Australian Government

Defence

# DEFENCE VULNERABILITY DISCLOSURE PROGRAM – PUBLIC POLICY

This document is issued for use by the Department of Defence as the publically available policy statement for awareness of the Defence Vulnerability Disclosure Program.



All classified Defence information is protected from unauthorised disclosure and it is an offence to release classified information under the *Criminal Code Act 1995* and the *Privacy Act 1988*.Information contained in Defence publications may only be released in accordance with the Defence Security Principles Framework.

## Introduction

1.1 The Defence Vulnerability Disclosure Program (VDP) expands Defence's cyber security capability to include identification and remediation of ICT vulnerabilities from sources within the organisation and also provides a pathway for external notifications.

1.2 The concept of the VDP works under the assumption that individuals will often come to acquire knowledge of vulnerabilities that have not been detected by other processes.

1.3 Increased visibility of vulnerabilities can better inform risk management processes, and therefore contribute to better security outcomes.

## Objective

1.4 The objective of the Defence Vulnerability Disclosure Program is to reduce residual ICT system risk levels by empowering individuals to appropriately report vulnerabilities, whilst complying with relevant ISM controls and Defence VDP policy.

1.5 The Defence Vulnerability Disclosure Program is intended to solicit constructive communication from internal Defence and external parties regarding ICT vulnerabilities that exist within Defence-owned/operated/managed ICT and OT systems and environments.

1.6 The implementation of a Vulnerability Disclosure Program is mandated by the Australian Government Protective Security Policy Framework (PSPF) and is expanded upon through Information Security Manual (ISM) controls. The PSPF requires that all non-corporate Commonwealth entities must operate a Vulnerability Disclosure Program.

## Scope

1.7 This document outlines the parameters of disclosure of Defence related vulnerabilities from external sources.

## Audience

1.8 This document applies to Defence staff, contractors, service providers and the public who utilise Defence systems, or, who wish to report vulnerabilities that have become known to them.

## Prohibited Vulnerability Research

1.9 All research and discovery of vulnerabilities must be conducted ethically with regard to the safe and secure operation of the service or platform.

1.10 Active assessment methods of research of Defence IT and OT capabilities are strictly prohibited. This policy does not authorise any entity to conduct active assessment of any capability such as penetration testing activities against Defence systems.

1.11 The following types of research are strictly prohibited:

(1) Attempting to modify or destroy any data.

(2) Attempting to exploit a vulnerability.

(3) Executing or attempting to execute a denial of service (DOS/DDOS) attack against Defence.

(4) Conducting social engineering of Department of Defence employees, contractors or any other party.

(5) Accessing or attempting to access Defence IT or OT access accounts or data.

(6) Posting, transmitting, uploading, and linking to, sending or storing malware, viruses or similar harmful software that could impact Defences systems or services.

(7) Committing a data breach under any circumstances.

(8) Physical attacks.

(9) Using automated vulnerability scanners, penetration testing software, network scanners and the like against Defence systems or services.

(10) Any activity that violates any user policy, system policy, acceptable use policy or any Australian or International law.

Engaging in conduct of the type listed in this section may expose individuals to penalties, including criminal prosecution and imprisonment.

**Vulnerability Disclosure Report**

1.12 Vulnerability disclosure reports from external sources may be submitted via the: Defence Vulnerability Disclosure (Online Form Link) under the ‘Contact us’ heading on Defence’s public facing web presence.

1.13 The following details will be required in the report:

(1) System or environment that contains the vulnerability.

(2) Specifics of the vulnerability.

(3) Brief assessment of the risk posed by the vulnerability.

(4) The name (or alias) and contact details of the reporter (optional).

(5) Any other information that would assist Defence in locating and investigating the vulnerability.

1.14 To allow Defence to effectively and appropriately respond, reporters are requested to avoid public disclosure of vulnerabilities found within a Defence systems, websites or applications.

1.15 Defence may provide feedback to reporters where possible however, this should not be an expectation.

**Recognition of Reporting**

1.16 Defence does not provide public recognition or reward to reporters who identify potential or confirmed security vulnerabilities