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:	06/07/2021

Purpose

Vulnerability scanning, assessment, 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, interns, 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. Program or Chief Information Risk Officer (CIRO) initiates a vulnerability assessment by submitting an OIS Service Desk ticket to the Information Security and Privacy Office (ISPO).
2. Enterprise Information Services (EIS) Cyber Security Services (CSS) utilizes a dedicated account for authenticated scans, which will not be used for any other administrative activities and will be tied to specific machines at specific Internet Protocol (IP) addresses. [1]
3. EIS CSS performs authenticated vulnerability scans with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. [1]
4. 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 operating system (OS): EIS Data Center Services (DCS)
   b. For server application: Information system owner, Office of Information Services (OIS), and/or EIS CSS.

[1] 2019 Statewide Information and Cyber Security Standards, Risk Assessment (RA)-5(5)

c. For desktop OS: OIS Customer Services and Support (CSS)
d. For desktop application: OIS CSS

5. The responsible party deploys 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. [2]
6. The responsible party prioritizes and continually reviews the vulnerability scan reports produced by the Security Content Automation Protocol (SCAP)-compliant vulnerability scanning tool and any other known zero-day vulnerabilities to verify where possible that vulnerabilities have been remediated in a timely manner.[3]
7. ISPO also reviews the vulnerability scans and rates the risks 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.
8. Based on the risk-rating generated in step #7, ISPO:
   a. Adds vulnerabilities with *high* or *critical* rating to the risk register.
   b. Creates a Service Desk ticket for each *high* or *critical* vulnerability, and assign it to the responsible party in order to assist in any remediation effort(s).
   c. Works with the responsible party to notify affected stakeholders when a remediation plan is required.
9. When the information system owner cannot comply with the scanning requirements, the requirement to review scans, or the requirements to patch vulnerabilities, an exception is requested. (Refer to MSC 3489 Risk Exception Request Form)
   a. If approved by the program manager or designee, a risk assessment is completed.
   b. The results of the risk assessment are submitted to the CIRO for final review and approval.
10. ISPO documents and tracks remediation of vulnerabilities through completion.

References

45 CFR 164
Oregon Revised Statute (ORS) 192.355
Criminal Justice Information Services (CJIS) Policy
Federal Information Processing Standards (FIPS) Publication (Pub) 200
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Microsoft SecurityTech Center Security Bulletin Severity Rating System, GG309177
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev. 1
NIST SP 800-40 Rev. 3
NIST SP 800-53 Rev. 5
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019
ODHS|OHA 090-007-02 Continuous Vulnerability Management Process Map
Center for Internet Security (CIS) Controls

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

Forms

MSC 3489 Risk Exception Request Form

Related policies

DAS 107-004-052 Information Security
DAS 107-004-120 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 Policy

Contact

Office of Information Services
Service Desk: 503-945-5623
DHS.ServiceDesk@dhsoha.state.or.us

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 02/0518
Version 5 ODHS|OHA 090-007-01 revised 06/07/2021

Keywords

Applications, assessment, authenticated, Cyber Security Services, CSS, deploy, Enterprise Information Services, EIS, information system owner, patch, remediated, responsible party, risk, risk rating, risk register, SCAP-Compliant Scanning Tool, security, Security Content Automation Protocol, systems, test, vulnerability, vulnerability scan

---