Date: November 10, 2026

To: Agency Security Administrators

Agency Chief Financial Officers and Accounting Directors

Agency Human Resources Directors

RE: Annual System Security Review and Verification Due Thursday, December 31, 2026

Minnesota Management and Budget (MMB) requires all state agencies to annually review the security roles assigned to their employees in the statewide systems—including SWIFT, SEMA4, ELM, and the EPM Data Warehouse—and to sign and return a verification form. All changes to security roles as a result of the review process as well as signed verifications are due **Thursday, December 31, 2026**, to the MMB Statewide Systems Security Team at sema4.security.mmb@state.mn.us.

This memo provides agency security administrators, chief financial officers, accounting directors, and human resources directors with the instructions and resources needed to complete this annual security review and verification.

Who must complete the annual security review and verification?

An agency's assigned security administrator coordinates the annual security review process and must also sign the verification form. Additionally, an agency's chief financial officer or accounting director must review security roles and sign the verification for SWIFT access and related data in the EPM Data Warehouse. The agency's human resources director must review security roles and sign the verification for SEMA4 and ELM access and related data in the EPM Data Warehouse. Other staff in each agency, such as supervisors, managers, and leaders, may also have responsibilities in their agency's annual security review and verification depending on their agency's internal policies, procedures, and processes.

Policies and procedures

Following is a list of policies and procedures to guide you in the review and verification process.

1. MMB Statewide Operating Policy 1101-07 Security and Access: Requires each agency to designate a security administrator and defines the responsibilities of the administrator.
2. MMB Statewide Operating Procedure 1101-07.1 Agency Security Administrators: Requires the annual security review and verification and provides for other specific security administration processes.
3. MMB Operating Procedure 1101-07.02 Compensating Controls: Details the compensating controls procedures required when incompatible roles exist and cannot be segregated.

Resources

1. **Security role descriptions:**
    i. Role descriptions for SWIFT
    ii. Role descriptions for SEMA4
    iii. Role descriptions for ELM
    iv. Role descriptions and other details for SWIFT, AMA, EPM Data Warehouse, and ELM
2. **SWIFT Security Role Conflict Matrix**: Identifies security roles that should not be assigned to the same individual unless compensating controls are implemented and documented.
    i. SWIFT Conflicting Security Roles (as of 10/01/2020): Outlines each security role and respective conflicts.
    ii. SWIFT CONFLICT MATRIX (as of 10/01/2020) is a graphic representation of which security roles conflict.
3. **Instructions for Statewide Systems Security Administrators:** Provides resources and instructions to agency security administrators.
4. **Instructions for completing the Annual Security Review and Verification** (attached).
5. **Security Verification Form**: Send the completed verification form to the MMB Statewide Systems Security Team via email at sema4.security.mmb@state.mn.us by **Thursday, December 31, 2026**.

New Reports and Queries for SEMA4 and SWIFT Available for Security Review

New tools are now available to help Agency Security Administrators review user access that may fall outside standard row-level security views and to support the annual security review and verification process.

Four new SEMA4 reports provide expanded visibility into user access across Department IDs (DeptIDs) and Agency Codes, including access granted outside of your home agency:

- **Security Access to My DeptIDs**
  Identifies users who have access to the DeptID you enter but who are not part of your home agency.
- **Security Access to Other DeptIDs**
  Identifies users who work under the DeptID you enter but have access to DeptIDs outside your home agency.
- **Security Access to My Agencies**
  Functions like "Security Access to My DeptIDs," but uses Agency Code instead of DeptID. Shows users with access to your agency's DeptIDs who are not part of your home agency.
- **Security Access to Other Agencies**
  Functions like "Security Access to Other DeptIDs," but uses Agency Code instead of DeptID. Shows users employed in the entered agency who have access outside that agency's boundaries.

New SWIFT queries also provide visibility into financial and procurement access—both for users inside your agency with access to other agencies' data and for users outside your agency with access to your data. These queries highlight SetID and financial transaction access that may not appear in traditional HR-based reports:

- **SECURITY_ACCESS_TO_MY_AGENCIES**
  Shows users who have access to your agency's financial data but are not employed by your agency.
- **SECURITY_ACCESS_TO_OTH_AGNCYS**
  Shows users who belong to the agency you enter but have access to financial data for other agencies.

SWIFT voucher entry and approval roles

To strengthen system security and internal controls over state payments, MMB plans to implement a SWIFT restriction in 2027 that will prevent a user from approving a voucher (payment) they also entered ("self-approve") at level 3 (over $100, 000). The security role combinations that may be affected are listed below as well as in the SWIFT Conflicting Security Roles (as of 10/01/2020) document.

Agencies should carefully evaluate these roles, eliminate conflicts (segregate roles) where feasible, and, if such conflicting roles must be maintained, document and enforce adequate compensating controls. Under the changes, a user may retain both voucher entry and approval roles, but the user will be restricted from approving any voucher the user also created over $100,000.

Completing this review and making changes in advance of the deadline will help ensure uninterrupted payment processing at your agency. Please note that MMB does not plan to automatically remove conflicting voucher entry and approval security roles retained by users.

Security Role Name: M_FS_AP_VOUCHER_ENTRY

Relevant conflicting Security Role Names: M_FS_WF_AP_APPR_03

MMB's Accounting Services Division intends to provide additional guidance on the voucher self-approval restrictions in 2027.

Questions?

1. Questions about the annual security review and verification process should be directed to the MMB Statewide Systems Security Team at sema4.security.mmb@state.mn.us.
2. Questions about conflicting security roles and/or compensating controls should be directed to the MMB Internal Control and Accountability Unit at InternalControl.MMB@state.mn.us.

Instructions for completing the Annual System Security Review and Verification

Instructions for Agency Security Administrators

(See the full Instructions for Statewide Systems Security Administrators document here: https://mn.gov/mmb-stat/statewide-systems/security-administrators/asa-instructions.pdf)

1. Coordinate the review and verification process with your agency's other security administrators, chief financial officer or accounting director, human resources director, and any additional staff as needed. If you need the names of the security administrators designated for your agency, contact sema4.security.mmb@state.mn.us.

2. Review the SEMA4 On-Demand Reports for Operator Security for your agency. Spot-check these reports to ensure they provide a complete and accurate list of all users and their assigned security roles for the agency or agencies you administer.

   • **SWIFT Security Roles by User (PFHR5195)**
   This report identifies users' administrative roles in SWIFT, SEMA4, ELM, and the EPM Data Warehouse. Users with only basic SEMA4 and ELM Self Service roles (such as time entry or training registration) are excluded.
   The report is organized alphabetically by user name and lists:
   – Security roles tied to the Employee ID (SWIFT, EPM, ELM)
   – Security roles tied to the mainframe login (SEMA4 administration), if applicable
   The report also includes Row Level Security codes (SEMA4), the Primary Permission List (SWIFT), the user's Department ID, Supervisor Name, and Supervisor Employee ID.

   • **SWIFT Incompatible Security (SQR)**
   This report identifies agency users who have Conflicting Role Pairs assigned in SWIFT, based on the SWIFT Security Role Conflict Matrix developed by MMB Internal Control and Accountability.
   The final pages include the SEMA4 Incompatible Security Reports.
   The report also includes the user's Department ID, Supervisor Name, and Supervisor Employee ID.

   • **Incompatible Security Reports (SEMA4)**
   These seven reports identify agency users with incompatible access assignments in SEMA4. When "Incompatible Security Reports" is selected from the On-Demand Report menu, all seven reports appear in Report Manager:
   – Personal Data/Job Data and Direct Deposit (PFHR5187BI)
   – Personal Data/Job Data and Adjust Retro Pay (PFHR5186BI)
   – Personal Data/Job Data and Mass Time (PFHR5185BI)
   – Personal Data/Job Data and Business Expense (PFHR5184BI)
   – Direct Deposit and Adjust Retro Pay (PFHR5182BI)
   – Direct Deposit and Mass Time (PFHR5181BI)

– Direct Deposit and Business Expense (PFHR5180BI)

3. Run the new reports and queries developed for SEMA4 and SWIFT to verify role security for users across Department IDs and agencies. Print or save the reports.
4. Run the On-Demand security reports (see page 13 of the *Instructions for Statewide Systems Security Administrators*). Print or save the reports.
5. Send these items to your agency's chief financial officer or accounting director for review of SWIFT access and related EPM Data Warehouse information;
    a. SWIFT Security Roles by User report
    b. SWIFT Incompatible Security reports
    c. Output from new security queries
        i. SECURITY_ACCESS_TO_MY_AGENCIES
        ii. SECURITY_ACCESS_TO_OTH_AGENCIES
    d. The verification form
6. Send these items to your agency's human resources director for review of SEMA4 and ELM access and related EPM Data Warehouse information;
    a. SWIFT Security Roles by User report
    b. The seven SEMA4 Incompatible Security reports
    c. Output from new security queries
        i. Security Access to My DeptIDs
        ii. Security Access to Other DeptIDs
        iii. Security Access to My Agencies
        iv. Security Access to Other Agencies
    d. The verification form

Instructions for Agency Chief Financial Officers/Accounting Directors and Human Resources Directors

1. Verify that each employee has the appropriate security roles necessary for the employee's job duties.
2. For users listed on the Incompatible Security reports, either segregate roles or verify that compensating controls are in place and documented in accordance with MMB Operating Procedure 1101-07.02-compensating-controls-procedure.
3. Identify any roles that should be deleted to correct the user's access. List the user name, user ID, and role name exactly as they appear on the SWIFT Security Roles by User Name report.
4. Complete and sign the verification form.
5. Send the signed form and the list of any roles to be deleted to your Agency Security Administrator.

Instructions for Agency Security Administrators

1. Delete any roles identified by the agency's chief financial officer or accounting director and human resources director (see page 11 of the Instructions for Statewide Systems Security Administrators document).
2. Sign the verification form indicating the agency's security review is complete.
3. Send the completed verification form to the MMB Statewide Systems Security Team via email at sema4.security.mmb@state.mn.us by **Thursday, December 31, 2026**. Retain documentation in your agency's records (e.g., lists of security roles to delete; documentation of compensating controls).