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: Thomas Smith-Vaughan, Chief Operating Officer

Date: November 21, 2024

Annual Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access

Comptroller Memo #FY2025-07

Executive Summary

This memo is to inform Department Security Officers (DSOs) of the requirement to complete the Annual Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access by Wednesday, January 8, 2025. In accordance with the Department Head Signature Authorization in MMARS Policy, the Statewide Enterprise Systems Security Policy and the Key State Finance Law Compliance Roles and Responsibilities Guidelines, DSOs are required to review and certify user access to enterprise systems that contain financial, payroll, and related data.

DSO Review and Approval of Statewide Enterprise Systems Security Access

In accordance with CTR's Department Head Signature Authorization in MMARS Policy and Statewide Enterprise Systems Security Policy, departments must assign enterprise security access 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 job responsibilities. The Annual DSO Security Access Review and Approval helps DSOs ensure that their department complies with this requirement.

The DSO Security Access Review encompasses both the enterprise systems managed by CTR and all individuals who can enter, submit and approve obligations and expenditures. Approvals include users with Department Head Signature Authorization (DHSA) to execute contracts, sign off on payroll, incur obligations, authorize payments on behalf of a

department head, even if that individual does not access enterprise systems directly or regularly.

CTR has provided a list of security reports to facilitate a department's review of their users' current enterprise system access and roles in the Annual **DSO Review and Approval of Enterprise Security Job Aid**. These security reports will be available via Mobius by the end of the first week of December, and the reports will be run again in mid-December for DSOs to verify any changes you have made.

As part of the review process, and for audit purposes, DSOs must retain supporting documentation (paper or electronic) of 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.

CTR is not responsible for retaining record copies of department supporting documentation and proof of review. Departments must retain security reports and evidence of your security review locally at your department, in accordance with your records retention and secure document storage protocols.

As part of the annual Internal Control Certification (ICC) process, department heads are required to certify compliance with CTR security access requirements, including the annual DSO Review and Approval of Statewide Enterprise Systems Security Access.

In addition to the annual Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access, department leadership must review and update security roles whenever a user's responsibilities change and must immediately terminate access within 24 hours when an employee is terminated, suspended, transfers or has an extended leave. The Executive Office of Technology Services and Security (EOTSS) Access Management Standard defines an extended leave as more than 90 days. Periodic reviews are necessary to mitigate the risk of improper system access, system security compromises and to prevent fraud, waste and abuse.

Statewide Key Contact - Primary DSO and Back-Up DSO Must be Current

The Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access form will be accessed and completed via the DocuSign platform. The invitation link will be sent to the department Primary DSO listed on the Statewide Key Contacts Listing.

Department Primary DSO and Back-up DSOs are designated using the Key State Finance Law Compliance Responsibilities Update Form. Once the PowerForm is electronically signed by the department head, it will be routed to CTR to update the Statewide Key Contacts Listing.

Departments are responsible for ensuring that Key Contacts, including the Primary DSO and Back-up DSOs are up-to-date on the Statewide Key Contacts Listing. It is important for departments to keep their Statewide Key Contacts Listing current because important CTR information, including DocuSign invitation links and other communications, are sent to the listed Key Contacts.

If updates are needed, please submit a Key State Finance Law Compliance Responsibilities Contacts Update Form no later than Monday December 2, 2024. For resources related to the DocuSign PowerForm, please see: Electronic Signatures - Office of the Comptroller Intranet

When you are ready to update the Primary DSO or Back- Up DSO, navigate to: https://intranet.macomptroller.org/electronic-signatures/#section-14 and click on the link for the PowerForm.

There will be three recipient boxes to enter the correct name and email addresses. Please make sure that the correct email address is entered to ensure that the PowerForm will be sent to the department designee and then the department head:

1. Department Contact – the person filling out the top half of the form – the actual designation(s) and the employing department. Note that most designations are required to be employees of the department for which the designee will be managing security roles. In very limited, temporary exceptions, CTR may approve designees that are employed by another department subject to an

ISA approved for this purpose through CTR that allows a limited, temporary foreign department designation.

2. Key Contact Designee – A place for the designee to sign, acknowledging their designation, and provide their information. The person will also need to review Key State Finance Law Compliance Roles and Responsibilities Guidelines.
3. Department Head – All Key Contact Designees must be approved signed off on by the department head

Deactivating Inactive Users, Major Changes in User Roles

As part of the DSO Review and Approval of Statewide Enterprise Systems Access, DSO's must ensure that users who are not active in the Statewide Enterprise Systems, as well as any user who has separated from service, transferred, or is on extended leave are deactivated. Failure to timely manage security access, including promptly deactivating system access for inactive users, is considered a significant cybersecurity and operational controls risk and a department may be subject to audit findings for weak operational controls.

As part of CTR's desk review process, the Statewide Risk Management Team periodically reviews user access to enterprise systems, and users who have had major changes in roles and have not been deactivated or updated. CTR will contact DSOs to deactivate system access (and deactivate associated UAIDs) for users who have not logged into the enterprise systems during the prior 12 months, and for users that appear to have separated from service or transferred to another department.

DSOs should also refer to the Executive Office of Technology Services and Security Enterprise Information Security Policies and Standards and IS.003: Access Management Standard for the Commonwealth's default information security standards.

Submission of Department Security Officer Review and Approval of Statewide Enterprise Systems Security Access Form through DocuSign

The Primary DSO identified in the Statewide Key Contacts Listing will receive an email with a brief set of instructions for the DSO Annual Approval of Statewide Enterprise System Security Form from securityrequests@mass.gov **on December 4, 2025**.

The invitation email will provide instructions on how to complete DocuSign electronic signature approval and submission. DSOs should review the **DocuSign DSO Annual Review and Approval of Enterprise Security Job Aid** that is available on PowerDMS. See DSO Resources section below.

On the same day, Primary DSOs will receive an email from CTR.DocuSign.Security.DSO_AA@mass.gov with a link to the DSO Annual Approval of Statewide Enterprise System Security Form in DocuSign.

The DocuSign form does not allow attachments. Please DO NOT email any security related information to the CTR Security Team, including copies of the DSO Annual Approval of Statewide Enterprise Systems Security Forms. Security access information is highly sensitive and should not be sent to CTR or outside your department.

DSO Resources Available on PowerDMS.

Please see the following resources that are available on PowerDMS. All DSOs are provided with access to PowerDMS.

- Security Folder:
  - DocuSign DSO Annual Review and Approval of Enterprise Security Job Aid
  - MMARS Security Roles Guide
- HR/CMS Security Roles Guide (available on HR/CMS Knowledge Center)
- Department Security Officer (DSO) Quick Reference Guide

Thank you for your time and cooperation. Your diligence in complying with this policy is vital to mitigating risks inherent to managing enterprise systems. Please direct any questions to: securityrequest@mass.gov.

Cc: MMARS Liaisons
Payroll Directors
General Counsels
Internal Distribution