



WILLIAM McNAMARA
COMPTROLLER

Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

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



MEMORANDUM

To: Department Heads, Security Officers, and Chief Fiscal Officers
From: Peter J. Scavotto, Assistant Comptroller for Risk
Date: May 26, 2023
Subject: Department Head Annual Review and Approval of Statewide Enterprise Systems

Comptroller Memo: FY2023-18

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 access MMARS to execute a transaction but instead may sign a document externally to approve an expense, obligation, receipt, or other transaction. This is because in addition to being the Commonwealth's financial system of record, MMARS is also the repository of information about those with delegated Department Head Signature Authorization. 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 Friday, June 30, 2023, 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, 2023, either as a new department head or due to staffing changes, you have satisfied the requirement set forth in this Fiscal Year Memo.

Certification Form Completed Through DocuSign

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 expenditures (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 by failing to submit this required review by the June 30th deadline may result in temporary 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, but also that employees have 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. **SECMARS:** 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.
 - 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:** Verification of Segregation of Duties. 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:** 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 (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:** 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 department security officers and security administrators request access to these Enterprise Systems.
[Related Mobius report to review users with access to InTempo:](#)
1. **SECINTEM:** Displays 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 DSOs.

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

DocuSign

Once this memo is issued, DSOs will receive an email from the CTR Risk Management Team (CTR-Risk.Management.Team@mass.gov) providing instructions on how to initiate the review using the certification form.

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 email is 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 by 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 must review the security reports and any supporting documents provided by their DSO and approve any changes to be processed. DSOs can facilitate this review with the department head in person, or virtually in Teams or Zoom. **All security related documentation is considered highly sensitive and confidential and must be stored and transferred in an encrypted format to prevent this data from unauthorized access. Do not send/store security related documents through email or Teams unless encrypted.**

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

DSOs will facilitate any changes approved by the department head through the normal process to add, delete, or modify security roles.

Please complete this certification no later than June 30, 2023.

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 in managing these systems.

CC: MMARS Liaisons
General Counsels
Payroll Directors
Internal Control Officers
Internal Distribution