Commonwealth of Massachusetts

THOMAS G. SHACK III, ESQ.
COMPTROLLER

To: Legislative Leadership, Judicial Branch Administrators, Elected Officials, Secretariats, Department Heads, Chief Fiscal Officers and Single Audit Liaisons

From: Thomas G. Shack III, Comptroller

Date: April 25, 2018

Re: Audit Issues from the 2017 Single Audit - Preparation for 2018

Comptroller Memo FY#2018-19

Executive Summary

The Commonwealth's FY2017 Single Audit has been completed as required by OMB's Uniform Guidance. The guidance can be found at Title 2 CFR Subtitle A, Chapter II, Part 200. This year we have noted some common themes to the findings prepared by KPMG LLP, the independent audit firm. These are described below to allow departments to consider whether changes are needed in preparation for the FY2018 Single Audit, which is currently underway.

Issues from the FY 2017 Single Audit

The auditors reported the following observations as part of the FY2017 Single Audit. Some resulted in audit findings and others in management letter comments. The topics below are not specific to any one finding or department. The complete audit results can be found at https://www.macomptroller.org/single-audits.

Cash Management
Departments need to improve their monitoring of cash reimbursement to subrecipients and should document their procedures specific to Cash Management.

Departments are required to maintain internal control over Federal programs that provide reasonable assurance that the department is managing Federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its Federal programs. Maintaining and improving written procedures over cash management will ensure and minimize the time elapsing between the transfer of federal funds and disbursement of funds.

Earmarking
The Single Audit found that earmarking requirements were not always met.

The State has various earmarking requirements under different award programs that each department must follow. Earmarking includes requirements that specify the minimum and/or maximum amount or

percentage of the program's funding (approved by State or Federal) that must/may be used for specified activities, including funds provided to subrecipients.

Eligibility Determination for Grant Programs
Departments did not always ensure that all program eligibility requirements were met.
Calculations of eligibility requirements for the allocation of grant funds were not always consistent.
Documentation of processes for review was lacking.

Every grant requires some form of eligibility for a recipient to receive funds. For example, credentialing criteria, income eligibility, or professional licensing may need to be established and verified for vendors or others who receive grant awards. Departments must establish and maintain effective internal controls over federal awards received as well as substantiate their eligibility process with full documentation must be kept in accordance with the grant. All eligibility determinations must be made in accordance with either a state plan filed with the Federal government, the grant award itself, or General Laws. Evidence must be readily available to prove eligibility.

Special Tests and Provisions
Some examples of the specific requirements to awarded programs found during the Single Audit:
- A formal documented policy and written communication was not maintained per requirements
- Deficiencies in system security requirements
- Inconsistency of documentation and review of work performed

Each Federal program is unique and has specific requirements for Special Tests and Provisions which can be found in the statutes, regulations, and the provisions of contract or grant agreements pertaining to the program. For example, if the grant program focuses on utilization control and program integrity, this focus requires the department to perform (1) methods or criteria for identifying suspected fraud cases; (2) methods for investigating these cases; and (3) procedures, developed in cooperation with legal authorities. Regardless of their unique & specific requirements, under the Uniform Guidance, departments must establish and maintain effective internal controls over Federal awards that provide reasonable assurance that they are managing these awards in compliance with Federal statutes, regulations, and the provisions of contracts or grant agreements that could have a material effect on each of its Federal programs.

Sub-recipient Monitoring
Not all sub-recipients were notified of the details of the awards they received.
Some state agencies did not perform risk assessments of their sub-recipients.

When departments are granting federal funds to a sub-recipient (a municipality or a non-profit), or another state agency, the department remains responsible for sufficient oversight of the funds (sub-recipient monitoring) to ensure that the funds are spent in accordance with federal grant requirements. The Uniform Guidance (2 CFR section 200.331) requires every department that is granting federal funds to a sub-recipient to follow these key components: identify the award and applicable requirements; evaluate the risk of noncompliance; monitor the activities of sub-recipients; and ensure accountability of For-Profit sub-recipients (if applicable).

Reminders for All Departments

Information Technology System Issues and Data Security
Data in department-managed systems must be protected, especially systems containing personally identifiable information and those that interface with the financial systems, MMARS and HR/CMS. Data should be backed up at least daily and a copy stored at an off-site location. Restoration processes should be tested at least annually to assure that data can be restored from backup media. Departments need to assure that all new hires have the proper security to their systems (no more than is needed to complete their duties) and that they are monitored. Personnel who terminate service with the department should have security access and functions cancelled immediately.

The Statewide Enterprise Systems Security Policy requires that departments monitor access to statewide systems (MMARS, HR/CMS, CIW, Luminist/DocDirect, and InTempo) on a regular basis to ensure that levels of access are appropriate and proper segregation of duties is in place. Such monitoring must also be in place for department-managed systems.

cc: MMARS Liaisons, Payroll Directors, General Counsels, Internal Control Officers, Internal Distribution