



Internal Audit Department

350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Date: September 20, 2016

To: Audit Committee

Re: Office of the State Auditor Management and Compliance Report Finding 2014-003

The Office of the State Auditor published their Management and Compliance Report for the City of Minneapolis in June of 2016 for the fiscal year ending 12/31/15. Upon review of the report, the Audit Committee requested that Internal Audit conduct an analysis into the finding regarding system access (Finding 2014-003 – Network and System Access Termination). The intent of the analysis and this memo was to identify the root cause of a component of this finding and report back to the Audit Committee with results.

The finding stated that one City employee's access to the general ledger system that was not disabled timely had accessed the general ledger system after their termination date. Internal Audit gathered information from the department that employed this individual, Finance staff and IT staff to understand the sequence of events that lead to this finding.

The component of the State Auditor's finding that asserts a terminated employee's account was used to access the general ledger appears to be inaccurate. The information the State Auditors were using to assert this appears to be flawed. Below is a timeline of events as it relates to this employee's access termination:

- 7/10/15 last COMET login (general ledger)
- 8/13/15 last day of employment
- 9/8/15 job change form signed by supervisor
- 10/15/15 HR account locked
- 1/6/16 PeopleSoft Finance account locked
- 8/9/16 Active Directory account locked

As the State Auditor's finding mentions, access termination is a sequence of events that involve multiple departments. If information doesn't move within this process in a timely manner, or deviates from the typical process for some reason, the outcome can leave the City unnecessarily exposed to risk.

The details do, however, illustrate the effects of a decentralized access provisioning process that creates an opportunity to leave the City unnecessarily exposed to the risk of allowing access to potentially confidential information to unauthorized individuals.