Attachment A

What is a cyber security vulnerability?
The Australian Cyber Security Centre (ACSC) defines a vulnerability as: *A weakness in a system's security requirements, design, implementation, or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.* (Glossary | Cyber.gov.au). Vulnerabilities can be caused by several factors, including flaws in the underlying software or hardware of a system, or in the way that the system is configured. These vulnerabilities can be exploited by cyber security threats to gain access to information, disrupt the system, and perform other malign activities. Recent threat reporting released by the ACSC indicates that once a vulnerability becomes publicly available, threat actors will aggressively seek to exploit these vulnerabilities – in 21% of cases within 48 hours increasing to 51% over a two-week period. As such, the timely identification and remediation of security vulnerabilities prior to their public release is essential.

What is vulnerability disclosure?
Vulnerability disclosure is the process by which a party who has discovered a vulnerability within a system *discloses* that information to another party.
A common practice within the cyber security community is the responsible disclosure of vulnerabilities, where the party who has identified a vulnerability within a system confidentially advises the owner of the system that a vulnerability exists. Importantly, this provides the system owner an opportunity to remediate the vulnerability (typically through the application of a 'software patch' or changing the system configuration) prior to the vulnerability being made public and providing an opportunity for a cyber threat actor to exploit the system.

How does vulnerability disclosure occur?
Whilst there is general convention on how *responsible disclosure* of vulnerabilities should occur, it is important to note that there is no formal legislative or regulatory process that mandates any specific process. As such, there is no obligation for a party that has discovered a vulnerability to disclose this information to the system owner in a responsible manner – i.e. ahead of its public disclosure, to ensure that the system owner has an opportunity to address the vulnerability.
Public disclosure of vulnerabilities can occur in many forms, notably through a combination of 'official' avenues such as the CVE program (sponsored by the US Department of Homeland Security and Cybersecurity and Infrastructure Security Agency (CISA)) but also potentially through 'unofficial' avenues such as through social media (X, BlueSky, Reddit, etc). Where vulnerabilities have not been responsibly disclosed, and public release has occurred, the effected system is potentially at a very high risk of cyber-attack.

What happens when a vulnerability is disclosed?
The ACSC provides guidance for organizations on how to implement and maintain a Vulnerability Disclosure Program. Within an ACT Government context, this function is fulfilled by the ACT Cyber Security Centre within Digital, Data and Technology Solutions (DDTS).
Upon receipt of a vulnerability disclosure, the ACT Cyber Security Centre conducts a detailed review of the disclosure and conducts a technical risk assessment of the vulnerability. The specific course of action taken to address a vulnerability is determined by several factors including the risk posed by the vulnerability, potential impacts of both its exploitation but also any impacts resulting from any remediation activities, and stakeholders required to conduct remediation activities. The ACT Cyber Security Centre will also notify the respective parties involved in system operation including the relevant ACT Government Directorate(s), and where appropriate, contracted system vendors and service providers. The ACT Cyber Security Centre within DDTS acts as a key facilitator to ensure that security vulnerabilities are identified and addressed, and the risk to ACT Government systems and services is mitigated.

Attachment A

Is there any ACT Government policy on vulnerability disclosure?
Yes, vulnerability disclosure is addressed in the ACT Government Cyber Security Policy, paragraph 18.7. Specifically, this policy directs that: *ACT Public Service staff and contractors must report identified security vulnerabilities directly to DDTS Cyber Security.*
This public facing policy also encourages Security researchers not employed or contracted to ACT Government to perform responsible disclosure by contacting DDTS Directly, or via the effected system owner who will then subsequently notify DDTS.

Why is this important for the ACT Legislative Assembly?
The Legislative Assembly may receive information from members of the public that relate to vulnerabilities within ACT Government systems. For example, Standing Committees may receive public submissions to inquiries. These submissions may contain information on vulnerabilities that may not have been responsibly disclosed to the ACT Government, or to another relevant agency such as the ACSC. Subsequently, these submissions may contain information on vulnerabilities that may be susceptible to exploitation by cyber threats, if adequate disclosure and remediation actions have not been undertaken.
A recent example has illustrated that there is a risk that information relating to active security vulnerabilities that remain unresolved may be inadvertently made public if DDTS has not been afforded an opportunity to manage the vulnerability through a formal vulnerability management process. Whilst in this specific case, the member of the public did conduct a responsible disclosure to DDTS and the ACSC, there is a risk that in future cases this may not occur.

What is recommended to address this risk?
It is recommended that the Legislative Assembly review their processes, policies and procedures and ensure that:

a. Upon receipt of information (via any means including public submissions to inquiries or other possible methods) that explicitly relates, or may relate to, cyber security vulnerabilities in ACT Government systems, that they notify the ACT Cyber Security Centre within Digital, Data and Technology Solutions (DDTS) via email at cyber.security@act.gov.au or via phone on (02) 6207 2038.

b. Prior to publishing information that explicitly relates, or may relate to, cyber security vulnerabilities in ACT Government systems, that they seek validation from the ACT Cyber Security Centre within Digital, Data and Technology Solutions (DDTS) that vulnerabilities have been appropriately addressed and are not able to be exploited by threat actors.