Overview

Governments have the primary responsibility to prevent, detect and respond to fraud, loss and other illegal activity, and should have effective policies and procedures in place to accomplish these fiscal responsibilities in the service of protecting public resources.

State law (RCW 43.09.185) requires all state agencies and local governments to immediately report known or suspected losses of public funds or other illegal activity to the Office of the Washington State Auditor (SAO). In 2022, the Legislature updated this law to require the SAO to adopt policies that further define the loss reporting process.

SAO takes seriously all instances of misappropriation and loss of public funds in government and reserves the right to investigate any potential loss or illegal activity, regardless of its nature. SAO receives reports and information about known or suspected losses through several channels, depending on the nature of loss. These channels include but are not limited to the fraud loss submission process, whistleblower submission process, citizen hotline, and risk assessment inquires with the government's management as part of regular audit planning.

SAO has now updated this policy with the goal of clarifying which losses should be reported to SAO specifically through the fraud loss submission process.

If after reviewing this policy you still have questions, please contact the Special Investigations Division at: fraud@sao.wa.gov

Section 1 - Losses or Illegal Activities Exempt from Reporting Requirement

As stated in the policy overview, SAO receives reports and information about known or suspected losses of public funds through several channels, depending on the nature of loss. These channels include but are not limited to the whistleblower submission process, citizen hotline, and risk assessment inquires with the government's management as part of regular audit planning.

Additionally, although certain losses are exempt from reporting to SAO under this policy, these losses should be documented somehow, such as in a government's accounting system or inventory system, to name just two examples. Governments also should bring these matters to the auditor's attention during the regularly scheduled SAO audit. Finally, governments should determine whether communications or notifications to other parties are necessary for any potential loss of public funds, including those listed here. For example, if losses involve federal funds or programs, the government should contact their federal grantor (or follow their grantor's prescribed loss reporting procedure).

If employee involvement cannot be ruled out in any of the listed exemptions, governments should then report the loss or illegal activity to SAO even if the loss or activity is on the exemption list. "Employee involvement" means the scheme involved or was carried out by an employee of the affected government.

The following is a list of losses or illegal activities that state agencies and local governments are NOT required to report to the SAO through the fraud loss submission process.

- Normal and reasonable "over and short" situations from cash receipting operations. We recommend governments record these transactions in the accounting system as miscellaneous income and expense, respectively, and monitor this activity for any unusual trends.
- Reasonable inventory shortages identified during a physical count. We recommend governments record inventory adjustments in the accounting system.
- Unauthorized credit card attempts and/or transactions initiated by an external party, that are determined fraudulent by the bank and refunded.
- Breaking and entering or vandalism of property, including assets stolen out of government vehicles. We recommend governments report these to the police.
- Loss of cellphones, tablets, laptops or similar type assets assigned to employees that were stolen by an external party. We recommend governments report these to the police.
- Non-Sufficient Funds (NSF) checks accepted by the government. We recommend governments document these in their accounting records.
- Counterfeit currency accepted by the government. Governments should report these to the FBI.
- Eligibility-based funding provided to an external party based on incorrect or falsified eligibility

information. (See additional considerations below). Examples include, but are not limited to:

- Families misreport their income to become eligible for free-reduced lunch
- Tenant or client falsifies their income or other eligibility criteria to receive housing assistance funding
- Claimant submits a fraudulent unemployment claim for payment

We recommend governments document these items and notify interested parties depending on the source of funds.

- Cybersecurity incidents that did not have an impact on finances or financial records. See *Section 2: Clarification of Losses to Report – Cybersecurity Incidents* for additional details.

Losses to report directly to the audit team as part of the regular audit process

- With the exception of cyber losses defined in Section 2, losses or illegal activity resulting from actions made by parties external to your government – including vendors, contracted service providers, sub-recipients and other non-government parties – should be reported to your audit team.

Section 2 – Clarification of losses to report Cybersecurity Incidents

State agencies and local governments must report cybersecurity incidents that involve the finances or financial records in some way. Below are some examples of activity you must report:

- Your government experiences a ransomware attack and makes a payment to the criminal actors to regain access to your data, even if your insurance company either pays the ransom or reimburses your government for the payment. This extortion payment is a financial loss as a result of illegal activity.
- Your government falls victim to a ransomware attack. You can restore your data from backups and do not pay the ransom. You should report this incident if it's possible the attackers accessed any financial records. Keep in mind that even though attackers may have only encrypted non- financial records, they could have accessed financial records and are waiting to ransom them at a later point. Determining which records the attackers accessed involves more than simply evaluating which records the attackers ransomed.
- Your staff relies on a fraudulent email to change banking information and an electronic payment is sent to a criminal, instead of to a vendor or employee, even if your insurance company covers the loss, or the bank is able to recover your funds.
- Someone gains unauthorized access to your computer system and they may have accessed your financial records, even if those records were not harmed or impacted in any way.
- You have a security incident that might have impacted your financial records or systems, but you are not certain.