Vulnerability Disclosure Standard

Introduction

OMES Information Services is committed to ensuring the security of State of Oklahoma systems and protecting sensitive information from unauthorized disclosure. This standard provides vulnerability reporters clear guidelines for conducting vulnerability discovery activities and to convey the state's preference in how to submit discovered vulnerabilities.

Purpose

This document provides guidelines for reporting security vulnerabilities to the State of Oklahoma.

Standard

The State of Oklahoma requires vulnerability reporters to notify Oklahoma Cyber Command within 24 hours of discovery of a vulnerability, unless specified otherwise contractually.

Vulnerability reports are submitted by emailing cybercommand@omes.ok.gov. Submissions should include the following information.

- Location the vulnerability was discovered and the potential impact of exploitation.
- Detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).

A legitimate vulnerability reporter exhibits the following characteristics.

- Notifies Oklahoma Cyber Command within 24 hours once a real or potential security issue is discovered.
- Makes every effort to avoid privacy violations, degradation for user experience, disruption to production systems and destruction or manipulation of data.

An illegitimate vulnerability reporter exhibits the following characteristics that may be subject to criminal prosecution under the Oklahoma Computer Crimes Act.

- Uses an exploit to compromise or exfiltrate data, establish command line access and/or persistence or use the exploit to pivot to other systems.
- Performs network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Participates in physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.

Information submitted under this standard is used for defensive purposes only – to mitigate or remediate vulnerabilities.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- CISA Coordinated Vulnerability Disclosure (CVD) Process.
- Oklahoma Computer Crimes Act.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 03/08/2022	**Review cycle:** Annual
Last revised: 03/08/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	