Australian Government
Department of the Prime Minister and Cabinet

Vulnerability disclosure policy

This policy gives security researchers a point of contact to directly submit their research findings if they believe they have found a potential security vulnerability within the Department of the Prime Minister and Cabinet (PM&C).

About this policy

The security of PM&C's systems is a top priority and we take every care to keep them secure. Despite our efforts, there may still be vulnerabilities.

PM&C is keen to engage with the security community. This policy allows security researchers to share their findings with PM&C. If you think you have found a potential vulnerability in a PM&C system, service or product, please tell us as quickly as possible.

We do not provide compensation for finding potential or confirmed vulnerabilities, nor do we publish the names or details of researchers that have provided vulnerabilities.

What this policy covers

This policy covers:

- any product or service wholly owned by PM&C to which you have lawful access
- any product or service wholly owned by one of PM&C's portfolio agencies to which you have lawful access.

This policy does not cover:

- clickjacking
- social engineering or phishing
- weak or insecure SSL ciphers and certificates
- denial of Service (DoS)
- physical attacks
- attempts to modify or destroy data.

How to report a vulnerability

To report a vulnerability, please use PM&C's contact form. Provide enough detail that we can reproduce your steps.

If you report a vulnerability under this policy, please keep it confidential. Do not make your research public until PM&C has finished investigating and fixed or mitigated the vulnerability.

What happens next

PM&C will:

- respond to your report within 5 business days
- keep you informed of our progress
- agree upon a date for public disclosure, if required.