Date: May 28, 2024

To: Agency Security Administrators
Agency Chief Financial Officers and Accounting Directors
Agency Human Resources Directors

From: Blake Chaffee, Deputy Commissioner, Enterprise Employee Resources
Paul Moore, Assistant Commissioner, Accounting Services

RE: Annual System Security Review and Verification due August 30, 2024

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 sign a verification form. All changes to security roles as a result of the review process as well as signed verifications are due **Friday, August 30, 2024**, 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. This memo and the deadline for signed verifications is later this year compared to 2023 due to changes to certain reports that now include new data elements, as described below.

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, and 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

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 that are required when incompatible roles exist and cannot be segregated.

Resources

1. **Security role descriptions:**
    a. Role descriptions for SWIFT
    b. Role descriptions for SEMA4
    c. Role descriptions for ELM
    d. Role descriptions and other details for SWIFT, AMA, EPM Data Warehouse, and ELM
2. **SWIFT Security Role Conflict Matrix**: Identifies roles that should not be assigned to the same individual unless compensating controls are implemented and documented.
    a. SWIFT Conflicting Security Roles (as of 10/01/2020): Outlines each role and respective conflicts.
    b. SWIFT CONFLICT MATRIX (as of 10/01/2020) is a graphic representation of which 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 **Friday, August 30, 2024**.

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

1. Coordinate the review and verification process with your agency's other security administrators, chief financial officer or accounting director, human resources director, and other staff as needed. You can contact sema4.security.mmb@state.mn.us if you need the names of the other security administrators designated for your agency.
2. Review the following SEMA4 On-Demand Reports for Operator Security for your agency:
    - **SWIFT Security Roles by User (PFHR5195)** identifies users' administrative roles in SWIFT, SEMA4, ELM, and the EPM data warehouse. Users are excluded if they have only basic SEMA4 and ELM Self Service roles, such as time entry and training registration. The report is in alphabetical order by user name and lists security roles associated with the Employee ID (for SWIFT, EPM, and ELM) followed by those for the employee's mainframe login (SEMA4 administration) if applicable. The report includes the codes for the user's Row Level Security (SEMA4) and Primary Permission List (SWIFT). The report has been updated this year to include the user's Department ID, Supervisor Name, and Supervisor Employee ID.
    - **SWIFT Incompatible Security (SQR)** identifies agency users with Conflicting Role Pairs assigned in SWIFT. These SWIFT conflicts appear on the SWIFT Security Role Conflict Matrix developed by the MMB Internal Control and Accountability Unit. The last pages of the report will include the Incompatible Security Reports (SEMA4). The report has been updated this year to include the user's Department ID, Supervisor Name, and Supervisor Employee ID.
    - **Incompatible Security Reports (SEMA4)** identifies agency users with incompatible access assignments in SEMA4. Seven separate reports are organized by incompatible role pairs (when Incompatible Security Reports is selected from the On-Demand Report menu, all seven will appear in Report Manager):
        - Update/Correct for Personal Data/Job Data and Direct Deposit (PFHR5187BI)
        - Update/Correct for Personal Data/Job Data and Adjust Retro Pay (PFHR5186BI)
        - Update/Correct for Personal Data/Job Data and Mass Time (PFHR5185BI)
        - Update/Correct for Personal Data/Job Data and Business Expense (PFHR5184BI)
        - Update/Correct for Direct Deposit and Adjust Retro Pay (PFHR5182BI)
        - Update/Correct for Direct Deposit and Mass Time (PFHR5181BI)
        - Update/Correct for Direct Deposit and Business Expense (PFHR5180BI)

3. Run the on-demand security reports (see page 15 of the Instructions for Statewide Systems Security Administrators document). Print or save the reports.
4. Send a copy of the SWIFT Security Roles by User Name and the SWIFT Incompatible Security reports and the verification form to the agency's chief financial officer or accounting director for review of SWIFT access and related data in the EPM Data Warehouse.
5. Send a copy of the SWIFT Security Roles by User Name, the seven SEMA4 Incompatible Security reports, and the verification form to the agency's human resources director for review of SEMA4 and ELM access and related data in the EPM Data Warehouse.

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.
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 **Friday August 30, 2024**. Retain documentation in your agency's records (e.g., lists of security roles to delete; documentation of compensating controls).