Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

RESPONSIBLE RELEASE PRINCIPLES FOR CYBER SECURITY VULNERABILITIES

The Australian Signals Directorate (ASD) is committed to making Australia the safest place to connect online.

We are proud that our Australian Cyber Security Centre is the nation's premier cyber security authority. Its advice to governments, businesses and families is informed by ASD's other roles, which include gathering foreign intelligence and conducting offensive cyber operations in support of the Australian military.

As part of our work, we sometimes discover security weaknesses or vulnerabilities in technology that are unknown to the vendor and may pose a threat to Australians and Australian systems.

For many years, we have made these vulnerabilities known to vendors so they can patch or otherwise mitigate the threat to their systems and customers.

Our starting position is simple: when we find a weakness, we disclose it.

Occasionally, however, a security weakness will present a novel opportunity to obtain foreign intelligence that will help protect Australians. In these circumstances, the national interest might be better served by not disclosing the vulnerability.

The decision to retain a vulnerability is never taken lightly. It is only made after careful multi-stage expert analysis, and is subject to rigorous review and oversight.

Our decision-making framework is based on a single objective: ensuring the safety and security of Australia and Australians.

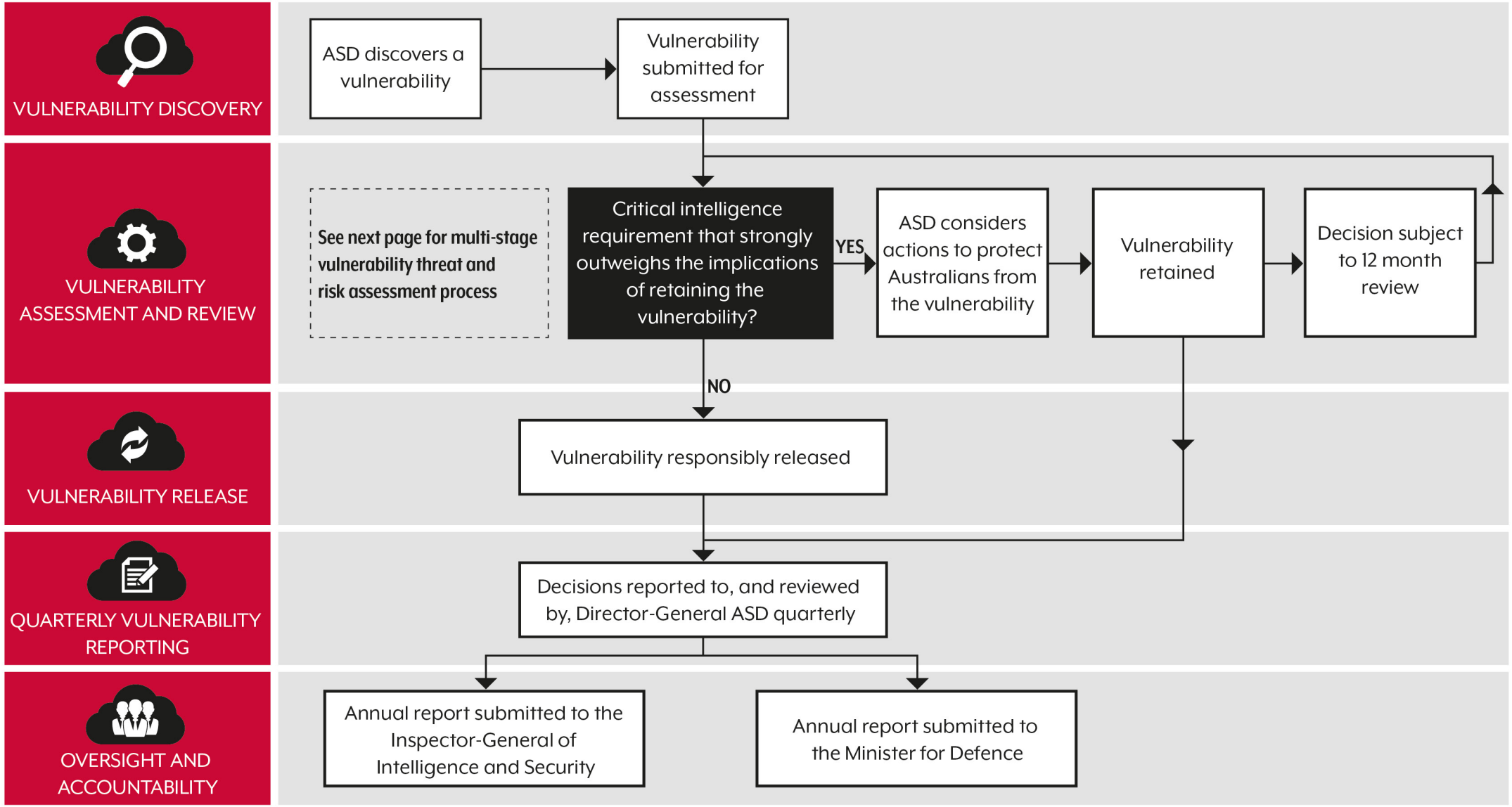
The process is guided by eight essential principles:

1. **Security first.** ASD's default position is to release information on vulnerabilities when we become aware of them. Protecting Australians is our top priority.
2. **The national interest.** We only retain a vulnerability if the national interest in keeping it strongly outweighs the national interest in disclosing it. This might happen if the weakness allows us to gather foreign intelligence that will prevent a terrorist attack, for example.
3. **Assess the risk.** ASD carefully considers the likelihood of a malicious actor being able to take advantage of the weakness. If we assess it is likely a malicious actor will discover and exploit the vulnerability, we will disclose the vulnerability so it can be fixed.
4. **Consider the consequences.** ASD carefully considers the potential impact if the weakness is exploited by a malicious actor. Considerations would include who and what could be affected, and how much damage could be done.
5. **Mitigate the threat.** If a vulnerability is retained, ASD will do all we can to protect Australian systems from being exploited. For instance, we might release security advice that mitigates the weakness.
6. **Responsible release.** ASD works closely with vendors to ensure that patches and other mitigation measures are available before information on a vulnerability is made public.
7. **Regular review.** ASD reviews all vulnerability retention decisions on an on-going basis. We do not 'set and forget'. If the national security imperatives are no longer pressing, we will release the vulnerability.
8. **Rigorous oversight.** All of ASD's vulnerability decisions are subject to independent review by the Inspector-General of Intelligence and Security. ASD submits an annual report covering all vulnerability decisions to the Inspector-General. A copy of this report is also provided to the Minister for Defence.

ASD acts lawfully and ethically. We operate within the letter and the spirit of the law. Australians can be assured that each and every decision about a cyber security vulnerability is made meticulously and in the national interest.

ASD AUSTRALIAN SIGNALS DIRECTORATE

RESPONSIBLE RELEASE FRAMEWORK FOR CYBER SECURITY VULNERABILITIES



ASD AUSTRALIAN SIGNALS DIRECTORATE

Vulnerability threat and risk assessment process