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience - 02 July 2020 - Q1 - Adequacy of cyber resilience of commonwealth entities - Mr Watts

Question reference number: 1

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

In the last report issued by the JCPAA on cyber security (Report 467) Recommendation 2 provided:

"The Committee recommends that the Australian Government mandate the Australian Signals Directorate's Essential Eight cybersecurity strategies for all Public Governance, Performance and Accountability Act 2013 entities, by June 2018."

In response, the government stated:

"The Government is committed to ensuring all Commonwealth entities raise their level of cyber security and understand the risks they face. The Essential Eight represents ASD's best advice on the measures an entity can take to mitigate the threat of a cyber incident and manage their risks. However, the Government will consider mandating the Essential Eight when cyber security maturity has increased across entities."

At his June 19th press conference the Prime Minister outlined an increasingly dangerous cyberspace threat environment for the Australian government; specifically highlighting that "Australian organisations are currently being targeted by a sophisticated state-based cyber actor… including all levels of government"

At the July 2nd JCPAA hearing the Attorney General's Department indicated that they had considered an decided not to increase the mandatory cyber security requirements within the PSPF from the Top 4 to the Essential 8.

Given Recommendation 2 of JCPAA's report on cyber resilience (Report 467), that the Essential Eight be made mandatory for all Public Governance, Performance and Accountability Act 2013 entities by June 2018, and given the increasingly dangerous cyber threat environment highlighted by the Prime Minister and the claimed improvement in the

cyber maturity levels of Commonwealth entities, why was the decision made not to incorporate ASD's Essential Eight mitigations as mandatory aspects of the PSPF?

Answer:

Questions relating to the PSPF are a matter for the Attorney-General's Department.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience - 02 July 2020 – Q2 - Impact of New Government Funding for ASD on Commonwealth Entity Cyber Resilience - Mr Watts

Question reference number: 2

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

The recently released 2020 Force Structure Plan highlighted an increasingly dangerous cyberspace threat environment for the Australian government:

"Defence is becoming more reliant on fast, reliable and secure internet based communications. But the threat to this connectivity from malicious actors is also growing. There has been a marked increase in cyber-attacks against Australia by foreign actors and criminals"

The 2020 Defence Strategic Update then outlined $15 billion of investment over the coming 10 years in the Information and Cyber domain.

How much of this funding will go to Commonwealth departments to progress their implementation the mandatory Top 4 cyber security controls specified in the PSPF?

Answer:

As announced through the Defence 2020 Force Structure Plan, $15 billion will be invested by the Defence Portfolio (including the Australian Signals Directorate) for cyber and information warfare capabilities in over the next decade. This includes the recently announced investment of $1.35 billion over 10 years from 2020-21 to enhance and continue initiatives focussed on national situational awareness of cyber threats, disrupting cyber criminals offshore and building partnerships with industry and government which enhance national cyber resilience.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience - 02 July 2020 - Q3 - Security implications of increased transparency and accountability mechanisms - Mr Watts

Question reference number: 3

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

In Senate estimates, when asking about Commonwealth entities' Top 4 compliance, the orchestrated response received from multiple entities read, in part:

"Publicly reporting on individual agency's compliance with the Essential 8 in response to these questions on notice would provide a single, detailed and individualised snapshot in time of the entire Federal Government's cyber security maturity and as a result may provide a heat map for vulnerabilities in Federal Government networks, which malicious actors may exploit and thus increase an agency's risk of cyber incidents."

But the Auditor General has challenged this response, stating, when appearing before the JCPAA on 19th May 2020:
"We never report a level of detail which we believe would put any particular entity at risk."

Over the past 6 years ANAO has conducted 5 public cyber resilience performance audits of 16 different Commonwealth entities examining ASD Top 4 compliance. It is currently undertaking such an audit into 9 government entities.

Why is it acceptable for the ANAO to be undertaking and publishing their audits but not for the government to implement transparent accountability mechanisms?

Answer:

ASD tabled its first *Commonwealth Cyber Security Posture* annual report to Parliament in March 2020 which includes aggregated results of the status of the Commonwealth's cyber security posture. As indicated at page 4 of that report, ASD does not identify the cyber security posture or vulnerabilities of individual Commonwealth entities as this may increase their risk of being targeted by malicious cyber actors.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience Inquiry - 02 July 2020 - Q4 - Mr Watts

Question reference number: 4

Senator/Member: Mr Watts
Type of question: Written,
Date set by the committee for the return of answer: 04 August 2020

Question:

How could a Member of Parliament hold a Commonwealth Entity accountable for non-compliance with mandatory cyber security requirements in commonwealth entities for which they are responsible?

Answer:

ASD is not able to advise on parliamentary processes.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience - 02 July 2020 - Q5 - Security implications of increased transparency and accountability mechanisms - Mr Watts

Question reference number: 5

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

Of the 25 Commonwealth entities that were involved in the government's 'Cyber Uplift', none were assessed to have achieved their recommended cyber security maturity level. The 2019 Posture Report concluded that "these entities are vulnerable to current cyber threats targeting the Australian government".

Why did the Cyber Uplift end if none of the entities involved had reached minimum cyber security requirements?

Answer:

Page 5 of the *Commonwealth Cyber Security Posture in 2019* Report to Parliament, indicates that the "Cyber Uplift included ACSC teams conducting 'sprint' programs to assess and baseline the maturity of 25 Commonwealth entities in implementing the *Essential Eight*."

The report also states on page 5 that each "entity received tailored advice and guidance, which provided a snapshot of their maturity level, as well as prioritised recommendations and a roadmap for future improvements to their cyber security maturity".

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience - 02 July 2020 - Q6 - Cyber uplift - Mr Watts

Question reference number: 6

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

Why was the Cyber Uplift unable to bring any of these entities up to minimum cyber security requirements?

Answer:

Page 5 of the *Commonwealth Cyber Security Posture in 2019* Report to Parliament, indicates that the "Cyber Uplift included ACSC teams conducting 'sprint' programs to assess and baseline the maturity of 25 Commonwealth entities in implementing the *Essential Eight*."

The report also states on page 5 that each "entity received tailored advice and guidance, which provided a snapshot of their maturity level, as well as prioritised recommendations and a roadmap for future improvements to their cyber security maturity".

As indicated at page 3-4, cyber security maturity is a "compliance and risk management issue for each accountable authority to balance in the context of their unique risk environments and the complexities of their operations."

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience – 02 July 2020 - Q7 - Cyber uplift costs - Mr Watts

Question reference number: 7

Senator/Member: Mr Watts
Type of question: Written,
Date set by the committee for the return of answer: 04 August 2020

Question:

What did this Cyber Uplift program cost? Is the ASD funded to run further Cyber Uplifts in the coming year?

Answer:

In accordance with longstanding practice, the expenditure details of these activities will not be published on national security grounds.

ASD will continue to invest in cyber resilience and uplift programs as part of the $1.35 billion dollar investment in cyber security recently announced by the Prime Minister, the Minister for Defence and the Minister for Home Affairs.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20) – 2 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience - 02 July 2020 - Q8 - Further Cyber Uplift Funding - Mr Watts

Question reference number: 8

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

Was funding for further Cyber Uplifts included in the Prime Minister's recent multi-billion dollar cyber security announcement?

Answer:

Yes. ASD will continue to conduct similar cyber uplift initatives as part of the $1.35 billion dollar investment in cyber security recently announced by the Prime Minister.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience Inquiry - 02 July 2020 - Q14 – Bug Bounty Program - Mr Watts

Question reference number: 14

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

Since 2016, more than 10,000 vulnerabilities have been discovered as security researchers were invited to US government bug bounties including: Hack the Pentagon, Hack the Army, Hack the Air Force, Have the Marine Corp and Hack the Defence Travel System.

Has the government considered the adoption of bug bounty programs for Commonwealth government agencies?

Answer:

No.

ASD operates in line with the Responsible Release Principles for Cyber Security Vulnerabilities, which are available at asd.gov.au.

In line with these principles, ASD engages actively with the information technology research community and industry who disclose vulnerabilities to ASD.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience Inquiry - 02 July 2020 - Q16 – Policies for Bug Bounty Programs - Mr Watts

Question reference number: Q16

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 04 August 2020

Question:

Are there any centralised guidelines or policies for Commonwealth agencies concerning the use of bug bounty programs for their IT systems? If not, why not?

Answer:

ASD operates in line with the Responsible Release Principles for Cyber Security Vulnerabilities, which are available at asd.gov.au.

In line with these principles, ASD engages actively with the information technology research community and industry who disclose vulnerabilities to ASD.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor General's Reports 1 and 13 (2019-20) - 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience Inquiry - 02 July 2020 - Q17- Centralised Vulnerability Disclosure Platform - Mr Watts

Question reference number: 17

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

Since August 2019, the United Kingdom's National Cyber Security Centre has operated a vulnerability disclosure platform of last resort for UK government entities on the HackerOne platform.

Why has the Commonwealth government not used a centralised vulnerability disclosure program to supplement the cyber security posture of Commonwealth entities?

Answer:

ASD operates in line with the Responsible Release Principles for Cyber Security Vulnerabilities, which are available at asd.gov.au.

ASD engages actively with the information technology research community and industry to identify vulnerabilities.

Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor General's Reports 1 and 13 (2019-20) – 02 July 2020

ANSWER TO QUESTION ON NOTICE

Australian Signals Directorate

Topic: ASD JCPAA Cyber Resilience Inquiry - 02 July 2020 - Q18 – Implementation Guidelines for Vulnerability Disclosure Programs - Mr Watts

Question reference number: 18

Senator/Member: Mr Watts
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Question:

Are there any centralised guidelines or policies for Commonwealth agencies concerning the implementation of vulnerability disclosure programs for their websites or IT systems? If not, why not?

Answer:

As this is a policy related question, it is best directed to the relevant policy department/s.