Process steps

Title:	ODHS|OHA 090-009-05 Geofencing Exception Request Process
Related to:	ODHS|OHA 090-009 Administrative, Technical and Physical Safeguards Policy
Effective date:	12/07/2020

Purpose

Tens of thousands of invalid access attempts to the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) agency systems from outside the United States (U.S.) pose an increased risk of breaches. Geofencing creates a virtual geographic boundary, prohibiting access to systems based on user geolocation. This process outlines the steps necessary for a user to obtain an exception to access ODHS|OHA information systems and servers from outside of the U.S.

Applicability

This process applies to all ODHS and OHA staff including employees, volunteers, trainees, interns, 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 Steps

1. Internet Protocol (IP) addresses used outside of the U.S. are blocked from accessing agency information systems or networks unless an exception is approved. An IP address is defined as standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
2. If there is a business need for ODHS|OHA staff to access agency information systems or networks from outside the U.S., the agency program requests an exception by submitting the MSC 3483 to the OIS Service Desk which includes the following information:
   a. The reason for the request.
   b. The specific circumstances requiring the exception.
   c. The information system or network to be accessed.
   d. How long the exception will be needed.
   e. How the exception will comply with all applicable statutes, contracts and rules.
3. When a third-party entity, either an organization or individual, needs to access an agency information system or network from outside of the U.S.:
   a. The agency program submits the MSC 0785 to the address listed on the form identifying the need.
   b. The InfoEx Coordinator drafts an appropriate agreement and submits the agreement to the third party and agency program for review, approval, and signatures.

A. If there is an existing agreement, the ISPO InfoEx Coordinator adds applicable language to the access agreement, and submits the revised agreement to the third party and agency program for review, approval, and signatures.
B. If the access agreement has expired, the InfoEx Coordinator notifies the program that the agreement needs to be renewed, and language and template updated if necessary. Use of an updated template requires staffing for signatures between the agreement parties.
C. If there isn't an access agreement, the ISPO InfoEx Coordinator drafts the agreement and submits it to the third party and agency program for review, approval, and signatures.

c. Once signed by both parties, the InfoEx Coordinator provides the program with a copy updating the language of the access agreement for their files.

4. The OIS Service Desk forwards the request to ISPO for review of the exception request.
   a. ISPO consults with the information system owner.
   b. ISPO consults with any other affected parties.
5. If approved, ISPO forwards the request to the OIS Chief Information Officer (CIO) or designee for approval or denial.
   a. If approved, ISPO forwards the request to Enterprise Information Services (EIS) Cyber Security Services (CSS).
   b. If denied, ISPO replies via the service desk ticket, notifying the agency program requestor of the denial.
6. Approved requests are processed by EIS CSS.
7. EIS CSS works with the EIS Data Center Services (DCS) to revise the firewall rules for the requested exception.
8. ISPO maintains and monitors the list of approved exceptions at least annually.
9. Access to federal tax information (FTI) is not eligible for this process.[1]

References

Center for Internet Security (CIS) Controls
Committee on National Security Systems (CNSS) No. 4009, April 6, 2015
Criminal Justice Information Systems Security Standards (CJIS)
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5
Statewide Information and Cyber Security Standards 2019
ODHS|OHA 090-003-08 Third Party Entity Approval for System Access Process
ODHS|OHA 090-009-06 Geofencing Exception Process Map

Forms

MSC 0785 Third Party Information System Access Request
MSC 3483 Geofencing Exception Request Form

Related policies

ODHS|OHA 090-003 Access Control Policy
ODHS|OHA 090-009 Administrative, Technical, and Physical Safeguards Policy

[1] Internal Revenue Service (IRS) Publication 1075, September 2016

Contact

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

Process history

Version 1 Established ODHS|OHA 12/07/2020

Keywords

Access, exception, geofencing, geolocation, internet protocol, IP, IP address, location

---