Vulnerability Disclosure Policy

Federal Aviation Administration

March 1, 2021

Introduction

The Federal Aviation Administration's (FAA's) continuing mission is to provide the safest, most efficient aerospace system in the world. In support of that mission, the FAA is committed to maintaining the security of FAA systems and protecting sensitive data and information from unauthorized disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey the procedures and conditions associated with submitting discovered vulnerabilities to the FAA in support of strengthening the FAA's systems.

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

The FAA is looking for suggestions to improve the FAA's information systems' security posture, including reporting potential system vulnerabilities.

Authorization

If you make a good faith[1] effort to comply with this policy during your security research, the FAA will consider your research to be authorized, work with you to understand and resolve the issue quickly, and will not recommend or pursue legal action related to your research conducted pursuant to this policy. Should a third party initiate legal action against you for activities conducted in accordance with this policy, the FAA will make this authorization known.

Guidelines

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

- Notify the FAA immediately after you discover a real or potential security issue.
- Comply with the Test Methods section of this policy.

[1] Good faith means security research conducted with the intent to follow the FAA's VDP without malicious motive. The FAA may evaluate an individual's intent by taking into account all relevant facts and circumstances, including but not limited to: their actions, their statements, and the results of their actions. In other words, good faith security research means accessing a computer or software within the scope of this policy solely for the purpose of testing or investigating a security flaw or vulnerability and disclosing those findings in alignment with this policy. The security researcher's actions should be consistent with an attempt to improve security and to avoid doing harm, whether by unwarranted invasions of privacy, causing damage to property, compromising safety, or by other means.

A hallmark of good faith activity is a factual, timely report of a vulnerability on a system authorized for testing, sent directly to the FAA in accordance with this policy's instructions; however, a person could conduct research in good faith and have no reportable findings. In contrast, an individual who consciously decides to test systems that are not included within the scope of this policy would not be acting in good faith.

- Provide the Agency, at minimum 90 days, 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 or information (including personally identifiable information, financial information, proprietary information or trade secrets of any party, or information indicating a potential aviation safety or security hazard), **you must stop your test, notify the FAA immediately, not disclose this data or information, as applicable, to anyone else, and purge any stored FAA sensitive data and information from your systems immediately after reporting a vulnerability.**

Test Methods

Security researchers must not:

- Test any system other than the systems set forth in the 'Scope' section below;
- Disclose vulnerability information, except as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below;
- Engage in physical testing of facilities or resources;
- Engage in social engineering;
- Send unsolicited electronic mail to FAA users, including "phishing" messages;
- Execute or attempt to execute "Denial of Service" or "Resource Exhaustion" attacks;
- Introduce malicious software;
- Test in a manner that could degrade the operation of FAA systems, or intentionally impair, disrupt, or disable FAA systems;
- Test third-party applications, websites, or services that integrate with, or connect or link to or from, FAA systems;
- Delete, alter, share, retain, or destroy FAA data or information, or render FAA data or information inaccessible, or;
- Use an exploit to exfiltrate data or information, establish command line access, establish a persistent presence on FAA systems, or pivot to other FAA systems.

Security researchers may:

- View or store FAA sensitive data or information only to the extent necessary to document the presence of a potential vulnerability for reporting to the FAA. As stated below, you must purge any stored FAA sensitive data and information from your systems immediately after making your report to the FAA.

Security researchers must:

- Avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data or information.
- Only use exploits to the extent necessary to confirm a vulnerability's presence and consistent with the "Security researchers must not" provisions of this section.
- Cease testing and notify the FAA immediately upon discovery of a vulnerability;
- Cease testing and notify the FAA immediately upon discovery of an exposure of sensitive data or information; and,
- Purge any stored FAA sensitive data and information from your systems immediately after reporting a vulnerability.

Scope

This policy applies to the following FAA systems and services:

- www.faa.gov

Any system or service not expressly listed above, such as any integrated, connected or linked services, is excluded from scope and is not authorized for testing. Additionally, vulnerabilities found in systems from FAA vendors fall outside of this policy's scope. Before you conduct any security research on a vendor system, you must first visit the vendor's website for information on the vendor's vulnerability disclosure policy and report any vulnerabilities in the vendor's systems directly to the vendor according to its vulnerability disclosure policy. If you are not sure whether a system is in scope or not, contact the FAA at *vulnerabilitydisclosure@faa.gov* before starting your research.

Though the FAA develops and maintains other internet-accessible systems and services, the FAA requires that *active research and testing* only be conducted on the systems and services covered by the scope of this document. The following systems and services are currently within scope: www.faa.gov.

If there is a particular system or service not in scope that you think merits testing, please contact the FAA.

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 may affect other users of a product or service and not solely the FAA, the FAA may share your report with the Cybersecurity and Infrastructure Security Agency (CISA), where it will be handled under their coordinated vulnerability disclosure process. The FAA may also share your report with any affected vendors or open source projects, and the Transportation Security Administration (TSA), with which the Department of Transportation, including the FAA, shares responsibility for the aviation sub-sector of the Transportation Systems critical infrastructure sector*. The FAA will not share your name or contact information without your express permission.*

Note the 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 the FAA will not provide any type of recognition for disclosed vulnerabilities.

The FAA accepts vulnerability reports at *vulnerabilitydisclosure@faa.gov*. Reports may be submitted anonymously. If you share contact information, receipt of your report will be acknowledged within three business days.

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

What the FAA would like to see from you

In order to help triage and prioritize submissions, the FAA suggests that reports:

- Describe the vulnerability discovered, including its location and the potential impact of exploitation.
- Include the date you discovered the vulnerability.
- Provide a detailed technical description of the steps required to reproduce the vulnerability, including a description of any tools needed to identify or exploit the vulnerability.
- Identify any Common Vulnerabilities and Exposures (CVE) associated with the vulnerability.
- Images, e.g., screen captures, and other documents may be attached to reports. It is helpful to give attachments illustrative names.
- Reports may include proof-of-concept code that demonstrates exploitation of the vulnerability. The FAA requests that any scripts or exploit code be embedded into non-executable file types, including file archives.
- Be in English, if possible.

What you can expect from FAA

When you choose to share your contact information, the FAA commits to coordinating with you as openly and as quickly as possible.

- Within three business days, the FAA will acknowledge that your report has been received.
- When possible, the FAA will confirm the existence of the vulnerability to you and be as transparent as possible about the steps taken during the remediation process, including on issues or challenges that may delay resolution.
- The FAA will maintain an open dialogue to discuss issues.

Disclosure

The FAA is committed to timely correction of vulnerabilities and recognizes that public disclosure of a vulnerability in the absence of a readily-available corrective action likely increases versus decreases risk. Accordingly, the FAA requires that reporters of vulnerabilities refrain from public disclosure for a minimum of 90 calendar days from the date the FAA acknowledges receipt of the report. In some cases, the FAA may ask for an additional delay in public disclosure. **To the extent consistent with applicable law**, the FAA, generally, will not publicly disclose vulnerabilities identified in its systems, even once remediated.

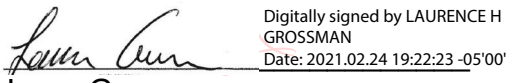
Privacy

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 principle purpose for which the information is intended to be used 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 the FAA to evaluate the submitted vulnerability report. The 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 the FAA with remediation of vulnerabilities. The FAA may also share contact information with CISA and TSA to assist in the cybersecurity activities of those agencies.

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

Questions

Questions regarding this policy may be sent to ***vulnerabilitydisclosure@faa.gov***. The FAA encourages security researchers to contact the FAA to request clarification on any element of this policy. Please contact the FAA prior to conducting research if you are unsure if a specific test method is inconsistent with or unaddressed by this policy. The FAA also invites you to provide suggestions for improving this policy.



Larry Grossman
FAA Chief Information Security Officer (CISO)

Document change history

Version	Date	Description
1.0	*March 1, 2021*	First issuance.