Australian Government
Civil Aviation Safety Authority

External Security Vulnerability Disclosure Program

November 2023

Acknowledgement of country

The Civil Aviation Safety Authority (CASA) respectfully acknowledges the Traditional Custodians of the lands on which our offices are located and the places to which we travel for work. We also acknowledge the Traditional Custodians' continuing connection to land, water and community. We pay our respects to Elders, past and present.

Inside front cover artwork: James Baban.

Document number	CASA-03-6682
Version	1.0 – November 2023
Approval Tier	Three
Owner	Inderpal Walia
Responsible Area Manager	Anthony Warnock

This document becomes an uncontrolled document when printed. Refer to <Document Catalogue> for current version.

The material contained in this document is provided for general information only and should not necessarily be relied upon for the purpose of a particular matter. Those using the document as a reference should always exercise their own judgement with respect to the use of this document and carefully evaluate the accuracy, currency, completeness and relevance of the information in this document for their purposes. Refer to the relevant legislation to ascertain the requirements of, and the obligations imposed by or under, the law.

Contents

Glossary

Acronyms and abbreviations

Acronym / abbreviation	Descriptions
CASA	Civil Aviation Safety Authority
PSPF	Protective Security Policy Framework
VDP	Vulnerability Disclosure Program

Reference material

Document type	Title
Legislative Framework	Protective Security Policy Framework (PSPF) Policy 11
Guidance	Vulnerability Disclosure Programs Explained | Cyber.gov.au
Internal	Vulnerability Management and Disclosure Plan (RMS # D23/125255)

Revision history

Revisions to this Standard Operating Procedure are recorded below in order of most recent first.

Version no	Date	Parts / sections	Details
1.0	Nov 2023		Develop the document

1. Purpose

As per the PSPF Policy 11 requirement, a Vulnerability Disclosure Program (VDP) should be implemented by CASA to establish a structured and responsible framework through which security researchers, ethical hackers, and other individuals can report identified security vulnerabilities in CASA's digital assets.

2. Scope

This program emphasizes the procedure and guidance that applies to the security researchers, ethical hackers and other individuals that need to report a potential security vulnerability to CASA.

3. Responsibilities

All participants (security researchers, ethical hackers, and other individuals) must act/comply with External Security Vulnerability Disclosure program and the defined procedure.

4. Procedure

Our priority is to ensure the online security of our systems, and we take every possible precaution to protect them. However, despite our diligence, there remains a possibility a vulnerability may exist.

We welcome collaboration with the security community and the public, and we have established a security vulnerability disclosure program that facilitates the responsible sharing of any findings with us. If you find a vulnerability in one of our systems, please inform us as quickly as possible.

We do not offer rewards such as money for discovering and reporting vulnerabilities. We will provide public acknowledgement and thanks if you consent to being publicly identified.

Please note that our program does not grant permission for conducting security testing or operations against CASA. If you suspect a vulnerability, please inform us, and we will manage the necessary testing and verification procedures.

4.1 What Program Covers

Our security vulnerability disclosure program covers:

- Any product or service that is operated by CASA and which you have legitimate need to access.
- Any product, service, and infrastructure that we share with service partners, and which you have legal authorization to access.
- Any services that are owned by third parties but utilized as a component of our services, and to which you have a legitimate need to access.

Under this program, you must not:

- Engage in physical testing of government facilities or services.
- Leverage deceptive techniques, such as social engineering, against CASA employees, contractors, or any other party.
- Execute resource exhaustion attacks, such as DOS (denial of service) or DDOS (distributed denial of service).
- Utilize automated vulnerability assessment tools.
- Introduce malicious software or harmful software that could impact our services, products, customers or any other party.

- Engage in unlawful or unethical behaviour.
- Engage in reverse engineering of CASA products or systems.
- Modify, destroy, exfiltrate, or retain data stored by the CASA.
- Provide deceptive, inaccurate, or hazardous information to CASA system.
- Attempt to access accounts or data that you are not authorized to do.
-

We ask that you do not disclose vulnerability information publicly. We also ask that you do not report security vulnerabilities relating to missing security controls or protections that are not directly exploitable. Examples include:

- SSL (secure sockets layer) or TLS (transport layer security) certificates that are weak, insecure, or misconfigured.
- DNS (domain name system) records that are misconfigured, including but not limited to SPF (sender policy framework) and DMARC domain-based message authentication reporting and conformance).
- Missing security HTTP (hypertext transfer protocol) headers (such as permissions policy).
- Theoretical cross-site request forgery and cross-site framing attacks.

For more information about our processes for handling vulnerability reports, contact us at vulnerability reporting portal.

If you believe you have discovered a vulnerability in any of our systems, you can report it to us through our vulnerability reporting portal.

In your report, please provide as much information as you can so we can recreate the steps you took to find the vulnerability:

- A description of the security vulnerability and its impact.
- The systems, users and services that may be affected (where possible).
- Potential steps to mitigate vulnerability.

4.2 What to Report?

Please report any cyber security vulnerabilities you discover in our systems. The systems covered by our security vulnerability disclosure program are:

- Any system that is owned by us.
- Any system, service, and infrastructure that we offer to industry members and stakeholders.
- Any services we offer through a third-party system.

4.3 What Happens Next?

We take all vulnerability reports seriously. We will stay in contact with you about the issue during and after our investigation into it. We may request further information if required, periodically update you about our progress on fixing it, and notify you when the vulnerability has been rectified. We will publish the contributor’s name who have identified the vulnerability, with the permission of the originator.