Process steps

| Title:       | DHS|OHA 090-005-01 Information Security Incident Reporting Process |
|-------------|--------------------------------------------------------------------------------|
| Related to: | DHS|OHA 090-005 Information Security Incident Management Policy                  |
| Effective date: | 9/12/2018                                                                          |

Purpose

This process outlines the steps necessary for the Department of Human Services (DHS) and the Oregon Health Authority (OHA) to appropriately identify and report all suspected or actual security breaches, incidents, and violations, including unauthorized or impermissible uses or disclosures when required by agency, state or federal law and requirements.

Process Steps

1. When DHS|OHA staff suspect, or become aware of any information security incident involving unauthorized access, loss, modification, or disclosure of agency information or systems including but not limited to, personally identifiable information (PII), protected health information (PHI), federal tax information (FTI), or Criminal Justice Information Services (CJIS) information, staff shall:
   a. Immediately notify the Information Security and Privacy Office (ISPO). Notification can be done by email, phone or using the MSC 3001 form.
   b. Immediately notify their manager or supervisor of the security incident.

2. ISPO shall review and process all reports of potential security incidents.

3. Security incidents involving suspected or the actual loss of Social Security Administration (SSA)-provided information shall be processed according to the following steps:
   a. ISPO shall notify the SSA Regional Office or the SSA Systems Security Contact as identified in the SSA Information Exchange Agreement (IEA) within one hour of notification of the suspected or actual loss of SSA-provided information.
   b. If ISPO is unable to make contact with the SSA Regional Office or the SSA Systems Security Contact within one hour, ISPO shall report the security incident to the SSA’s National Network Service Center (NNSC) toll free at 877-697-4889 (select “Security and PII Reporting” from the options list).
   c. ISPO shall provide updates as they become available to the SSA contact as appropriate.
   d. SSA shall make a determination about whether the risk presented by the breach or security incident requires the notification of the individuals whose information is involved and/or remediation action.

4. Security incidents involving suspected or the actual loss of Internal Revenue Service (IRS) provided FTI information shall be processed according to the following steps:
a. ISPO shall contact the Treasury Inspector General for Tax Administration (TIGTA) Field Division Office at 801-620-7734 immediately, but no later than 24 hours after notification of the suspected or actual breach.

b. Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, ISPO shall contact the office of the appropriate special agent-in-charge, TIGTA immediately, but no later than 24 hours after identification of a possible issue involving FTI.

c. If unable to contact the local TIGTA Field Division, ISPO shall contact the Hotline Number at 800-589-3718, TIGTA Homepage: https://www.treasury.gov/tigta, Mailing Address: Treasury Inspector General for Tax Administration Ben Franklin Station P.O. Box 589 Washington, DC 20044-0589

d. Concurrent to notifying TIGTA, the agency shall notify the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov.
   A. Reports shall be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email.
   B. Do not include any FTI in the data Incident report. Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

e. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:
   A. Name of agency and agency point of contact for resolving data incident with contact information.
   B. Date and time the incident occurred.
   C. Date and time the incident was discovered.
   D. How the incident was discovered.
   E. Description of the incident and the data involved, including specific data elements, if known
   F. Potential number of FTI records involved; if unknown, provide a range if possible
   G. Address where the incident occurred
   H. IT involved (e.g., laptop, server, mainframe)

f. The agency shall cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

5. Security incidents involving the actual loss of CJIS provided information shall be processed according to the following steps:
   a. The Local Agency Security Officer (LASO) shall promptly report incident information to the state CJIS Information Security Officer (CJIS ISO).
   b. The LASO shall utilize the Security Incident Response Form provided in Appendix F of the CJIS Security Policy when reporting incidents to the Oregon State Police and the Federal Bureau of Investigations (FBI) CJIS Division.

6. Security incidents involving suspected or the actual loss of any other regulated data including but not limited to Protected Health Information (PHI), shall be reported to the DHS|OHA Information Security Officer (ISO) within one hour of notification.

7. In accordance with HIPAA regulations and OHA policy 100-014, when ISPO determines that a breach has occurred, and PHI may have been acquired, accessed, used, or disclosed without
appropriate authorization, the responsible OHA program, in consultation with the Privacy Office shall:

a. Provide written notice of the breach to the affected individual or individuals no more than 60 days after the discovery of the breach; and

b. Provide ISPO with documentation that notice has been provided.

8. The ISO shall notify the DHS|OHA Chief Information Security Officer (CISO) within 24 hours of notification.

9. ISPO shall ensure identified remediation actions are performed as required by, including but not limited to, SSA, IRS, and CJIS.

10. ISPO shall report all information security incidents occurring within DHS|OHA to the Office of the Chief Information Officer (OCIO) Enterprise Security Office (ESO), in accordance with the Statewide Information Security Standards.

References

Statewide Information Security Plan
Center for Internet Security Top Twenty Critical Security Controls
45 CFR 160 and 164
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 (SP) 800-53 Rev. 4
NIST Cybersecurity Framework
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information Security Standards
DHS|OHA 090-005-04 Security Incident Reporting Process Map

Forms referenced

MSC 3001 DHS|OHA Privacy/Security Incident Report

Related policies

DAS 107-004-052 Information Security Policy
DAS107-004-120 Information Security Incident Response Policy
DHS|OHA 090-005 Information Security Incident Management
OHA100-014 Report and Response to Privacy and Security Incidents

Contact

Information Security and Privacy Office
Security 503-945-6812
Dhsinfo.security@state.or.us

Process History

Version 1 (Joint DHS|OHA) 09/11/2017
Version 2 DHS|OHA reviewed annually 09/12/2018
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.