Cybersecurity Compliance Inquiry

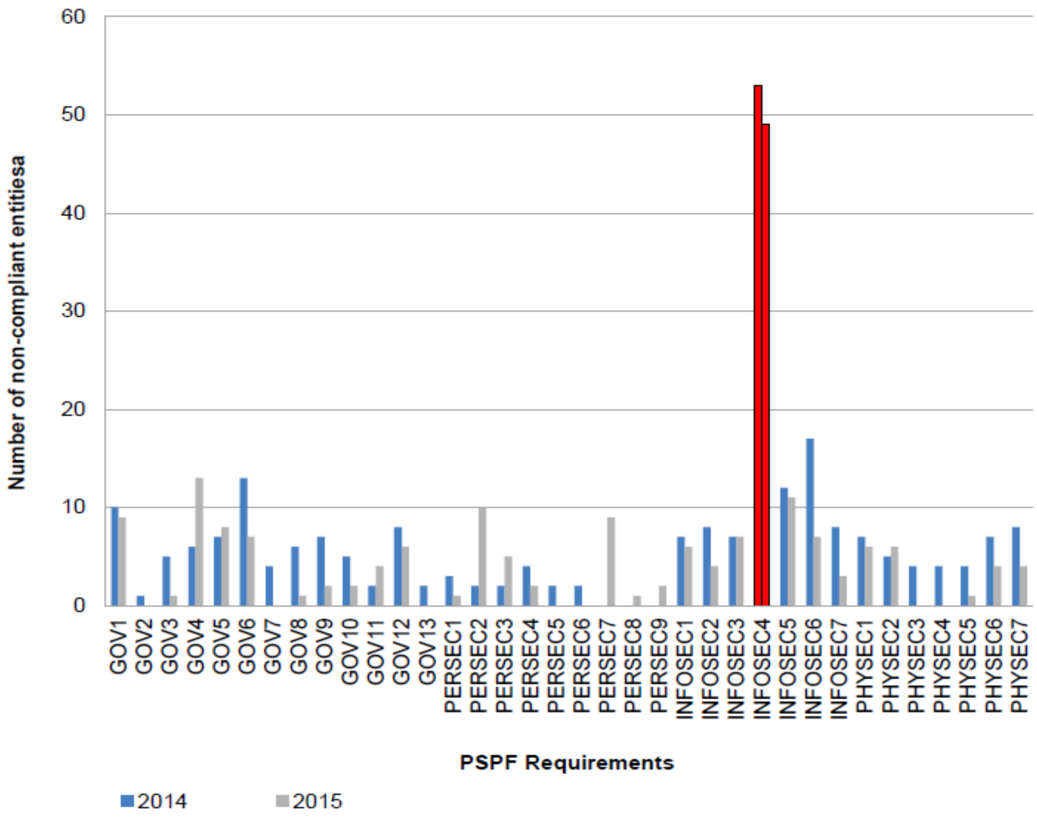
Joint Committee of Public Accounts and Audit

Submission by the Australian National Audit Office
1 May 2017

1. Building cyber resilience within the Australian public sector is a strategic priority of the Government, with controls identified that are designed to protect ICT systems by mitigating targeted cyber intrusions. These controls have been documented in the *Australian Government Information Security Manual* (ISM) since 2005 and in the *Australian Communications-Electronic Security Instruction 33* (ACSI 33) before that time.
2. In recognition of the risks associated with government entities' exposure to cyber threats, in 2010, the Australian Signals Directorate (ASD) consolidated the controls aimed to mitigate targeted cyber intrusions into a list of 35 strategies. ASD has estimated that the effective implementation of the 'Top Four' of these strategies can decrease cyber intrusions by 85 per cent. In 2013, the Government made the implementation of the 'Top Four' mitigation strategies—referred to as INFOSEC4—a mandatory requirement as part of the *Australian Government Protective Security Policy Framework* (PSPF) for all non-corporate Commonwealth entities.
3. The Attorney-General's Department is responsible for the development and delivery of the PSPF, with all non-corporate Commonwealth entities required to comply with the mandatory elements in accordance with their risk environment. Under the PSPF, entities are also required to conduct an annual self-assessment of their compliance with the framework and report their results to the department[1]. In 2014 and 2015, INFOSEC4 had the highest rate of non-compliance among the 36 mandatory PSPF requirements for reporting entities (refer to graph below).

[1] For internal audit and reporting purposes, a requirement of the PSPF is agencies must send a copy of their annual report on compliance with the mandatory requirements to the Auditor-General.

Australian National
Audit Office



Note a: A total of 104 entities conducted an annual PSPF compliance self-assessment.
Source: Attorney-General's Department, Protective Security Policy Framework 2014–15 Compliance Report.

4. Since 2013, the ANAO has conducted three cybersecurity performance audits [2]that assessed compliance with the INFOSEC4 requirements, with 11 different government entities subject to audit coverage. These audits found that only three of the entities reviewed were compliant with the requirements and were cyber resilient including the Department of Human Services, Australian Transaction Reports Analysis Centre and the Department of Agriculture and Water Resources. Entities that were not compliant with the mandatory requirements were not cyber resilient. The ANAO's audits and the PSPF self-assessment reporting point to a systemic issue of entities' non-compliance with the mandatory cybersecurity requirements.

5. The ANAO's most recent performance audit of cybersecurity, Audit Report No. 42 of 2016-17, *Cybersecurity follow-up Audit*—which is the subject of this inquiry—assessed

[2] ANAO report No.50 of 2013-14 Cyber Attacks: Securing Agencies' ICT Systems, ANAO Report No.37 of 2015-16 Cyber Resilience, ANAO Report No.42 of 2016-17 Cybersecurity Follow-up Audit

whether the Australian Taxation Office, the Department of Human Services, and the Department of Immigration and Border Protection were compliant with INFOSEC4 requirements. Each of these three entities had previously given assurances to the Joint Committee of Public Accounts and Audit that compliance with the INFOSEC4 requirements would be achieved during 2016. The ANAO concluded that, of the three entities, only the Department of Human Services had achieved compliance with the INFOSEC4 requirements and was cyber resilient.

6. Through its audit coverage, the ANAO has found that the fundamental obstacles for entities achieving compliance with the INFOSEC4 requirements and cyber resilience were at the entities' governance level, including a lack of: effective governance arrangements; strategic prioritisation for cybersecurity; and a clear and effective cybersecurity strategy.
7. The Prime Minister recently reinforced the Government's positioning of cyber resilience as a strategic priority during the release of the *Australia's Cybersecurity Strategy 2016*. As part of the strategy, the Prime Minister announced 33 initiatives to improve cyber security for the nation, with three initiatives directly related to the ANAO's cybersecurity audit findings. The Government's first annual update of the strategy (which was released by the Minister Assisting the Prime Minister for Cyber Security in April 2017), indicated that, while progress has been made, these three initiatives had yet to be completed.