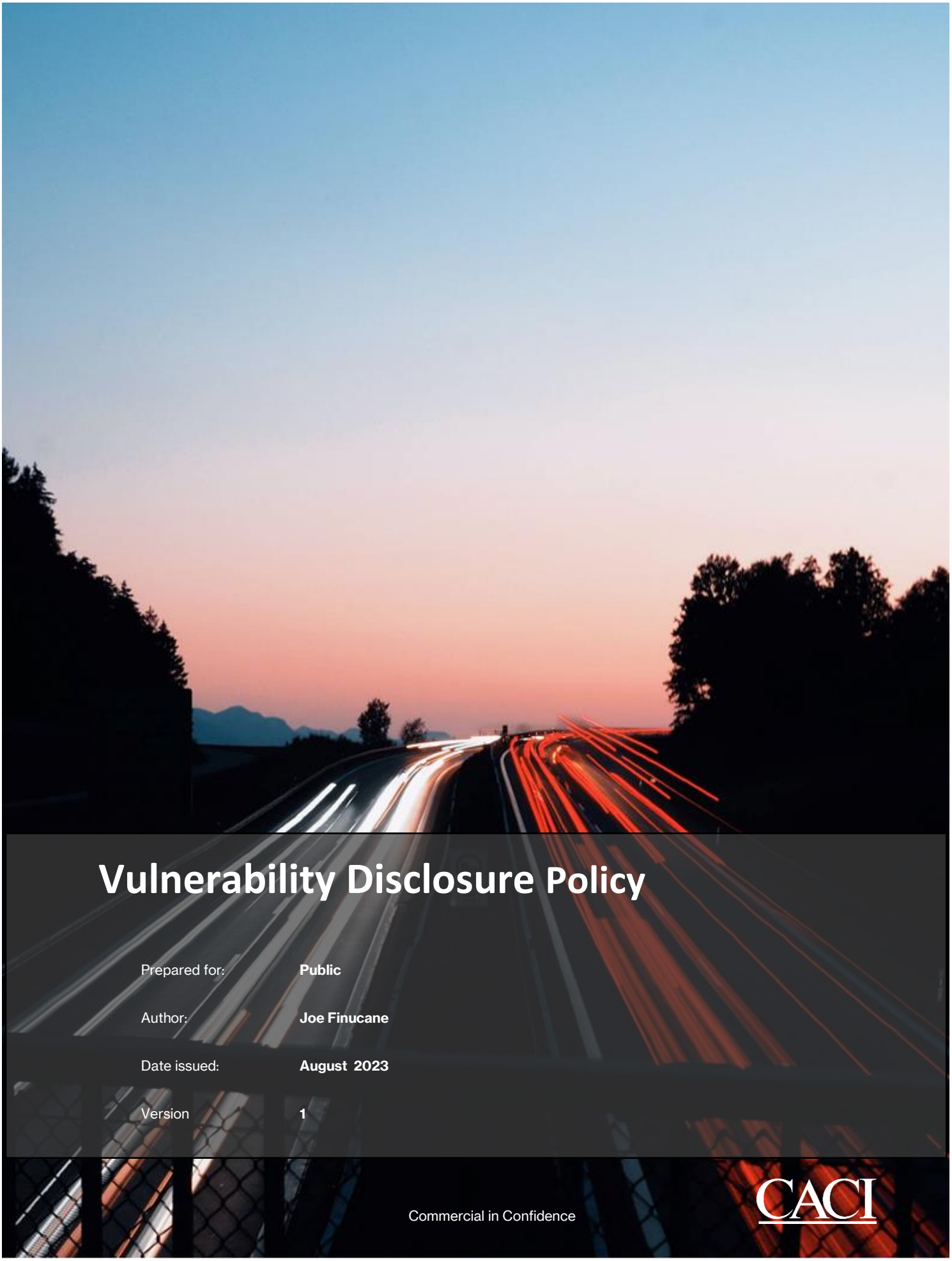

Vulnerability Disclosure Policy

Prepared for:	**Public**
Author:	**Joe Finucane**
Date issued:	**August 2023**
Version	**1**

Commercial in Confidence

CACI

Document Control

This section details document control in terms of its distribution, configuration management, amendment history and authorisation.

Amendment History

Note this is a live document and is subject to regular updates to reflect the latest changes to corporate policies.

Version	Author & Owner	Date	Changes
1	Joe Finucane	23/08/2023	New draft document

Contact Information

Owner/Writer	Department	Telephone Number
Joe Finucane	Technology Department	+44 (0) 20 7605 6003
Nigel Scott	Technology Department	+44 (0) 121 788 5964
Sean O'Brien	Technology Department	+44 (0) 20 7605 6146

Definitions/References

Terms	Definitions

Contents

Introduction

We value the security of our systems and services and recognize the importance of individual security researchers in helping keep our customers and suppliers safe. This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (“CACI Ltd"). We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: discloure@caci.co.uk. For secure communications, we recommend encrypting your email with our public PGP key which can be found here: Link to CACI website with public key.

In your report, please include details of:

- The website, IP or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example, “XSS vulnerability”.
- Steps to reproduce the issue (proof-of-concept scripts or detailed procedures are helpful).
- Any possible mitigations or workarounds you're aware of.
- Your contact details for further communication.

These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

Disclaimer: In regards to the above, please note the following:

- Do not upload screenshots, videos, or exploit code to a publicly accessible server/repository in preparation of your email..
- Do not zip or archive your files (just attach them directly to the email).
- Very low quality reports such as those which only contain automated output will be rejected.

In Scope Systems and Services

Any CACI Ltd-owned web service that handles sensitive user data is intended to be in scope. This includes:

CACI hosted web apps.

CACI owned Web domains, such as:

- *.caci.co.uk
- *.areadata.co.uk
- *.caci-csg-servicesportal.co.uk
- *.caci-im.net
- *.caci.uk
- *.caciseminar.co.uk
- *.data-ace.info
- *.doncasterccm.co.uk
- *.ecustomerservices.info
- *.insite.info
- *.invocom.net
- *.none.cacisurveys.com
- *.socialsoftware.co.uk
- *.sophronconsulting.co.uk

Out of Scope Systems and Services

Any third party website or system.

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress. Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate public release with us.

Guidance

You must NOT:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in the CACI's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt the CACI's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, ‘phish’ or physically attack CACI's staff or infrastructure.

You must:

- Always comply with data protection rules and must not violate the privacy of the CACIs users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause CACI Ltd or partner organisations to be in breach of any legal obligations.

.