



Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
TELEPHONE (617) 727-5000
WWW.MACOMPTROLLER.ORG

THOMAS G. SHACK III, ESQ.
COMPTROLLER

To: Department Security Officers and Chief Fiscal Officers

From: Jeffrey S. Shapiro, Esq., First Deputy Comptroller

Date: November 27, 2018

Re: Department Security Officer (DSO) Review of Statewide Enterprise Systems Security Access. Due December 31, 2018

Comptroller Memo FY2019-12

Executive Summary

In accordance with the [Department Head Signature Authorization and Electronic Signatures for MMARS Transactions Policy](#) and the [Statewide Enterprise Systems Security Policy](#), Department Security Officers are required to certify individuals' access to Enterprise Systems that contain financial, payroll, and related data. This certification must be completed and returned to the Comptroller's Office by the last business day of the calendar year, December 31, 2018.

Departments must assign security roles that promote segregation of duties and ensure that users have the correct, appropriate, and lowest level of access to perform transactions relative to their responsibilities.

In addition, department leadership must review and update security roles whenever a user's responsibilities change and must immediately terminate access for any individual who separates from service or is placed on extended leave.

These reviews are required steps, as per Comptroller policy, in the overall process to mitigate the risk of improper Systems access and to prevent fraud, waste and abuse.

New FY19 items

eLearning Course: *Further details to follow at a later date.*

The Office of the Comptroller (CTR) is pleased to announce that an eLearning module has been created specifically for Department Security Officers (DSOs). This module reviews the DSOs' responsibilities and the Enterprise Systems. It also provides tips to perform the user access review. Tips include the four key reports to utilize, how to document evidence of the review, and how to complete the annual review form. CTR encourages all DSOs to complete the eLearning module which will be circulated shortly.

Deactivating Inactive Users:

CTR has implemented a new security review step in which CTR's Statewide Risk Management team will contact DSOs to delete system access for any users that have not logged into the Enterprise Systems within the prior 12 months. For users who are not regularly active but do need to maintain their access, DSOs should ensure that these individuals update their passwords as required by each relevant Enterprise System to avoid being deactivated.

Department Security Officers Review and Certification

Department Security Officers review encompasses the Enterprise Systems listed below and all individuals who can approve obligations and expenditures (execute contracts, signoff on payroll, incur obligations, authorize payments, etc.) on behalf of a Department Head, even if that individual does not access directly or regularly these Enterprise Systems.

Department Security Officers must use the annual review period to analyze individual role assignments to ensure that no one user has more system access than is required by his/her role.

List of Enterprise Systems:

- **MMARS/LCM:** The Massachusetts Management Accounting and Reporting System, including the Labor Cost Management sub-system, supports the financial functions performed by Commonwealth Departments. In no case should a user have privileges beyond those necessary to complete his/her job duties.
- **HR/CMS:** The Human Resource/Compensation Management System supports time and attendance, human resources and payroll. In no case should a user have privileges beyond those necessary to complete his/her job duties.
- **CIW:** The Commonwealth Information Warehouse provides access to financial, labor cost management, time and attendance, human resources and payroll data for MMARS, LCM, UMASS and HR/CMS as well as a variety of historical databases - Classic MMARS, PMIS and CAPS. In no case should a user have privileges beyond those necessary to complete his/her job duties.
- **InTempo:** The Executive Office of Technology Services & Security's online security system through which your Department Security Officers and Security Administrators request access to these Enterprise Systems.

Security reports to facilitate review and ongoing oversight

Four security reports are available in Luminist (formerly DocDirect) for department review and use. These reports are run monthly.

Security reports:

1. SECMARS (MMARS)
2. SECHRCMS (HR/CMS)
3. SECCIW (CIW)
4. SECINTEM (INTEMPO)

These reports display all active user profiles with their assigned security roles and signature authority. Access to these reports can be granted to Department Heads, Chief Fiscal Officers (CFOs), Internal Control Officers (ICOs) and Security Officers (DSOs).

The next Enterprise security reports will be available via Luminist on December 1st, and the reports will be run again mid-December for you to verify any changes you have made.

Additional tools for Enterprise Systems review

In addition, Department Heads, CFOs, and DSOs, as part of their internal controls, must review MMARS user activity using the following tools:

1. **Luminist Reports:**
NMF580W: MMARS Monthly User Activity Report
NMF581W: MMARS Monthly Verification of Segregation of Duties: Encumbrances and Payments
2. **CIW Views:**
User Activity Details: M_USER_ACTIVITY_DETAILS
User Activity Report: M_USER_ACTIVITY_REPORT

For Questions:

Enterprise Applications	Contacts for Security Related Issues
MMARS and HR/CMS	Comptroller's Security Team Phone: (617) 973-2468 Email: Securityrequest@mass.gov
CIW, VPN, and InTempo	Executive Office of Technology Services & Security's CommonHelp Phone: (866) 888-2808 Email: commonhelp.desk@mass.gov

Evidence of Enterprise Systems access review and certification

Evidence of all system access reviews must be maintained at the agency. Evidence of such review must be provided upon the request of the Office of the Comptroller and internal/external auditor(s). These reports serve as the evidence of your review. In the event that a department has its own method of tracking user access (Excel, Access, etc.), and demonstrates an active review for compliance which is clearly marked, signed and dated, it may substitute the annotated reports noted above.

All changes, no matter the method, must be clearly marked, initialed and dated. If there are no changes, that must be noted, initialed and dated as well.

After reviewing the security reports, process all changes as appropriate, submit each annotated page as your evidence of review, and provide department certification via the [Department Security Officer Annual Review Form](#). Please email this review form from the Department Security Officer's email account to securityrequest@mass.gov no later than December 31, 2018.

Thank you for your time and cooperation. Your diligence in complying with this policy is vital to mitigating risks inherent to managing these systems.

Cc: Department Heads
MMARS Liaisons
Payroll Directors
General Counsels
Internal Distribution