

Federal Energy Regulatory Commission

Vulnerability Disclosure Policy (VDP)



March 1, 2021

Federal Energy Regulatory Commission
Cybersecurity and Information Assurance Division
888 1st Street NE
Washington, DC 20426

Document Control

This is a controlled document produced by the Federal Energy Regulatory Commission (FERC). The control and release of this document is the responsibility of the document owner. This includes any amendment that may be required.

Document Control	
Date	March 1, 2021
Author	Lisa Guevara
Document Title	Vulnerability Disclosure Policy (VDP)

Customer Details	
Name	Eric Rippetoe
Office/Region	Federal Energy Regulatory Commission, Washington, DC 20426
Contact Number	202-502-6097
E-mail Address	Eric.Rippetoe@ferc.gov

Revision History			
Issue	Date	Author	Comments
0.1	February 15, 2021	Lisa Guevara	DRAFT/Original Release
1.0	March 1, 2021	FERC	Official Release

1. INTRODUCTION

The Federal Energy Regulatory Commission (FERC) is committed to ensuring the security of the American public by protecting their information. As such, the FERC has created a Vulnerability Disclosure Policy. Vulnerability Disclosure is the “act of initially providing vulnerability information to a party that was not believed to be previously aware.” The individual or organization that performs this act is called the researcher. The FERC Vulnerability Disclosure Policy is intended to give security researchers clear guidelines on the following:

- Conducting vulnerability discovery activities on FERC systems;
- What systems and types of research are covered under this policy;
- What researchers can expect from the Commission;
- What the Commission expects from researchers, including how long researchers should wait before publicly disclosing vulnerabilities;
- Steps for disclosing vulnerabilities to the Commission, and how to send the vulnerability reports;

The FERC encourages researchers to contact the Commission to report potential vulnerabilities in the FERC systems. This program allows researchers to alert FERC on security flaws they identify within the FERC public-facing websites. Feedback received through this program allows the FERC to remediate flaws quickly when possible, thereby, strengthening the integrity of the organization information technology systems and enhancing protection of government-owned data.

2. BACKGROUND

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Vulnerabilities are often found in individual software components, in systems comprised of multiple components, or in the interactions between components and systems. They are typically exploited to weaken the security of a system, its data, or its users, with impact to their confidentiality, integrity, or availability. The primary purpose of fixing vulnerabilities is to protect people, maintaining or enhancing their safety, security, and privacy.

3. AUTHORIZATION

If researchers make a good faith effort to comply with this policy during their security research, the Commission shall work with researchers to understand and resolve the issue quickly. Should legal action be initiated by a third party against researchers for activities that were conducted in accordance with this policy, the Commission shall make this authorization known.

- A Binding Operational Directive (BOD) is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1).
- The Department of Homeland Security (DHS) develops and oversees the implementation of BODs pursuant to the Federal Information Security Modernization Act of 2014 (“FISMA”). Id. § 3553(b)(2).

- Federal agencies are required to comply with these DHS-developed directives. Id. § 3554(a)(1)(B)(ii). DHS binding operational directives do not apply to statutorily defined “National Security Systems” or to certain systems operated by the Department of Defense or the Intelligence Community. Id. § 3553(d)-(e)

4. GUIDELINES

Under this policy, “research” means activities in which researchers must:

- Notify the FERC as soon as possible after researcher(s) 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 the FERC a reasonable amount of time to resolve the issue before researchers disclose it publicly; and
- Do not submit a high volume of low-quality reports.

Once researchers 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), researcher(s) must stop the test, notify the FERC immediately, and not disclose this data to anyone else. (Please refer to *Section 7 – Reporting a Vulnerability* for procedures on how to submit the vulnerability.)

5. TEST METHODS

Typical Vulnerabilities Accepted:

- OWASP Top 10 Vulnerability categories
- Other vulnerabilities with demonstrated impact.

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.

6. SCOPE

This policy applies to the following systems and services:

- www.ferc.gov and its subdomains
- www.eLibrary.ferc.gov and its subdomains
- All other Commission applications are excluded from this policy

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 researchers are not sure of the FERC systems in scope, contact the FERC at vdpfeedback@ferc.gov before starting the research (or at the security contact for the system's domain name listed in the Vulnerability Disclosure Mailbox).

Though the FERC develops and maintains other internet-accessible systems or services, the Commission asks that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a system not in scope that researchers think merits testing, please contact the FERC to discuss it first. The Commission shall increase the scope of this policy over time.

7. REPORTING A VULNERABILITY

Information submitted under this policy shall be used for defensive purposes only – to mitigate or remediate vulnerabilities. If the FERC findings include newly discovered vulnerabilities that affect all users of a product or service and not solely the FERC assets, the may share the report with the Cybersecurity and Infrastructure Security Agency, where it shall be handled under their [coordinated vulnerability disclosure process](#). FERC shall not share your name or contact information without express permission. FERC accepts vulnerability reports via vdpfeedback@ferc.gov. Reports may be submitted anonymously. If researchers share contact information, the Commission shall acknowledge receipt of researchers report within 3 business days.

7.1 What FERC Would Like to See from Researchers

In order to help FERC triage and prioritize submissions, the Commission recommends that the researcher reports:

- Describe the location where 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); and
- Provide the information in English.

7.2 What Researchers Can Expect from FERC

When researchers choose to share your contact information with FERC, the Commission commits to coordinating with researchers as openly and as quickly as possible. Within 3 business days,

FERC shall acknowledge that your report has been received. To the best of our ability, the Commission shall confirm the existence of the vulnerability to researchers. FERC will be as transparent as possible about what steps the Commission is taking during the remediation process, including issues or challenges that may delay resolution. The FERC shall maintain an open dialogue to discuss issues with researchers.

8. QUESTIONS

Questions regarding this policy may be sent to vdppfeedback@ferc.gov. The Commission also invites researchers to contact FERC with suggestions for improving this policy.

9. AUTHORITY

9.1 References

No.	<i>Document Name, Version, Location and/or Link</i>
1	Office of Management and Budget (OMB) Circular A-130, <i>Management of Federal Information Resources</i> , Appendix III, <i>Security of Federal Automated Information Systems</i>
2	FISMA Modernization Act of 2014, Public Law 113-283
3	Binding Operational Directive 20-01, cyber.dhs.gov - Binding Operational Directive 20-01
4	U.S. Department of Justice, A Framework for a Vulnerability Disclosure Program for Online Systems, https://www.justice.gov/criminal-ccips/page/file/983996/download