Senate Economics Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Supplementary Budget Estimates

2019 - 2020

Division/Agency: Australian Prudential Regulation Authority
Question No: SBT 617
Topic: PSPF and Essential 8 Compliance: Mandatory 4 implementation
Reference: Written
Senator: Katy Gallagher

Question:

3. Has the Department implemented Protected Security Policy Framework INFOSEC 10, requirement 1: 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?

Answer:

3-6.

The Government has agreed to the Joint Committee of Public Accounts and Audit Report 467: Cyber Security Compliance recommendation that the Attorney-General's Department and Australian Signals Directorate, in consultation with the Department of Home Affairs, report annually to the Parliament on the Commonwealth's cyber security posture. The first report will be delivered by the end of quarter 1 (2020 calendar year).

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.