CYBERSECURITY — GOVERNMENT AGENCIES

667. Hon TJORN SIBMA to the Minister for Innovation and the Digital Economy:

I refer to cybersecurity across the Western Australian public sector network.

(1) How many cybersecurity incidents have been reported to the Office of Digital Government by affected agencies this year?

(2) What was the nature of these incidents?

Hon STEPHEN DAWSON replied:

I thank the honourable member for some notice of the question.

(1) From 1 January 2023 to 16 June 2023, 10 232 incidents were reported to the Office of Digital Government's cyber security operations centre.

(2) The answer to (2) is in tabular form. I seek leave to have it incorporated into *Hansard*.

[Leave granted for the following material to be incorporated.]

Discovery	Techniques used to gain knowledge about systems and internal networks.
Command and Control	Techniques to communicate with systems under an adversary's control within a victim's network.
Initial Access	Techniques that use various entry vectors to gain an initial foothold within a network.
Credential Access	Techniques used for stealing credentials.
Exfiltration	Techniques used to steal data from your network.
PreAttack/Resource Development	Techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.
Impact	Techniques used to disrupt availability or compromise integrity of a network.
Defence Evasion	Techniques that adversaries use to avoid detection.
Collection	Techniques adversaries use to gather information.
Execution	Techniques that result in adversary-controlled code running on a local or remote system.
Lateral Movement	Techniques used to enter and control remote systems on a network.
Persistence	Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
Reconnaissance	Techniques used to actively or passively gather information that can be used to support targeting.