UNITED STATES OFFICE OF
GOVERNMENT ETHICS

Vulnerability Disclosure Policy

US Office of Government Ethics

February 2021

Introduction

The US Office of Government Ethics (OGE) is committed to ensuring the security of our systems and protecting sensitive information from unlawful disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to describe how to submit discovered vulnerabilities to us.

In accordance with Department of Homeland Security (DHS) Binding Operational Directive (BOD) 20-01 and Office of Management and Budget (OMB) Memo M-20-32, 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 reporters to wait before publicly disclosing vulnerabilities.

We encourage researchers to contact us to report potential vulnerabilities in our systems. For reports submitted in compliance with this policy, OGE will acknowledge receipt within three business days.

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 OGE 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 command line access and/or persistence, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time (as described below) to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

If you 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**. You are prohibited from disclosing any personally identifiable information discovered to any third party.

Test Methods

The following test methods **are not authorized**:

- Test any system other than the systems set forth in the 'Scope' section below
- Engage in physical testing of facilities or resources
- Engage in social engineering
- Send unsolicited electronic mail to OGE users, including "phishing" messages
- Execute or attempt to execute "Denial of Service" or "Resource Exhaustion" attacks
- Introduce malicious software
- Test third-party applications, websites, or services that integrate with or link to or from OGE systems
- Use an exploit to exfiltrate data, establish command line access, establish a persistent presence on OGE systems, or "pivot" to other OGE systems
- Delete, alter, share, retain, or destroy OGE data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Authorized tests may:

- View or store OGE nonpublic data only to the extent necessary to document the presence of a potential vulnerability.

Reporters must:

- Cease testing and notify us immediately upon discovery of a vulnerability
- Cease testing and notify us immediately upon discovery of an exposure of nonpublic data
- Purge any stored OGE nonpublic data upon reporting a vulnerability

Scope

This policy applies to the following systems:

- www.oge.gov
- www.integrity.gov

Any systems or services not explicitly listed above, such as any connected services, are excluded from scope and are not authorized for testing. 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). If you aren't sure whether a system is in scope or not, contact us at security@oge.gov before starting your research.

Reporting a Vulnerability

Reports are accepted via electronic mail at security@oge.gov. Acceptable message formats are plain text, rich text, and HTML.

Reports should 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. 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. We request that any scripts or exploit code be embedded into non-executable file types.

Researchers may submit reports anonymously. If you choose to share contact information, and any preferred methods or times of day to communicate, we may contact reporters to clarify reported vulnerability information or other technical interchange.

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 resolve vulnerabilities within 90 days and notify you of the outcome of your report, if you have provided contact information. If you believe others should be informed of the vulnerability before receiving notification of resolution, we require that you coordinate in advance with us. We will maintain an open dialogue to discuss issues.

We may share vulnerability reports with the Cybersecurity and Infrastructure Security Agency (CISA), as well as any affected vendors.

Questions

Questions regarding this policy must be sent to security@oge.gov. The OGE encourages security researchers to contact us for clarification on any element of this policy. We also invite security researchers to contact us with suggestions for improving this policy.