PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

Joel Bateman
Committee Secretary
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Mr Bateman

I refer to your letter of 18 February 2019 regarding the Committee's inquiry based on ANAO Report No. 53 (2017-18) examining cyber resilience. The following submission has been prepared by the Department of Parliamentary Services (DPS).

DPS is the primary Information and Communication Technology (ICT) service provider for the Parliament of Australia and therefore has overall responsibility for cyber security across the parliament. DPS undertakes a comprehensive body of proactive and reactive work to enhance the cyber resiliency of the parliamentary network. This network extends beyond Parliament House and includes Electorate and Commonwealth Parliament Offices, including over 5,000 users, 5,000 PCs and laptops, 1,000 servers and in excess of 2,000 mobile devices.

DPS Approach to Cyber Security

Effective cyber resiliency extends beyond the Australian Signal Directorate's (ASD) Top Four and Essential Eight and involves the development of a comprehensive strategy to predict and protect against and detect and respond to cyber threats.

In the prediction space, DPS works to understand the complex cyber environment and learn about emerging threats. This allows us to proactively mitigate threats before they reach our network. DPS participates in the whole of government gateway consolidation program to draw upon the expertise of commercial providers and over 30 other government agencies in predicting and proactively blocking cyber threats at our network boundary. DPS has implemented an industry leading threat intelligence platform which allows collation of a variety of threat feeds from open source, commercial entities and government agencies. Agreements are also in place with the parliaments of the other FVEYS nations to share threat information and to assist in planning for and mitigating cyber threats within the global parliamentary context.

Significant investment has been made by DPS in the cyber protection domain. An annual program of work is fully funded to implement the ASD Information Security Manual (ISM) and other additional controls to harden the parliamentary network to reduce the risk of cyber intrusion. In addition to technical controls, DPS has developed overarching information and ICT security policies to guide user behaviour. Security awareness has also been a critical component of our protect strategy with a range of initiatives including face to face and online modalities being introduced in the past two years.

In the current cyber environment it is inevitable that a small number of sophisticated threats will evade preventative controls and as a result no system can be considered completely invulnerable. When a compromise occurs, best practice requires rapid detection of the intrusion and a robust response to remove the attacker from the network as quickly as possible to limit damage or loss.

This is a capability that DPS had identified within the parliamentary cyber defenses that needs to mature through new capability and which it has been building over the past 18 months. In 2018, DPS secured $9 million in Commonwealth funding to continue the development of a dedicated parliamentary Cyber Security Operations Centre (CSOC). The CSOC is a critical component of our strategy to detect and respond to cyber threats and incidents.

DPS response in the context of ANAO Report No. 53

a) Implementation of cyber risk mitigation strategies

DPS is unable to publically comment on the specific security controls in place within the environment as to do so may assist potential malicious actors to refine their methods of attack. DPS can however confirm that it has implemented the Top Four strategies to mitigate cyber intrusions and has a priority program in place to obtain maturity level three in the Top Four strategies within the next 12 months. Of the four remaining strategies in the Essential Eight, one has been fully implemented, one has been implemented to level of approximately 70% and one is currently in pilot.

The remaining Essential Eight strategy which has not been implemented is due to the impact this would have on the flexibility of systems and software used by parliamentarians and is being risk managed to the extent this is possible. Within our unique environment the variety of software and services utilised by parliamentarians is highly varied and most likely exceeds the volume and diversity evident in other Commonwealth agencies. However in light of recent events reevaluation of all controls within the Essential Eight is being undertaken to ensure maximum protection of the environment is enabled.

Report No. 53 places specific emphasis on reduction of privileged access. Significant work has been undertaken by DPS in the last two years to greatly reduce the number of staff with high level system access. All domain administration duties also require use of multi factor authentication and technical controls are currently being implemented to limit the granting of administrative privilege to users on a 'per request basis' as opposed to this access being permanently available.

Within the context of the report, DPS is in transition from internally resilient status to that of cyber resilient.

b) Self-assessment

DPS is not an accountable authority in terms of mandating reporting compliance within the Essential Eight and cannot comment on the report's findings in relation to the activities of the Attorney General's Department, Home Affairs or ASD. However DPS has actively participated in the annual reporting scheme managed by these agencies and will continue to do so. DPS will continue to track ongoing changes in the Protective Security Policy Framework (PSPF), Essential Eight and the wider ISM and will ensure these changes are reflected in our voluntary and mandatory reporting requirements.

c) Management arrangements and cyber risk culture

DPS pursues a comprehensive risk-based approach to cyber security. Cyber security is embedded at the enterprise level within the organisational risk register and is backed by established response plans to address cyber related incidents, disaster recovery scenarios and business continuity events. Cyber security also features prominently within ICT governance frameworks. Cyber security teams are involved and consulted as part of the ICT change management process, architectural design, and ICT security risk assessments are performed for all project related activities.

An annual program of work is included within the DPS capital works program to build ongoing cyber security capabilities. This work program not only addresses the Essential Eight but also builds capability across the wider 'strategies to mitigate cyber incidents' as detailed in the ISM. The program is also critical to building maturity in the predict, protect, detect and respond domains. DPS recognises that the current work program is developed on an annual basis and is working to evolve a longer term three-year cyber security strategy which will align to the wider Digital Strategy for the Parliament of Australia.

Cyber security has significant executive support within the organisation. Recently a dedicated branch under the management of an SES band 1 Chief Information Security Officer (CISO) was established to provide leadership in this critical area. The CISO, who reports to the Chief Information Officer, regularly reports on cyber related issues and plans to the DPS Executive Committee, Security Management Board, Audit Committee, the Parliamentary ICT Advisory Board (PICTAB) and other inter-parliamentary governance groups. These activities elevate cyber security issues to a high level of visibility and allow cyber related matters to form part of informed decision-making across the parliament.

Cyber security is everyone's responsibility. ICT support and operations staff work closely with cyber security teams to ensure that relevant ICT security measures are followed on a daily basis. Cyber security awareness for all staff is also a major priority. All DPS staff undertake mandatory security training which includes a cyber component. More detailed briefings are also conducted on an annual basis for all staff in parliamentary departments. DPS has also launched online cyber security awareness training with a number of modules being compulsory for all staff. Security briefings have also been provided to new parliamentarians and their staff. Additional written and online material will be made available leading up to the election and face-to-face briefings on cyber security matters always form part of the induction for new parliamentarians.

DPS has undertaken a shift in focus away from protecting systems to the protection and treatment of information as a strategic asset. An information audit is underway to identify the key information sources within the department. The audit also involves the identification of information owners, current controls and residual risk. The results of this audit will be a significant guidepost to ensure that our cyber activities are prioritised to protect the information that is of most value to the parliament.

Conclusion

DPS has made significant advances in the area of cyber resiliency and with high levels of executive support and dedicated funding for cyber security will continue to evolve our capabilities in this area.

In February 2019 the parliamentary network was exposed to a significant cyber incident in the form of a sophisticated attack by a state-sponsored actor. This event tested our processes and highlighted a number of issues which will be the target for future and ongoing improvement. Early indications are that the intrusion was detected early and addressed rapidly. During the remediation the parliamentary network was unavailable for less than three hours in the early hours of the morning on 8 February, highlighting our resilience to continue operations and respond effectively during a major cyber incident. DPS also acknowledges the support and assistance of ASD and the Australian Cyber Security Centre (ACSC) who worked side by side with DPS staff to address the issue. The partnership and collaboration with ASD and the ACSC is a critical and ongoing component of our cyber security approach.

The Australian Parliament is a unique environment where there is a high demand for flexibility which must be balanced against the need to maintain a robust security posture. ICT operations supporting

needs. This presents a greater challenge compared to government departments where controls and restrictions are easier to implement and enforce to achieve cyber resiliency. The evolving cyber landscape will undoubtedly result in an increase in cyber threats facing the parliament. DPS is committed to pursuing the optimum point between security and flexibility. However it is highly likely in coming months and years the level of security, control and restrictions required will need to be increased in order to ensure the security and the integrity of the ICT environment within which the parliament operates.

DPS has provided this submission to emphasise the work that continues to occur in building our cyber resiliency and to highlight the impact this work has had on our ability to effectively respond to a significant cyber incident. Discussing operational security would expose the parliament's system to greater risk of future incidents. On this basis, DPS is unable to publicly further detail cyber resilience measures.

Yours sincerely

Rob Stefanic
Secretary

7 March 2019