Process steps

Title:	ODHS|OHA 090-007-01 Continuous Vulnerability Management Process
Related to:	ODHS|OHA 090-007 Information Technology Vulnerability Management Policy
Effective date:	04/03/2023

Purpose

Vulnerability scanning and remediation, collectively noted as vulnerability management, are essential for protecting against cyber security threats, and maintaining strong security for information systems and data. The purpose of continuous vulnerability management is to provide a framework for detecting, analyzing, and mitigating continually evolving cyber security threats to the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) information systems, applications, and data. The process below aligns with the Statewide Information and Cyber Security Standards and the Center for Internet Security (CIS) Controls.

Applicability

This process applies to all ODHS and OHA staff including employees, volunteers, trainees, as well as contractors and partners.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Process

1. The Office of Information Services (OIS) utilizes a Security Content Automation Protocol (SCAP)-compliant tool to accomplish authenticated and unauthenticated vulnerability scanning and reporting.
   a. Dedicated accounts for authenticated scans will not be used for any other administrative activities.

   b. Dedicated accounts will be tied to specific machines at specific Internet Protocol (IP) addresses.[1]
   c. Internal and external vulnerability scans will be performed with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.[2]
2. The responsible party for the following steps varies based on system type (server or desktop) and software type (operating system [OS] or third-party application):
   a. For server OS: EIS Data Center Services (DCS) and information system owners.
   b. For server application: Information system owner, OIS, and/or Enterprise Information Services (EIS) Cyber Security Services (CSS).
   c. For desktop OS: OIS Customer Services and Support (CSS).
   d. For desktop application: OIS CSS, OIS Solution Development and Delivery (SDD), or external vendor.
   e. For mobile OS: OIS CSS.
3. The responsible parties deploy automated software update tools to ensure the operating systems and third-party software are running the most recent security updates provided by the software vendor. [3]
4. The responsible parties have access to, prioritize, and continually review the vulnerability scan reports and any other known zero-day vulnerabilities to verify where possible that vulnerabilities have been remediated in a timely manner.[4] A zero-day vulnerability is a software weakness previously unknown to the vendor and being actively exploited.
5. ISPO also reviews the vulnerability scans and prioritizes the risk of any vulnerabilities not remediated in a timely manner, including:
   a. Vulnerabilities for which a patch doesn't exist yet or patching causes other issues or risks.
   b. Vulnerabilities that don't require a patch-based remediation.
6. Based on the remediation prioritization of the risk-rating generated in step #5, ISPO:
   a. Works with the responsible parties to notify affected groups when a remediation plan is required.
   b. Adds high risk, high impact vulnerabilities to the ODHS and OHA Information Security Risk Register, and assigns it to the responsible party in order to assist in any remediation effort(s).
7. When the information system owner is unable to comply with the scanning requirements, the requirement to review scans or the requirements to patch vulnerabilities, the responsible parties request an exception. (Refer to MSC 3489 Risk Exception Request Form)

---

[1] 2019 Statewide Information and Cyber Security Standards, Risk Assessment (RA)-5(5)
[2] 2019 Statewide Information and Cyber Security Standards, Risk Assessment (RA)-5(5)
[3] 2019 Statewide Information and Cyber Security Standards, System and Information Integrity (SI)-2(2)
[4] 2019 Statewide Information and Cyber Security Standards, RA-5

a. A risk evaluation is completed by the ISPO Risk Management Team.
b. If the exception is approved by the information system owner or the program director, the CIRO conducts the final sign off of the results of the risk evaluation.
c. If the exception is denied, the information system owner or program director implements compensating controls and submits the request to the ISPO Risk Management Team for reevaluation.
d. The ISPO Risk Management Team tracks the exception, and reevaluates at least every ninety days or when the exception has expired.

References

45 CFR 164 Security and Privacy

Oregon Revised Statute (ORS) 192.355 Public Records Exempt from Disclosure

Criminal Justice Information Services (CJIS) Policy

Federal Information Processing Standards (FIPS) Publication (Pub) 200 Minimum Security Requirements for Federal Information and Information Systems

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume I Harmonized Security and Privacy Framework Version 2.2

Microsoft SecurityTech Center Security Bulletin Severity Rating System, GG309177

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev. 1 Guide for Conducting Risk Assessments

NIST SP 800-40 Rev. 4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

Social Security Administration Information Exchange Security Requirements and Procedures

Statewide Information and Cyber Security Standards 2019

ODHS|OHA 090-006-01 Information Security Risk Assessment Process

ODHS|OHA 090-007-02 Continuous Vulnerability Management Process Map

Center for Internet Security (CIS) Controls

Forms

MSC 3489 Risk Exception Request Form

Related policies

DAS 107-004-052 Cyber and Information Security

DAS 107-004-120 Cyber and Information Security Incident Response

ODHS|OHA 090-005 Information Security Incident Management Policy
ODHS|OHA 090-006 Information Security Risk Assessment Policy
ODHS|OHA 090-007 Information Technology Vulnerability Management Policy
ODHS|OHA 090-009 Administrative, Technical, and Physical Safeguards of Information Policy

Contact

Office of Information Services
Service Desk: 503-945-5623
DHS.ServiceDesk@odhsoha.oregon.gov

Process history

Version 1 DHS|OHA 090-006-03 established 10/16/15
Version 2 DHS|OHA 090-006-03 revised 10/24/16
Version 3 DHS|OHA 090-007-01 replaced DHS|OHA 090-006-03 on 06/05/2017
Version 4 DHS|OHA 090-007-01 revised 02/05/2018
Version 5 ODHS|OHA 090-007-01 revised 06/07/2021
Version 6 ODHS|OHA 090-007-01 revised 04/03/2023

Keywords

Authenticated vulnerability scans, dedicated accounts, information technology, patch, patch management, scan, security, security content automation protocol, SCAP, unauthenticated vulnerability scans, vulnerability, vulnerabilities

---