Australian Government
Civil Aviation Safety Authority

External Security Vulnerability Disclosure Program

July 2025

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.

Version	2.0 – July 2025

This document becomes an uncontrolled document when printed.

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

Acronyms and abbreviations

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

Reference material

Document type	Title
Policy Framework	Protective Security Policy Framework (PSPF)
Guidance	Information Security Manual (ISM)
Guidance	Vulnerability Disclosure Programs Explained | Cyber.gov.au

Revision history

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

Version no	Date	Parts / sections	Details
2.0	June 2025	All	Updated following changes to documentation, aligned with PSPF 2024 release.
1.0	Nov 2023		Develop the document

1. Purpose

As per the PSPF a Vulnerability Disclosure Program (VDP) must be implemented by CASA, it is a set of processes and guidelines for identifying, verifying, fixing, and reporting security vulnerabilities, whether they come from internal or external sources. This document satisfies the External Vulnerability Disclosure element of the requirement.

CASA welcomes collaboration with the security community and the public, this Program facilitates the responsible sharing of findings with us. CASA recognise the valuable role that security researchers, ethical hackers and other external entities play in improving our security posture.

This document outlines how to report potential security vulnerabilities, what information is required and CASA's commitment to responding to those reports.

2. Scope

Our External Security Vulnerability Disclosure Program applies to:

- 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 authorisation to access.
- Any services that are owned by third parties but utilised as a component of our services, and to which you have a legitimate need to access.

All CASA systems are listed on this webpage: www.casa.gov.au/resources-and-education/our-systems.

3. Your Responsibilities

Please note that our program does not grant permission for conducting security testing or operations against CASA. Under this program, any participant must not:

- Engage in physical testing of government facilities or services.
- Leverage deceptive techniques, such as phishing or social engineering.
- Execute resource exhaustion attacks, such as denial of service or distributed denial of service.
- Utilise automated vulnerability assessment, exploitation or penetration testing tools.
- Introduce malicious 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 CASA.
- Provide deceptive, inaccurate, or hazardous information to CASA system.
- Attempt to gain unauthorised access accounts or data.

CASA request that you do not:

- Disclose vulnerability information publicly.
- 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.
  - Misconfigured DNS (domain name system) records, such as 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.

4. Recognition

We value collaboration and look to facilitate responsible sharing of findings.

If your report leads to a valid security fix or identification of vulnerability in any CASA-owned system, and you consent, we will recognise and publicly thank you for your efforts.

CASA do not offer monetary rewards or a bug bounty initiative.

5. Vulnerability Disclosure

CASA's priority is to ensure the security of our systems, and every practicable precaution is taken to protect them. Despite our diligence, there remains a possibility that a vulnerability may exist. If you believe you've found a vulnerability in our systems, we want to hear from you. You can report it to us through our vulnerability reporting portal.

This section provides guidance on making a report.

5.1 What to Report

In your report, please provide relevant information to enable recreation of the steps you took to find the vulnerability. Appendix A outlines the Vulnerability Reporting Portal form fields, below are the details of mandatory fields.

Contact Details

If you wish to be contacted provide details to any of the optional fields including: name, phone, email number.

Details of vulnerability

System or software information

Provide details of the system affected, including:

- System name, version number
- IP or URL
- Your device details including: device type, OS, etc.

Further Information

Provide information regarding the vulnerability including:

- A description of the security vulnerability and its impact.
- Steps to replicate your discovery of the vulnerability.
- Potential steps to mitigate vulnerability.
- Proof-of-concept code (where applicable)
- Names of any test accounts you have created (where applicable)

Policy consent

Provide your consent to agreeing with this program. Failing to do so will prevent submission of the report.

5.2 When to Report

Following discovery of a vulnerability of a system outlined in Section 2 Scope and collection of information satisfy the requirements of 5.3 How to Report, please submit your report as soon as possible.

5.3 How to Report

Report any cyber security vulnerabilities you discover in our systems through our vulnerability reporting portal, located at the following URL:

https://www.casa.gov.au/about-us/contact-us/report-system-vulnerability

5.4 Vulnerability Assessment and Treatment

CASA will assess and treat the vulnerability report in accordance internal CASA procedures. Following replication and confirmation, appropriate remediation and/or mitigative measures will be implemented.

You will be notified of progress during this stage. CASA may request further information from you if required.

5.5 Outcome Notification and Publishing of Findings

Following Vulnerability Assessment and Treatment, CASA will notify you of the outcome. Pending your permission, your name will be published in public recognition of your discovery of the vulnerability.

Appendix A – External Vulnerability Disclosure Form

Contact Details	
Given name	
Family name	
Phone	
Email	
What is the enquiry about?	
Details of vulnerability	
System or Software information	
Further Information	
Consent	