Process steps

| Title | DHS|OHA-090-007-01 Vulnerability Assessment Process |
|------|--------------------------------------------------|
| Related to: | DHS|OHA-090-007 Vulnerability Assessment Policy |
| Effective date: | 02/05/18 |

Purpose
The Information Security and Privacy Office (ISPO) conducts periodic risk based vulnerability assessments of the Department of Human Services (DHS) and the Oregon Health Authority (OHA) information systems and applications. The purpose of vulnerability assessments is to identify and manage vulnerabilities and related information security risks.

Process
1. Program or Chief Information Security Officer (CISO) initiates a vulnerability assessment by submitting an OIS Service Desk ticket to ISPO.
2. ISPO engages with stakeholders such as assigned application owners, system vendors, programmers, and developers, and if necessary, Enterprise Technology Services (ETS) on the scope of the vulnerability assessment regarding the following:
   a. Informing stakeholders of the vulnerability assessment process and associated risks;
   b. How and when the test will be done;
   c. The anticipated duration of the assessment;
   d. What stakeholders will be notified;
   e. Actions that will and will not be performed;
   f. Acquiring account access necessary to conduct authenticated vulnerability assessment;
   g. The testing platform (development, test, or user acceptance test); and
   h. If necessary, obtaining application source code, firewall rules, and other “insider” information for the assessment.
3. ISPO completes the vulnerability assessment. If the vulnerability assessment phase continues beyond the expected duration or if problems are encountered during the assessment, ISPO shall provide the stakeholders with an update on the status.
4. ISPO updates the vulnerabilities scanned at least every thirty days or when new vulnerabilities are identified and reported.
5. ISPO shares the results of the scanning activities with the Chief Information Officer (CIO) and appropriate stakeholders.
6. ISPO repeats the vulnerability assessments to ensure the vulnerabilities have been addressed.

References
45 CFR 164
Criminal Justice Information Services (CJIS) Policy
Related policies

- DAS 107-004-052 Information Security
- DAS 107-004-120 Information Security Incident Response
- DHS|OHA-090-002 Information System Audit and Monitoring Policy
- DHS|OHA-090-005 Information Security Incident Management
- DHS|OHA-090-006 Information Security Risk Assessment Policy
- DHS|OHA-090-007 Vulnerability Management Policy
- DHS|OHA-090-009 Administrative, Technical, and Physical Safeguards Policy

Contact

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

Process history

- Version 4 DHS|OHA-090-007-01 revised 02/05/18
- Version 3 DHS|OHA-090-007-01 replaced DHS|OHA-090-006-03 on 06/05/2017
- Version 2 DHS|OHA-090-006-03 revised 10/24/16
- Version 1 DHS|OHA-090-006-03 established 10/16/15

Keywords

Applications, assessment, Enterprise Technology Services, ETS, public facing, requirements, risk, security, stakeholders, systems, test, vulnerability, weakness

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.