Additional Estimates – ASD Director-General Opening Statement, 4 March 2020

As the Committee is aware, ASD has three principal missions:

- the collection of signals intelligence;
- our cybersecurity mission; and
- our cyber offensive role

In all cases, our primary imperative is to protect Australians and the integrity of Australian systems – and our digital borders – from serious threats – from the threat of terrorism, to protecting and supporting our defence force personnel when they are deployed overseas.

ASD's functions are set out in its legislation, in particular, Section 7 of the Intelligence Services Act 2001. However our core functions date back to when ASD's precursor organisation was first established in 1947.

Our functions include:

- Obtaining intelligence about the capabilities, intentions or activities of people or organisations outside Australia (s7(1)(a))
- Providing material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information (cybersecurity) (s7(1)(ca))
- Providing assistance to the Defence Force in support of military operations (s7(1)(d))

In performing its functions, ASD has a range of specialised technical capabilities that can also be used to assist other government agencies in the performance of their own roles. This includes providing assistance to law enforcement and security agencies. This assistance function is clearly set out in the Intelligence Services Act (s7(1)(e) and s7(1)(f)).

In July 2018, the Government expanded ASD's functions under the Intelligence Services Act to include a power to prevent and disrupt cybercrime conducted outside Australia (s7(1)(c)). This change also included the authority for ASD to prevent and disrupt cybercrime undertaken by, or enabled by, an Australian person offshore, in special circumstances, subject to authorisation by the Minister under Section 8(1)(iii) of the Act.

As this Committee knows, while much of our cybersecurity role, and the protection of Australia's digital borders, is conducted domestically – ASD is prohibited by legislation from producing intelligence on Australian persons except in rare circumstances, and only then under the authority of a Ministerial Authorisation. This is an important safeguard, and one that is fundamental to ASD's work. Our responsibility to protect the online safety and privacy of Australians is paramount.

Since 1 July last year, the ACSC has responded to over 1,275 cybersecurity incidents, at an average of more than 5 incidents per day.

On 25 December, ACSC released a public notification, warning organisations of a critical vulnerability in Citrix devices. In the absence of an official patch to the vulnerability, the ACSC provided mitigation strategies to organisations, including all Commonwealth, state and territory chief information security officers. We updated this advisory most recently on 13

February to provide further information on malicious actors actively exploiting the vulnerability.

Throughout February this year, the ACSC has worked closely with Toll Group, at their behest, in relation to their recent ransomware incident. Our assistance has included providing technical experts to identify the nature and extent of the compromise, and provide Toll with tailored mitigation advice.

The Cyber Incident Management Arrangements (CIMA) were activated twice since July 2019, including for the Emotet malware campaign. The ACSC coordinates CIMA activations through its role on the National Cyber Security Committee (NCSC). Partnership with our state and territory counterparts is essential to the successful detection and response to multi-jurisdictional cybersecurity incidents.

Following the establishment of the ACSC's new online cybercrime reporting tool, ReportCyber, on 1 July 2019, over 36,000 reports of cybercrime have been received. That's an average of over 145 reports a day – or more than one report every ten minutes.

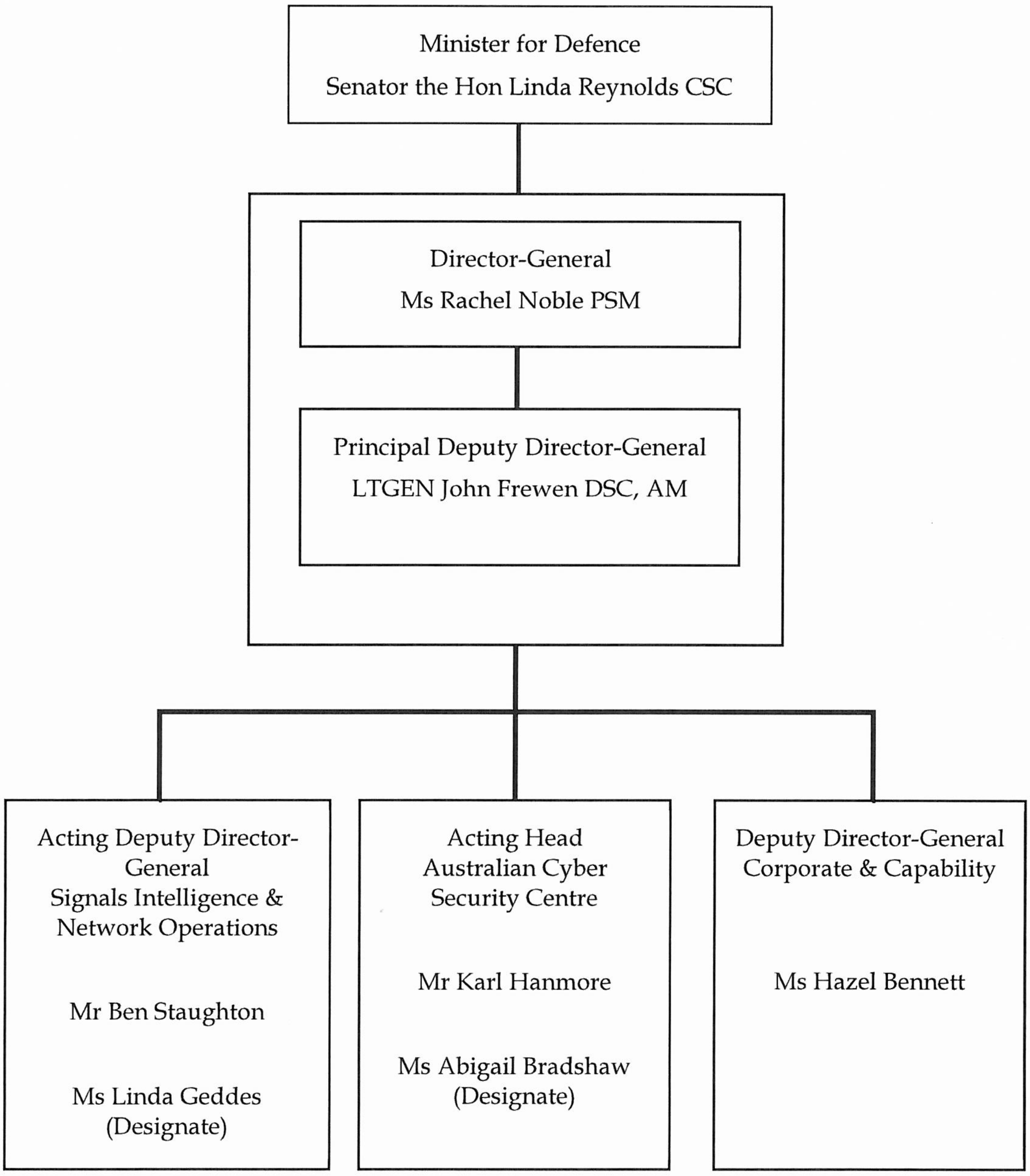
Since ASD last appeared before this Committee, we have also released our Cybercrime in Australia report, which outlines the scale and impact of cybercrime activity in Australia during the July-September quarter of 2019. Over this time, individuals and small to medium enterprises self-reported financial losses to ReportCyber of more than $890,000 each day – representing estimated annual losses to cybercrime of $328 million.

Under our recently legislated role of preventing offshore cybercrime, we are also seeing significant results. In one case, ASD, in collaboration with our UK counterpart GCHQ, identified over 200,000 stolen credit cards globally, including over 11,000 stolen Australian cards. These stolen credit cards represent potential losses of over $90 million globally, and over $7.5 million domestically. This case also demonstrates how our intelligence actions offshore, can directly impact online safety and security here at home.

I would like to table for the Committee an updated organisation chart with our senior officers.

I thank the Committee for its time, and I welcome your questions.

ASD Organisational Structure



Minister for Defence
Senator the Hon Linda Reynolds CSC

Director-General
Ms Rachel Noble PSM

Principal Deputy Director-General
LTGEN John Frewen DSC, AM

Acting Deputy Director-General
Signals Intelligence & Network Operations

Mr Ben Staughton

Ms Linda Geddes (Designate)

Acting Head Australian Cyber Security Centre

Mr Karl Hanmore

Ms Abigail Bradshaw (Designate)

Deputy Director-General Corporate & Capability

Ms Hazel Bennett