| | |
|---|---|
| To: | Department Heads, Security Officers, and Chief Fiscal Officers |
| Date: | May 16, 2022 |
| From: | Peter J. Scavotto, Assistant Comptroller for Risk |
| Subject: | Department Head Annual Review and Approval of Statewide Enterprise Systems |

Comptroller Memo: FY2022-22

## Executive Summary

Annually, Department Heads must review and confirm: (1) the employees they have authorized to access, process, and approve transactions within the Commonwealth's Enterprise Systems on their behalf; and (2) any other individual(s) from their agency who are authorized to obligate and expend funds (execute contracts, approve payroll, incur obligations, authorize payments, etc.) on behalf of the Department Head, even if those individuals do not directly access the Enterprise Systems themselves, i.e., they do not go into MMARS to execute a transaction but instead may sign a document externally or approve an expense. This is because in addition to being the Commonwealth's financial system of record, MMARS is also the repository of those with delegated Department Head Authority. This certification must be completed and returned to the Office of the Comptroller before the last business day of the fiscal year, which will be Thursday, June 30, 2022, this year.

New Department Heads must approve security roles within 30 days of their appointment. If you have reviewed and approved security for your department and submitted a certification on or after April 1, 2022, either as a new Department Head or due to staffing changes, you have satisfied the requirement set forth in this Fiscal Year Memo.

## New FY22 Item

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

## Department Head Review and Certification

As described in the [Statewide Enterprise Systems Security Policy](#), Department Heads are required to certify security access to the Commonwealth's Enterprise Systems annually in conjunction with the Closing and Opening of the fiscal year. Department Security Officers (DSOs) are also required to certify security access at the end of the calendar year; thus, a formal review is performed every six months. This review covers the Enterprise Systems listed below and should include any individual who can approve obligations and/or

cxpenditures (execute contracts, signoff on payroll, incur obligations, authorize payments, etc.) on behalf of a Department Head, even if that individual does not access these Enterprise Systems.

Non-compliance with the Statewide Enterprise Systems Security Policy and the submission of this required review by the June 30th deadline may result in suspension of the department's access to Enterprise Systems.

Department Heads have legal spending authority for their appropriations and are responsible for assuring that employees' access to automated systems reflects their job duties that such access is as narrow as possible, while also with enough access to complete their job responsibilities. Approval of transactions to "Final" status in the state financial systems serve as a certification from the Department Head to the Comptroller that transactions comply with State Finance Law and the documents are accurate and complete, the expenditures or other obligations are supported by sufficient legislatively authorized funds, are made in accordance with the Department's legislative mandates and funding authority, and comply with all applicable laws, regulations, policies, and procedures.

## Enterprise Systems and related reports for review:

A. **MMARS/LCM**: The Massachusetts Management Accounting and Reporting System, including the Labor Cost Management sub-system, supports the financial functions performed by Commonwealth Departments.
   Related Mobius reports to review users with access to MMARS:
   1. **SECMMARS**: display all active user profiles with their assigned security roles and Department Head Signature Authorization (DHSA) flag(s) if any.
   2. **NMF580W:** User Activity Report**.**
      a) **Related CIW views to further review the details of NMF580W (i.e. query for dates beyond one month)**
         (1) **M_USER_ACTIVITY_REPORT**: This table/view provides a summary of users' MMARS transaction history.
         (2) **M_USER_ACTIVITY_DETAILS**: This table/view provides details of each user's specific MMARS transaction history.
   3. **NMF581W**: This report will show users that have both created and submitted encumbrances and payments**.**
   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.

B. **HR/CMS:** The Human Resource/Compensation Management System supports time and attendance, human resources, and payroll.
   Related Mobius reports to review users with access to HR/CMS:

1. **SECHRCMS:** Display 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 (CIW) 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 users with access to CIW:

1. **SECIW:** Display 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 Department Security Officers and Security Administrators request access to these Enterprise Systems.
Related Mobius report to review users with access to InTempo:

1. **SECINTEM:** Display all active user profiles with their assigned security roles.

Access to these reports can be granted to Department Heads, Chief Fiscal Officers (CFOs), Internal Control Officers (ICOs), and Department Security Officers (DSOs).

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

## DocuSign

Once this memo is issued, Department Security Officers (DSOs) will receive two (2) 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 this certification form.
2. The second email will provide the access code needed to start the form in DocuSign.

As noted in the **Key State Finance Law Compliance Roles and Responsibilities,** DSOs are required to facilitate the Department Head's review and approval of enterprise systems user access. Thus, the first section of the form will require DSOs to acknowledge their participation and assistance.

Once the above emails are sent, DSOs will receive an automated email from DocuSign to initiate and complete the first section of the form. Once DSOs complete this section, Department Heads will receive an automated DocuSign email requesting they review, certify approval of access, and submit the form.

## Evidence of Enterprise Systems access review and certification

Evidence of all Enterprise System access reviews must be maintained at the department. Evidence of such review must be provided upon the request of the Office of the Comptroller and internal/external auditor(s) and includes signing off on each report whether or not there are

any changes annotated.  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 for the annotated Mobius reports noted above.

Department Heads need to review the security reports and/or supporting documents provided by their Department Security Officer (DSO) and approve any changes to be processed.  Using the DocuSign platform, DSOs have the option to attach these in DocuSign for easier access by the Department Head.  Department Heads will be able review these attachments by scrolling down to the bottom of the DocuSign form.

Once both the DSO and the Department Head complete their respective sections, both parties will receive an email confirming the submission of the form.  This email provides the option to download a copy of the completed form.

Please complete this certification no later than June 30, 2022.

## For Questions:

Enterprise Applications Contacts for Security Related Issues

### **MMARS and HR/CMS**
Comptroller's Security Team
Email: Securityrequest@mass.gov

### **CIW, VPN, and InTempo**
Executive Office of Technology Services & Security's End User Support
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:    MMARS Liaisons
        General Counsels
        Payroll Directors
        Internal Distribution