Vulnerability Disclosure Policy – Federal Aviation Administration

Introduction

The Federal Aviation Administration's continuing mission is to provide the safest, most efficient aerospace system in the world. In support of the missions, FAA works to ensure a security conscious posture of FAA-operated information systems to maintain confidence in FAA from the American public. 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 and appreciate your support in correcting vulnerabilities in FAA 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 FAA 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 have established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, 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.**

Research and Test Methods

Testing methods authorized include examination of unique technology deployments including custom code and testing of procedural actions within custom code functional areas.

The following test methods are not authorized:

- Testing any system other than the systems set forth in the 'Scope' section below;
- Disclosing vulnerability information, except as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below;
- Conducting network denial of service (DoS or DDoS) tests or other tests that impair access, degrade operational capability to or damage a system or data;
- Executing physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing;
- Deploying attacks against underlying technology that are published or known in industry areas;
- Using general scanning capabilities that scan for common vulnerabilities or exploits
- Testing third-party applications, websites, or services that integrate with, connect or link to or from, FAA systems;

- Deleting, altering, sharing, retaining, or destroying FAA data or information, or rendering FAA data or information inaccessible; or
- Using an exploit to exfiltrate data or information, establishing command line access, establishing a persistent presence on FAA systems, or pivot to other FAA systems.

Scope

This VDP applies to the following systems and services. Any services not explicitly identified here are considered out-of-scope and are not authorized for testing. The scope of FAA assets subject to this policy will be updated regularly.

- All Federal Aviation Administration operated websites are in scope of this VDP.
- FAA operated sites will contain an FAA specific Vulnerability Disclosure Program link that may vary from the general FAA VDP scope.
- Sites and services that are accessed where FAA does not directly manage, affiliated to FAA mission, and operated through agreements with entities external to FAA are outside of the FAA VDP scope.

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 FAA, 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 your express permission.

FAA does not provide payment for vulnerability submissions and, by submitting a vulnerability report, you acknowledge that you have no expectation of payment and that you expressly waive any future payment claims against the U.S. Government related to your submission. Additionally, FAA will not provide any type of recognition for disclosed vulnerabilities.

We accept vulnerability reports at via vulnerabilitydisclosure@faa.gov. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 14 business days.

We do not support PGP-encrypted emails. For particularly sensitive information, please use a legitimate email address for consideration through email to vulnerabilitydisclosure@faa.gov.

By submitting a vulnerability report to FAA, researchers warrant the report and any attachments do not violate the intellectual property rights of any third party, and the submitter grants FAA a non-exclusive, royalty-free, world-wide, perpetual license to use, reproduce, create derivative works, and publish the report and any attachments.

What we would like to see from you

In order 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 ;
- Include the date you discovered the vulnerability;
- Offer a detailed description of the steps and tools needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful); and
- Be submitted in in English.

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 three (3) business days, we will acknowledge that your report has been received when a legitimate email address is used for submission
- 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.

Disclosure

FAA is committed to timely correction of vulnerabilities. We recognize that public disclosure of a vulnerability in the absence of a readily-available

corrective action likely increases versus decreases risk. Accordingly, we require that reporters of vulnerabilities refrain from public disclosure for a minimum of 90 calendar days from the date FAA acknowledges receipt of the report. In some cases, we may ask for an additional delay in public disclosure. **To the extent consistent with applicable law**, FAA, generally, will not publicly disclose vulnerabilities identified in its systems, even once remediated.

Privacy

This statement is provided pursuant to the Privacy Act of 1974, 5 USC § 552a: Vulnerability reports are solicited under the authority of Binding Operational Directive 20-01. The principal intent for the collection of information submitted is to identify and evaluate potential vulnerabilities to FAA's internet-connected services and systems. Contact information collected from the submission of vulnerability reports will be included in a Privacy Act System of Records known as DOT/ALL 16 titled, "Mailing Management System" and will be subject to the routine uses published. Provision of the requested information is voluntary; however, failure to furnish the requested information may result in an inability of FAA to evaluate the submitted vulnerability report. FAA may use contact information provided in vulnerability reports to follow-up with the submitter and contact information may be shared with contractors and other federal agencies assisting FAA with remediation of vulnerabilities.

FAA respects your right to privacy and will protect it when you visit our website in accordance with the FAA Privacy and Website Policy.

Questions

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