Commonwealth of Massachusetts
OFFICE OF THE COMPTROLLER
One Ashburton Place, 9th Floor
Boston, Massachusetts 02108
(617) 727-5000
macomptroller.org

William McNamara
Comptroller

To: Department Heads, Security Officers, and Chief Fiscal Officers

From: Peter J. Scavotto, Assistant Comptroller for Risk

Date: November 30, 2022

Re: Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access

Comptroller Memo #FY2023-09

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 (DSOs) 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 Office of the Comptroller (CTR) by the last business day of the calendar year, which this year will be Friday, December 30, 2022.

Departments must assign security roles that promote segregation of duties and ensure that users have the correct, appropriate, and lowest level of access necessary 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, per CTR policy, in the overall process to mitigate the risk of improper system access and to prevent fraud, waste and abuse.

New FY23 Item

The Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access form will be accessed and completed via the DocuSign platform. Please see the DocuSign section below for more information.

DSO Review and Certification

The DSO's review encompasses both the enterprise systems listed below and all individuals who can approve obligations and expenditures (those with Department Head Signature Authorization (DHSA) to execute contracts, sign off on payroll, incur obligations, authorize payments, etc.) on behalf of a department head, even if that individual does not access enterprise systems directly or regularly. Please refer to the various security reports below to facilitate your users' current enterprise system access and roles.

As part of the review process (and for audit purposes) DSOs must retain records supporting the review process including:

1. Copies of the security reports produced to complete this review

2. Evidence (emails, Teams chats, Sharepoint, etc.) that relevant managers were provided with copies of the security reports for staff, and that those managers confirmed that any changes to current access maintains segregation of duties and ensures that users have the correct, appropriate, and lowest level of access necessary to complete the user's job duties

3. Documentation, annotations, or other records of recommended manager modifications to the security reports

4. A copy of the Department Security Officer Review and Approval of Statewide Enterprise Systems Security form executed through DocuSign that is submitted to the Statewide Risk Management Team confirming and certifying completion of the review process

If 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 these for the documentation of review of reports noted above.

Deactivating Inactive Users, Major Changes in User Roles

CTR's Statewide Risk Management team will contact the DSO to delete system access (and deactivate associated UAIDs) for users who have not logged into the enterprise systems during the prior 12 months. Please ensure that users who utilize the enterprise systems for limited activities, such as close/open transactions, regularly update their passwords to avoid being deactivated.

Failure to promptly deactivate system access is considered both a significant cybersecurity and operational controls risk and is subject to audit findings. 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. DSOs should be coordinating regularly with HR/Payroll staff to be notified immediately of major changes to roles, separations of service and extended leaves.

Enterprise systems and related reports for review:

A. **MMARS/LCM:** The Massachusetts Management Accounting and Reporting System (MMARS), including the Labor Cost Management (LCM) sub-system, supports the financial functions performed by Commonwealth departments.

✓ **Related Mobius reports to review for users with access to MMARS:**

1. ***SECMMARS*:** Displays all active user profiles with their assigned security roles and Department Head Signature Authorization (DHSA) flag(s) if any.
2. ***NMF580W*:** User activity report.
3. ***NMF581W*:** Verification of segregation of duties: encumbrances and payments. Please note that CTR's Statewide Risk Management Team reviews enterprise system role requests in detail to ensure that, when combined, the roles requested do not violate segregation of duties.
4. ***MISRVE10*** (Organized by UAID) **and *MISRVE20*** (organized by last name)**:** These reports show all active UAIDs and enterprise systems to which users have access.

✓ **Related Warehouse views to review for users with access to MMARS:**

1. ***M_USER_ACTIVITY_DETAILS***: This table/view provides details of the user's specific MMARS transaction history.

2. ***M_USER_ACTIVITY_REPORT***: This table/view provides a summary of the user's MMARS transaction history.

B. **HR/CMS:** The Human Resource/Compensation Management System supports time and attendance, human resources, and payroll.

✓ **Related Mobius reports to review for users with access to HR/CMS:**

1. ***SECHRCMS***: Displays all active user profiles with their assigned security roles.
2. ***MISRVE10*** (Organized by UAID) ***and MISRVE20*** (organized by last name): These reports show all active UAIDs and enterprise systems to which users have access.

C. **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.

✓ **Related Mobius report to review for users with access to CIW:**

SECIW: Displays all active user profiles with their assigned security roles.

D. **InTempo:** The Executive Office of Technology Services & Security's online security system, through which your DSO and Security Administrators request access to these enterprise systems.

✓ **Related Mobius report to review for users with access to InTempo:**

SECINTEM: Displays all active user profiles with their assigned security roles.

DocuSign

DSOs will receive two emails from the CTR Risk Management Team (CTR-Risk.Management.Team@mass.gov):

1. The first email will provide instructions on how to initiate the review of the Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access form.
2. The second email will provide the access code needed to start the form in DocuSign.

Access to these reports can be granted to department heads, chief fiscal officers (CFOs), internal control officers (ICOs) and DSOs.

These security reports will be available via Mobius during the first week of December, and the reports will be run again mid-December for you to verify any changes you have made.

DO NOT attach security reports to the DocuSign form. Security forms are highly sensitive and should not be sent to CTR.

Documentation related to your security review should be maintained locally at your department in accordance with your records retention and secure document storage protocols.

Contact for Questions:

Enterprise Applications	Contacts for Security Related Issues
MMARS and HR/CMS	**CTR Security Team** **Phone**: (617) 973-2468 **Email**: Securityrequest@mass.gov
CIW, VPN, and InTempo	**Executive Office of Technology Services & Security End User Service Desk** **Phone**: (844) 435-7629 **Email**:massgov@service-now.com

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