Cyber Attacks: Securing Agencies' ICT Systems

Audit Report No.50 2013–14

Opening Statement by Auditor-General

JCPAA Review 24 October 2014

1. Chair, members of the Committee, ANAO Report No.50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems*, assesses selected government entities compliance with the four mandatory ICT security strategies and related controls in the *Australian Government Information Security Manual.*

2. Cyber crime is an international problem. In the government sector, the Australian Signals Directorate has estimated that in 2012, there were over 1790 security incidents against Australian Government entities. Of these, 685 were considered serious enough to warrant a Cyber Security Operations Centre response.

3. The Attorney-General's Department is responsible for administering the Australian Government's protective security policy, which has as its objective to promote the most effective and efficient ways to secure the continued delivery of Government business.

4. In addition, the Australian Signals Directorate has developed 35 specific strategies to assist Australian Government entities achieve the desired level of comfort over their ICT systems and mitigate the risk of cyber intrusions. ASD has advised entities that if fully implemented, the top four mitigation strategies would prevent at least 85 per cent of the targeted cyber intrusions to entity ICT systems.

5. An amendment to the *Protective Security Policy Framework* issued in April 2013 had the effect of mandating the top four mitigation strategies with immediate effect, and setting a target date of July 2014 for full implementation of the top four strategies.

6. Seven agencies were selected by the ANAO to be included in this performance audit, the: Australian Bureau of Statistics; Australian Customs and Border Protection Service; Australian Financial Security Authority; Australian Taxation Office; Department of Foreign Affairs and Trade; Department of Human Services; and IP Australia. These agencies were selected based on the character and sensitivity of the information primarily managed by the agency.

7. Overall, the audit concludes that the agencies subject to audit had established internal information security frameworks, implemented controls designed to safeguard the enterprise ICT environment from external cyber attack, and had stipulated change management processes to authorise the implementation of security patches for applications and operating systems. While these arrangements contributed to the protection of agency information, the selected agencies had not yet achieved full compliance with the top four mitigation strategies mandated by the Australian Government in 2013; a requirement reflecting heightened government expectations in response to the risk of cyber attack. Further, none of the selected agencies were expected, at the time of the audit, to achieve full compliance by the Government's target date of mid-2014, notwithstanding their advice regarding further initiatives which, when implemented, would strengthen ICT security controls and protection against cyber attacks.

8. Based on their stage of implementation of the top four mitigation strategies and IT general controls, the selected agencies' overall ICT security posture was assessed as providing a reasonable level of protection from breaches and disclosures of information from internal sources, with vulnerabilities remaining against attacks from external sources to agency ICT systems. In essence, agency processes and practices have not been sufficiently responsive to the ever–present and ever–changing risks that government systems are exposed to.

9. The ANAO made three recommendations directed towards achieving full compliance with the mandatory mitigation strategies and related controls, and to strengthen the selected agencies' overall ICT security posture.

* * *