OFFICIAL

Defence Portfolio

Parliamentary Inquiry Question on Notice

The Joint Committee of Public Accounts and Audit asked the Australian Signals Directorate at the Inquiry into Commonwealth Financial Statements 2021–22, upon notice, on 24 May 2023.

In relation to the Protective Security Policy Framework (PSPF).

GENERAL

1. Can the ASD provide an overview of the cybersecurity landscape for Australia, and for government entities in particular?

2. What is the role of the ASD's Cyber Security Centre in ensuring the implementation of cybersecurity measures?

3. How does the PSPF assist entities in protecting information and systems from internal and external threats?

ESSENTIAL EIGHT CYBER MITIGATION STRATEGIES

4. The PSPF requires non-corporate Commonwealth entities to implement the ASD's Cyber Security Centre's 'Essential Eight' cyber mitigation strategies.

Can the ASD provide a brief overview of the 'Essential Eight' cyber mitigation strategies?

5. How are the strategies defined and what are the four maturity levels for their implementation?

6. What are the current requirements for non-corporate Commonwealth entities regarding the 'Essenal Eight' strategies?

7. What are the current requirements for corporate Commonwealth entities?

8. Entities are required to implement each of the Essential Eight strategies at a minimum of Maturity Level Two.

How many Commonwealth entities have met this requirement?

9. How many Commonwealth entities have not met this requirement?

10. What is the trend in compliance over time?

11. What oversight or assurance mechanism is in place to ensure entities comply with the mandatory requirements?

REMOVAL OF USER ACCESS

12. How many entities have effective controls to monitor access or activity in their systems after a user's departure?

13. How many have ineffective controls for this?

14. What are the reoccurring challenges that government entities have in implementing effective controls for the timely removal of user access to government systems and data?

15. How many government entities lack a policy addressing user access removal (or defining the timeframe) following a user's departure?

16. What impact does the absence of termination controls in HR systems have on the timely removal of user access?

The Australian Signals Directorate has provided the following answers to the Joint Committee of Public Accounts and Audit's questions:

1. Australian Signals Directorate's Annual Cyber Threat Report 2021/2022 sets out the cyber security landscape.
2. The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC), consistent with ASD's functions as set out in the Intelligence Service Act 2001, provides technical advice and assistance to the whole of economy. ASD is not a regulator and does not oversee or enforce compliance with the advice and assistance it provides.
3. This question should be referred to the Attorney-General's Department who are responsible for the PSPF.
4. ASD's ACSC has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight, as outlined on www.cyber.gov.au in ASD's publication *Strategies to mitigate Cyber Security Incidents.*

   The mitigation strategies that constitute the Essential Eight mitigations are:

   - application control
   - patch applications
   - configure Microsoft Office macro settings
   - user application hardening
   - restrict administrative privileges
   - patch operating systems
   - multi-factor authentication, and
   - regular backups.

   The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks and is based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting entities with implementing the Essential Eight mitigation strategies.
5. The strategies are defined within the context of the Essential Eight Maturity Model which supports the implementation of the Essential Eight. There are four maturity levels which are Maturity Level Zero through to Maturity Level Three. Maturity Level Three is the highest maturity level that can be achieved.
6. In March 2022, the Attorney General's Department mandated the Essential Eight for all Non-Corporate Commonwealth Entities (NCCE) through amendments to the Protective Security Policy Framework (PSPF). Further questions should be referred to the Attorney General's Department.
7. Questions on the requirements of corporate Commonwealth Entities under the PSPF should be directed to the Attorney-General's Department.
8. For questions 8 to 10 please see the below combined response.
   a. As per *The Commonwealth Cyber Security Posture in 2022 - Report to Parliament*, tabled in December 2022:
      i. 11% of entities have reached Overall Maturity Level 2, relying on the implementation of Essential Eight controls alone; an increase from 4% in 2021.

ii. 19% of entities self-assessed that they had reached Maturity Level 2 when compensating controls to mitigate gaps in the Essential Eight implementation were taken into account; an increase from 14% in 2021.

iii. Between 2021 and 2022, the greatest improvements to the number of entities implementing an Essential Eight strategy to Maturity Level 2 were observed in Patch applications (26% improvement) and Patch operating systems (24% improvement).

b. For further detailed information please refer to Chapter 2.1 of *The Commonwealth Cyber Security Posture in 2022 – Report to Parliament* on www.cyber.gov.au.

11. ASD is not a regulator and does not oversee or enforce compliance with the advice and assistance it provides. Questions on compliance with the PSPF should be referred to the Attorney General's Department.

12. Questions 12 to 16 should be referred to the Attorney-General's Department which administers the PSPF on behalf of the Australian Government. ASD is not a regulator and does not oversee or enforce compliance with the advice and assistance it provides.