Office of Information Technology (OIT)

Vulnerability Disclosure Policy

[BOD 20-01]

January 23, 2023

` Document History

Version Number	Release Date	Summary of Changes	Section/ Page	Changes Made By
1.0	02/18/2021	Initial version for the Development Finance Corporation (DFC)	N/A	Michael Goulding
1.1	01/12/2023	Annual Review	All	Trevor Lowing
1.2	01/23/2023	Added policy expansion per CISA.	6	Trevor Lowing

Approval

This policy has been approved and issued under the authority granted to the Vice President Office of Information Technology (OIT)/Chief Information Officer (CIO) in accordance with DFC Office Function Directives-IT, Directive OD-13 Other Internal Rules, Handbooks, Template; and the Federal Information Security Modernization Act (FISMA) of 2014.

TREVOR LOWING

Digitally signed by TREVOR LOWING
DN: c=US, o=U.S. Government, ou=U.S. International Development Finance Corporation, cn=TREVOR LOWING, 0.9.2342.19200300.100.1.1=71051004729021
Date: 2023.01.25 07:36:28 -05'00'

DFC Chief Information Security Officer (CISO) Date

Table of Contents

Introduction

The Development Finance Corporation (DFC) is committed to ensuring the security of the American public by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized we will work with you to understand and resolve the issue quickly, and DFC will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information (PII), financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Test methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing
- Test any system other than the systems set forth in the 'Scope' section below,
- Introduce malicious software,
- Test in a manner which could degrade the operation of DFC systems; or intentionally impair, disrupt, or disable DFC systems,
- Test third-party applications, websites, or services that integrate with or link to or from DFC systems,
- Delete, alter, share, retain, or destroy DFC data, or render DFC data inaccessible, or,
- Use an exploit to exfiltrate data, establish command line access, establish a persistent presence on DFC systems, or "pivot" to other DFC systems.

Scope

The following systems / services are in scope:

- "This policy applies to all DFC-managed systems and services that are accessible from the Internet. This includes the registered domain name (DFC.gov)."

Any services not explicitly listed above are excluded from scope. Additionally, vulnerabilities found in non-federal systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to its disclosure policy (if any).

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at ciso@dfc.gov before starting your research (or at the security contact for the system's domain name listed in the .gov WHOIS).

Though we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely DFC, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We do not support PGP-encrypted emails. For particularly sensitive information, submit through https://www.dfc.gov/vulnerability-disclosure-policy

What we would like to see from you

To help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be sent to ciso@dfc.gov. We also invite you to contact us with suggestions for improving this policy.