Vulnerability Disclosure Policy

As part of a U.S. government agency, the Tennessee Valley Authority Office of Inspector General takes seriously the responsibility to protect the public's information, including financial and personal information, from unwarranted disclosure.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered, as set out in this policy, so that we can fix them and keep our information safe.

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.

Guidelines

We require that you:
- 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. 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. Once you've established that a vulnerability exists, or encountered any of the sensitive data outlined below, you must stop your test and notify us immediately.
- Keep confidential any information about discovered vulnerabilities for up to 90 calendar days after you have notified TVA Office of Inspector General.

Scope

This policy applies to the following systems:

- Tvaoig.gov

Any services not expressly 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 their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact us at hostmaster@tvaoig.gov before starting your research.

The following test types are not authorized:

- User interface bugs or typos.
- Network denial of service (DoS or DDoS) tests.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

If you encounter any of the below on our systems while testing within the scope of this policy, **stop your test and notify us** **immediately**:

- Personally identifiable information
- Financial information (e.g. credit card or bank account numbers)
- Proprietary information or trade secrets of companies of any party

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, will work with you to understand and resolve the issue quickly, and TVA OIG will not initiate or recommend legal action related to your research.

Reporting a vulnerability

We accept and discuss vulnerability reports via electronic mail at hostmaster@tvaoig.gov. Acceptable message formats are plain text, rich text, and html. Reports may be submitted anonymously. **Note: The TVA OIG prefers that vulnerability report messages be encrypted.**

Reports should include:

- Description of the location and potential impact of the vulnerability.
- A detailed description of the steps required to reproduce the vulnerability. Proof of concept (POC) scripts, screenshots, and screen captures are all helpful. Please use extreme care to properly label and protect any exploit code.
- Any technical information and related materials we would need to reproduce the issue.

Please keep your vulnerability reports current by sending us any new information as it becomes available.

We may share your vulnerability reports with US-CERT, as well as any affected vendors or open source projects.

Coordinated Disclosure

The Tennessee Valley Authority Office of Inspector General is committed to patching vulnerabilities within 90 days or less, and disclosing the details of those vulnerabilities when patches are published. We believe that public disclosure of vulnerabilities is an essential part of the vulnerability disclosure process, and that one of the best ways to make software better is to enable everyone to learn from each other's mistakes.

At the same time, we believe that disclosure in absence of a readily available patch tends to increase risk rather than reduce it, and so we ask that you refrain from sharing your report with others while we work on our patch. If you believe there are others that should be informed of your report before the patch is available, please let us know so we can make arrangements.

We may want to coordinate an advisory with you to be published simultaneously with the patch, but you are also welcome to self-disclose if you prefer. By default, we prefer to disclose everything, but we will never publish information about you or our communications with you without your permission. In some cases, we may also have some sensitive information that should be redacted, and so please check with us before self-disclosing.

Questions

Questions regarding this policy may be sent to hostmaster@tvaoig.gov. The TVA OIG encourages security researchers to contact us for clarification on any element of this policy. Please contact us prior to conducting research if you are unsure if a specific test method is inconsistent with or unaddressed by this policy. We also invite security researchers to contact us with suggestions for improving this policy.

Document Change History

Version	Date	Description
1.0	02/2021	First issuance
2.0	06/2024	Revised website