Security Liaison Handbook for Counties and Tribes

Minnesota Department of Human Services

Updated: December 2024

Warning: This document is owned by the System Security & Access Management (SSAM) Team and contains nonpublic security information that cannot be disclosed to the public. It should only be accessed by authorized Security Liaisons. If you have further questions, please contact the SSAM Team.
See Minnesota Statutes §13.37. Subd. 1(a) and 2.

Table of Contents

Welcome

We are the System Security & Access Management (SSAM) Team and have been performing security functions for a number of systems for many years. The SSAM Team was formed in 2012 when the mainframe security staff from the Child Support (PRISM), Transition Support Systems (MAXIS) and MMIS Divisions merged. In addition to the PRISM, MAXIS and MMIS systems we also provide access management for EBT/FIS eAccess, BOBI Reports, InfoPac/eReports, MEC², MEC² Pro, SIR system, METS (formerly MNsure), MnCHOICES, and various systems within the Department of Human Services. We have a successful history of working with County and Tribal users through our Security Liaisons, and hope to continue this relationship with all of you.

We work with Security Liaisons, instead of the individual users, because it is of utmost importance to know we are working with a "Trusted Source". We want to know that our "Trusted Source" (you) know the person really does have and use that logon ID and the new password will be passed onto the user in confidence. We also need to know that our "Trusted Source" will keep us updated on which user needs access, modify this access if job duties change and let us know when the user's access should be terminated.

We are happy to be of service to you. We are here to answer any questions you may have about your duties as Security Liaisons. Our business hours are Monday through Friday 7:00 am to 4:30 pm. Please don't hesitate to contact us via e-mail at SSAM@state.mn.us with questions.

In early 2018, we began the process of moving to BMC Remedy OnDemand (RoD) as it is the IT Service Management (ITSM) software used at the state. One of RoD's functions is to track our work via the ticketing system. It has been a long-time goal of ours to improve our access request process. This is why we are moving all of our forms into Remedy's Service Catalog and providing all Security Liaisons with access to these forms. Logging into RoD will allow you to:

- Access several forms in MNIT Mall, our Enterprise Service Desk. Forms are updated periodically.
- Submit these forms electronically – no more emailing!
- Create a request with a REQ number in the system
- Track requests, add notes and keep better records of each incident.
- Save time and use the Request Again option for requests that you submit over and over again.

As we move toward RoD, we will be changing our processes and ultimately plan to retire the SSAM@state.mn.us mailbox.

Security Liaison Guidelines

Purpose: Managing Access on Behalf of DHS, DCYF, and MNsure

This guideline supports DHS and State policies related to access management. It describes the Security Liaison's roles and responsibilities regarding managing user access to multiple DHS, DCYF, and MNsure applications. Security Liaisons help thousands of users in more than a hundred partner organizations (Counties, Tribal Nations, and Managed Care Organizations) perform their duties to help improve the lives of Minnesotans.

Key aspects of the Security Liaison model include:

- Partner organization's Human Services Director appoints "Security Liaisons" to prepare and submit its access requests.
- Security Liaisons coordinate all access requests on behalf of users. Users do not request their own access.
- Security Liaisons are authorized and trusted contacts to DHS, DCYF**,** MNsure, and MNIT.
- NOTE: State agencies may appoint "Security Liaisons" to manage staff access. By default, managers, and supervisors act in this role.

Security Liaison Definition

A "Security Liaison" is an appointed contact who is authorized to manage access and related needs on behalf of their agency.

Types of Security Liaisons That Primarily Work With SSAM

There are two types of Security Liaisons that primarily work with SSAM.

- Security Liaisons—Full
- Security Liaisons—Password Only

1. Security Liaison—Full Responsibilities

Agency Security Liaisons' responsibilities include, but are not limited to:

1. Aware of the system roles associated to all the Department of Human Service/MNsure applications.
2. Aware of the business rules associated to obtaining access to all the Department of Human Service/MNsure applications.
3. Review training requirements of both Security and privacy, and role, prior to submitting requests.
4. Request Logon IDs and system access on behalf of their agency.
5. Notify SSAM when staff have left employment or no longer require the same level of access so that unnecessary access may be removed.
6. Distribute pertinent information from SSAM to their agency (e.g., password requirement changes).
7. Follow up on any suspicious access attempts or activity.
8. Notify SSAM when a user is out on leave for more than 30 days.
9. Request SSAM reset passwords for mainframe MNEIAM accounts.
10. Monitor requests submitted via Remedy on Demand (RoD) to SSAM for status and/or additional information that may be needed to complete the request.

11. Maintain access by logging into security accounts on a regular basis to avoid 90 days of inactivity.
12. When a Security Liaison or attesting manager leaves their position, ensure a replacement is appointed. (*See page 7, "Adding, Removing or Modifying Security Liaison Access for Counties and Tribes.")*
13. May support the access recertification process for Department of Human Services/MNsure and other applications throughout the year. See "Access Recertification" section below for details.

2. Security Liaison—Password Only Responsibilities

1. Respond to daily requests for password resets and account unlocks.
2. Monitor requests submitted via MN service hub (RoD) for status and/or additional information that may be needed to complete the requested password resets and account unlocks.

ARS Access Recertification Primary and Backup Security Liaisons Responsibilities

Types of ARS Security Liaisons That Primarily Work with the ARS Team

There are three types of ARS Security Liaisons that primarily work with the ARS team.

1. ARS Primary Security Liaisons (review and attest)
2. ARS Backup Security Liaisons (review and attest)
3. ARS Reviewer Security Liaisons (review only)

Their responsibilities are defined below.

ARS Security Liaison Responsibilities for Access Recertification

The responsibilities for the appointed Access Recertification Primary and Backup Security Liaisons are:

1. From the group of general Security Liaisons, each county appoints one Access Recertification Primary Security Liaison and one Access Recertification Backup Security Liaison. These appointed roles have recertification duties during each Access Recertification cycle for DHS Systems.
2. Larger agencies may need to split access recertification duties by department and appoint an Access Recertification Primary and Access Recertification Backup Security Liaison for each department such as social services and economic assistance.
3. The Access Recertification Primary and Access Recertification Backup Security Liaisons will be the key contacts for the ARS Team. They will be notified via emails prior to and throughout each access recertification cycle.
4. Access Recertification Primary and Access Recertification Backup Security Liaisons must keep track of recertification cycles, arrange for coverage for any Leaves, and be prepared to step in as needed for each other during recertification.
5. Agencies may delegate Security Liaisons to have an ARS "Review" status to help review ARS training compliance by pulling training reports in the ARS application. To delegate, please contact the ARS team.

6. The Access Recertification Primary Security Liaisons complete recertification duties on a timely basis:
    a. Verify that training has been completed, and email staff that are not yet compliant. *Note: Training results take 2-3 days to load into training system and ARS.*
    b. Verify correct role is assigned to each individual.
    c. Review and attest recertification in ARS for all staff (to be completed by the Security Liaison or a supervisor by logging into ARS and finalizing the attestations).
    d. Complete recertifications in the first 4-5 weeks to allow final 1-2 weeks for addressing problems.

    NOTE: ***Access Recertification Backup Security Liaisons completes above recertification duties on*** **a timely basis** when Access Recertification Primary Security Liaison is out of the office on planned or unexpected leave.

7. *ARS Security Liaisons are not allowed to attest for themselves*. Access Recertification Primary and Access Recertification Backup Liaisons attest for each other's recertification.
8. Contact the ARS team for questions, to solve problems, and get help with recertification early enough to allow investigation and problem-solving. Contacts are on the emails you will receive during a recertification cycle.
9. Work with forms and directors to delegate or replace Access Recertification Primary or Access Recertification Backup Security Liaisons or attestation managers. (*See below, page 7, "Adding, Removing or Modifying Security Liaison Access for Counties and Tribes.")*

Training Requirements for Security Liaisons

Security Liaisons must complete the following prior to acting in their new role.

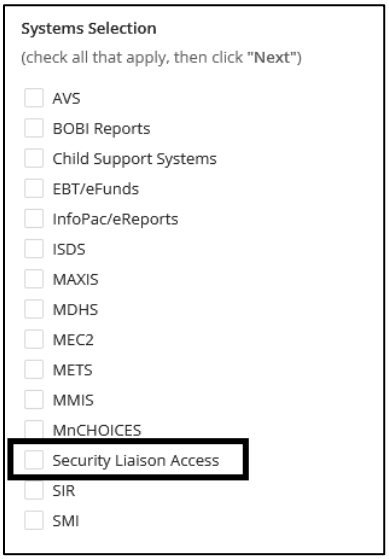
- Review the Security Liaison Handbook
- Complete the Mandated Data Practices and Security Training and assessments
- Complete any role specific training

Adding, Removing or Modifying Security Liaison Access for Counties and Tribes

How do I add a new Security Liaison?

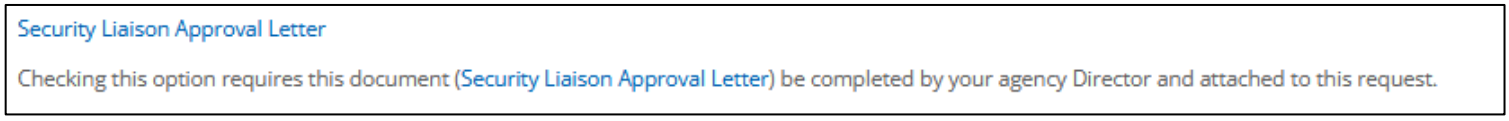
Submit the ***"System Access Request"*** form in the Minnesota Service Hub. (See below.)

1. Check the Security Liaison Access box under Systems.

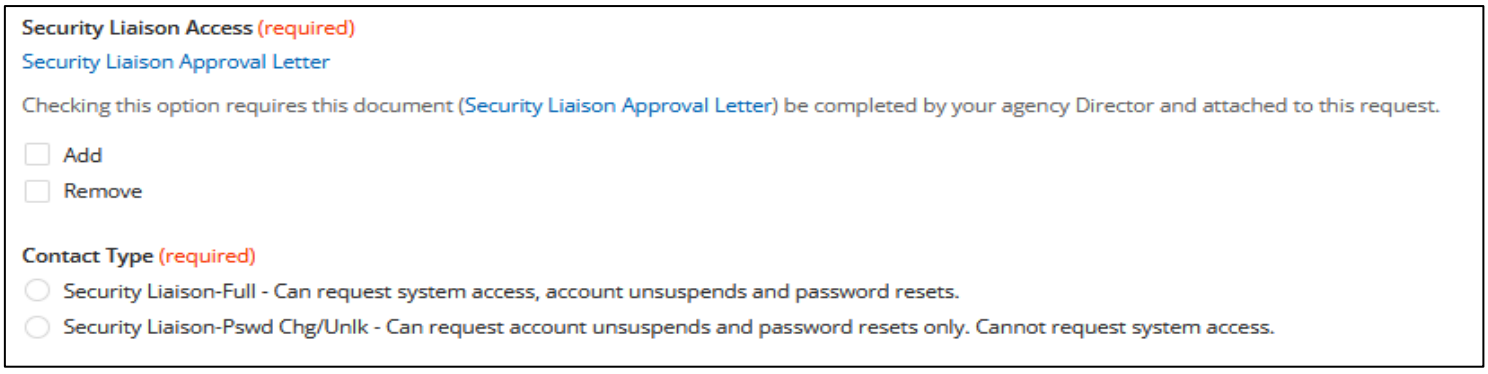


2. Click the Next button to continue.

3. Click on the Security Liaison Approval Letter link and email a copy of this letter to the Human Services Director at your agency. Please have the Director fill out the letter electronically and email it back to you. Attach a copy of the letter to the request when you submit it. Do not submit a scanned copy. If you have been authorized by your Director to appoint new Security Liaisons you do not need to include this letter with your request. (See below.)



4. Check the Add box under Security Liaison Access, then select an option from the Contact Type field. (See below.)



5. Security Liaisons for Counties and Tribal Nations will receive specific access and privileges depending on the Contact Type option selected.
    A. Security Liaison-Full will receive the following access and privileges upon being appointed.

A security liaison with Security Liaison-Full access will be set up with the following access:

DHS-SIR - SIR account added with webmail:

User added to @County-Security group so they can access the SSAM page on DHS-SIR. This group also adds the liaison to the County and Tribal Security liaison distribution lists in webmail.

Added to the @County-TSS-Security group giving them access to MAXIS and MMIS pages on DHS-SIR.

MAXIS - SECC role:

SECC gives access to the FIXT/MPRO function allowing updates to user information fields in MAXIS such as name, supervisor, address, phone and email.

MMIS - FI01 security group:

FI01 (MMIS SECURITY INQUIRY) allows access to look up user accounts in MMIS to view security groups.

FI06 security group:

FI06 (MMIS UNSUSPENDS) allows access to unsuspend/reset passwords for mainframe/ACF2 systems such as Infopac/eReports, MAXIS, MEC2, MMIS and PRISM.

MNEIAM - Admin access in SMI:

Allows access to reset passwords for users in MNEIAM.

Minnesota Service Hub - People record added with Security Liaison-Full access:

Allows user to submit all SSAM forms (Off-board a User, SSAM General Inquiry, System Access Request, System User Maintenance, PRISM COAD Record, PRISM Block and Unsuspend/Password Reset).

The Security Liaison-Full, may be granted additional access and privileges based on your agency needs. Check the Yes Box, to expand each option and select Add to request the additional role(s). Please keep in mind that they require additional training and must be complete prior to submitting the System Access request.

MEC²

☑ Yes

Add M004 role (required)

This is the security liaison update role in MEC². This role requires MEC² Home Page & Navigation TES260 and MEC² Inquiry TES261 training be completed.

☐ Add

☐ Remove

PRISM

☑ Yes

Add SEC position in PRISM (required)

Allows updates to limited information in the user's COPM record. To obtain the SEC position requires that the liaison complete Data Protection for Supervisors in Handling MN Information Securely and Safeguarding Protected Child Support Information CSE023.

User will also be added to @County Child Support Staff group in DHS-SIR.

☐ Add

☐ Remove

Is the Human Services Director of your agency authorizing this Security Liaison to appoint new Security Liaisons moving forward? This means they could appoint new Security Liaisons without the director being involved in the process.

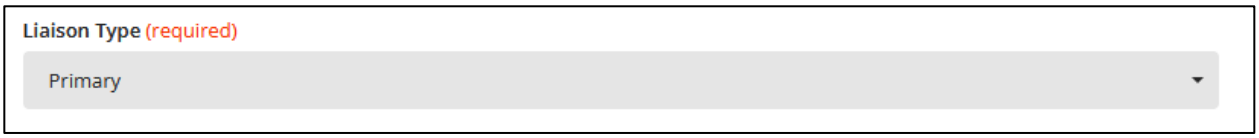
The Security Liaison-Full, may be designated as a Primary or Backup Security Liaison. If your agency has a Primary and a Backup, select none.

Each county/tribe should have one primary and one backup liaison. If your county/tribe does not currently have a designated primary and a designated backup liaison you can go ahead and designate a primary and backup liaison. If your agency already has people filling these roles, please do not designate another primary or backup. The exception to this is that large counties may designate a primary and backup for two departments such as social services and economic assistance.

If you are unsure if your agency already has a primary or backup liaison designated, please look at the Security Liaison lists located on DHS-SIR to find out. Below are links to the lists.

County Security Liaison List
https://www.dhssir.cty.dhs.state.mn.us/SSAM/Lists/Security%20Liaisons/County.aspx

Tribal Security Liaison List
https://www.dhssir.cty.dhs.state.mn.us/SSAM/Lists/Security%20Liaisons/Tribes1.aspx



B. Security Liaison-Pswd Chg/Unlk will receive the following access and privileges upon being appointed. There are no additional access or privileges available for these liaisons.

DHS-SIR - SIR account added with webmail:

User added to @County-Security group so they can access the SSAM page on DHS-SIR. This group also adds the liaison to the County and Tribal Security liaison distribution lists in webmail.

Added to the @County-TSS-Security group giving them access to MAXIS and MMIS pages on DHS-SIR.

MMIS - FI06 security group:

FI06 (MMIS UNSUSPENDS) allows access to unsuspend/reset passwords for mainframe/ACF2 systems such as Infopac/eReports, MAXIS, MEC2, MMIS and PRISM.

MNEIAM - Admin access in SMI:

Allows access to reset passwords for users in MNEIAM.

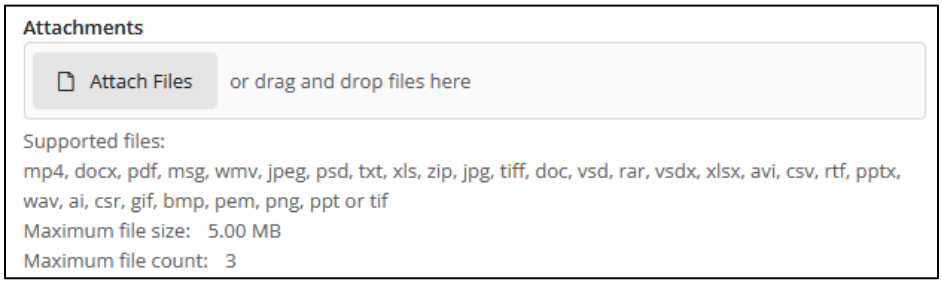
Minnesota Service Hub - People record added with Security Liaison-Pswd Chg/Unlk access:

Allows users to submit the Unsuspend/Password Reset request only. Cannot request system access.

6. How will the requested Security Liaison access be used? (See below)

   You must provide a business reason as to how this access will be used. In addition, this field can also be used for comments or additional instructions.

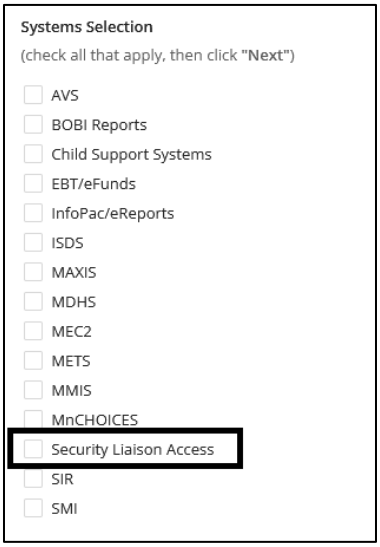
7. Complete any remaining sections of the System Access Request, attach the completed Security Liaison Access letter from your Director by clicking the Attach Files button and submit the request.



How do I modify existing Security Liaison access?

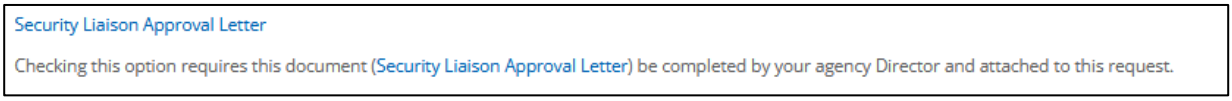
Submit the System Access Request in the Minnesota Service Hub. (See example below)

1. Check the Security Liaison Access box under Systems.

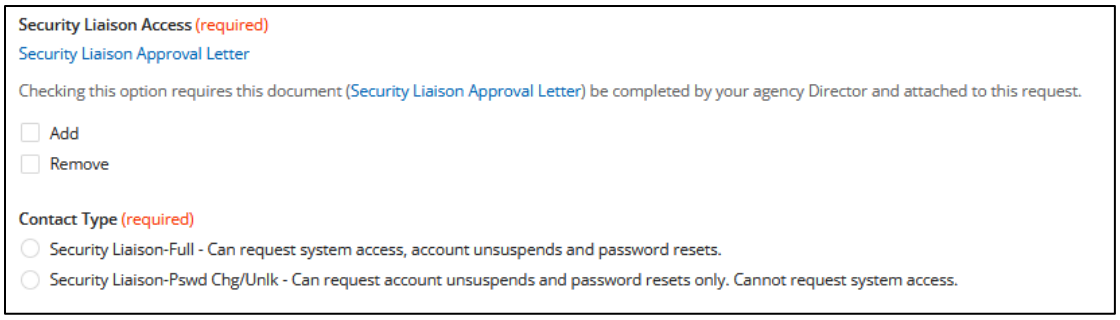


2. Click the Next button to continue.

3. Click on the Security Liaison Approval Letter link and email a copy of this letter to the Human Services Director at your agency. Please have the Director fill out the letter electronically and email it back to you. Attach a copy of the letter to the request when you submit it. Do not submit a scanned copy. If you have been authorized by your director to appoint new Security Liaisons you do not need to include this letter with your request.



4. Check the Add or Remove box based on what changes need to be made under Security Liaison Access, then select an option from the Contact Type field.



5. Security Liaisons for Counties and Tribal Nations will receive specific access and privileges depending on the Contact Type option selected.
    A. Security Liaison-Full will receive the following access and privileges upon being appointed.

A security liaison with Security Liaison-Full access will be set up with the following access:

DHS-SIR - SIR account added with webmail:

User added to @County-Security group so they can access the SSAM page on DHS-SIR. This group also adds the liaison to the County and Tribal Security liaison distribution lists in webmail.

Added to the @County-TSS-Security group giving them access to MAXIS and MMIS pages on DHS-SIR.

MAXIS - SECC role:

SECC gives access to the FIXT/MPRO function allowing updates to user information fields in MAXIS such as name, supervisor, address, phone and email.

MMIS - FI01 security group:

FI01 (MMIS SECURITY INQUIRY) allows access to look up user accounts in MMIS to view security groups.

FI06 security group:

FI06 (MMIS UNSUSPENDS) allows access to unsuspend/reset passwords for mainframe/ACF2 systems such as Infopac/eReports, MAXIS, MEC2, MMIS and PRISM.

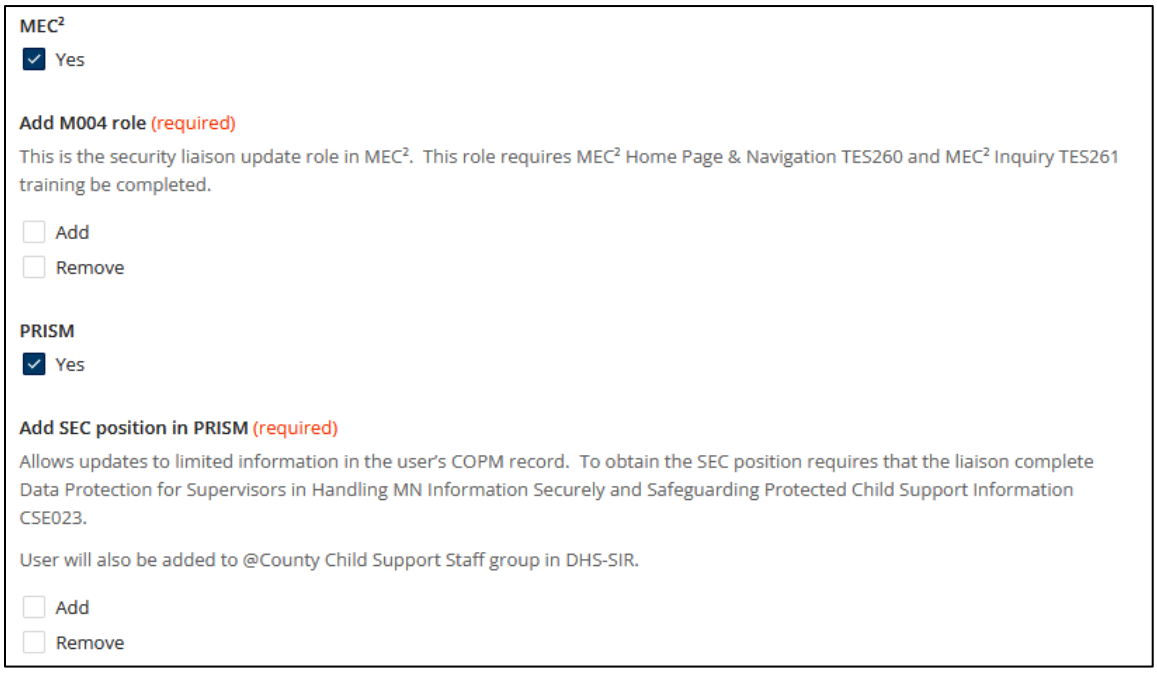
MNEIAM - Admin access in SMI:

Allows access to reset passwords for users in MNEIAM.

Minnesota Service Hub - People record added with Security Liaison-Full access:

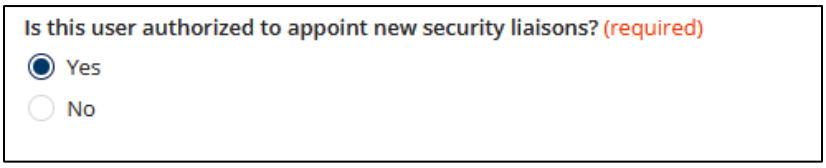
Allows user to submit all SSAM forms (Off-board a User, SSAM General Inquiry, System Access Request, System User Maintenance, PRISM COAD Record, PRISM Block and Unsuspend/Password Reset).

The Security Liaison-Full, may be granted additional access and privileges based on your agency needs. Check the Yes Box, to expand each option and select Add to request the additional role(s). Please keep in mind that they require additional training and must be complete prior to submitting the System Access request.



The Security Liaison-Full, may be granted the authority to appoint new Security Liaisons.

Is the Human Services Director of your agency authorizing this Security Liaison to appoint new Security Liaisons moving forward? This means they could appoint new Security Liaisons without the director being involved in the process.

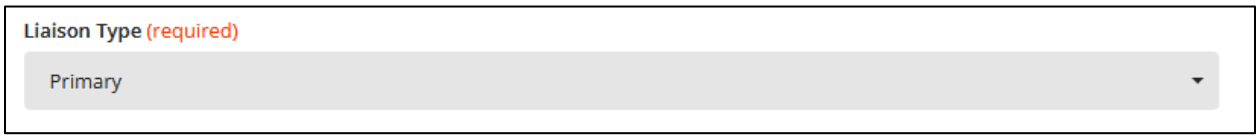


The Security Liaison-Full, may be designated as a Primary or Backup Security Liaison for ARS (Access Recertification). If your agency has a Primary and a Backup, select none.

Each county/tribe should have one ARS primary and one ARS backup liaison. If your county/tribe does not currently have one designated primary and one designated backup liaison you can designate this person as such. If your agency already has people filling these roles, please do not designate another primary or backup.
If you are unsure if your agency already has a designated ARS primary or ARS backup liaison, please look at the Security Liaison lists located on DHS-SIR to find out. Below are links to the lists.

County Security Liaison List
https://www.dhssir.cty.dhs.state.mn.us/SSAM/Lists/Security%20Liaisons/County.aspx

Tribal Security Liaison List
https://www.dhssir.cty.dhs.state.mn.us/SSAM/Lists/Security%20Liaisons/Tribes1.aspx



B. Security Liaison-Pswd Chg/Unlk will receive the following access and privileges upon being appointed. There are no additional access or privileges available for these liaisons.

DHS-SIR - SIR account added with webmail:

User added to @County-Security group so they can access the SSAM page on DHS-SIR. This group also adds the liaison to the County and Tribal Security liaison distribution lists in webmail.

Added to the @County-TSS-Security group giving them access to MAXIS and MMIS pages on DHS-SIR.

MMIS - FI06 security group:

FI06 (MMIS UNSUSPENDS) allows access to unsuspend/reset passwords for mainframe/ACF2 systems such as Infopac/eReports, MAXIS, MEC2, MMIS and PRISM.

MNEIAM - Admin access in SMI:

Allows access to reset passwords for users in MNEIAM.

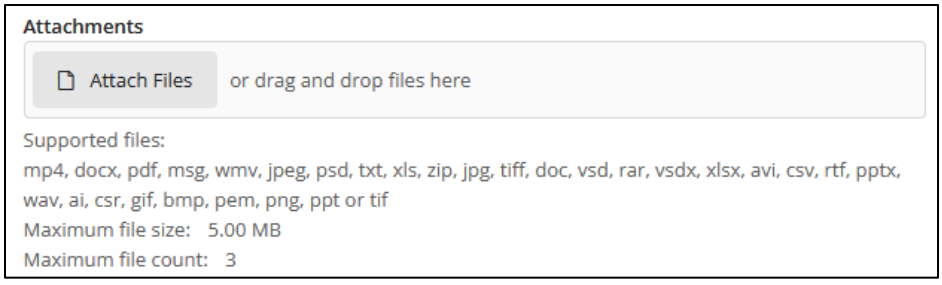
Minnesota Service Hub - People record added with Security Liaison-Pswd Chg/Unlk access:

Allows users to submit the Unsuspend/Password Reset request only. Cannot request system access.

6. How will the requested Security Liaison access be used?

   You must provide a business reason as to how this access will be used. In addition, this field can also be used for comments or additional instructions.

7. Complete any remaining sections of the System Access Request, attach the completed Security Liaison Access letter from your Director by clicking the Attach Files button and submit the request.

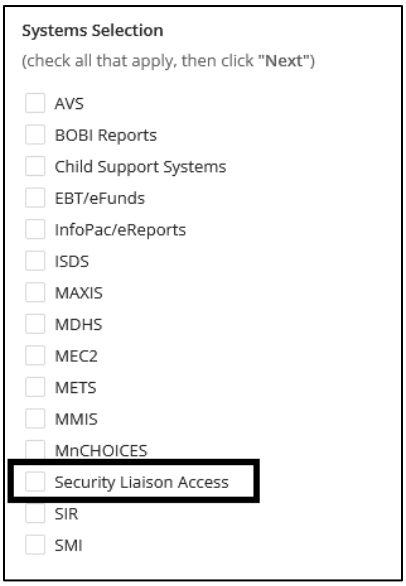


How do I remove existing Security Liaison access?

If the user has ended employment at the county/tribe then submit the Off-Board a User request in RoD so that all their access gets terminated. Please keep the User Request Number, as it is required to be able to replace a Security Liaison.

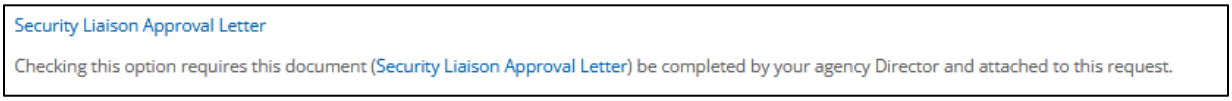
If the user will continue to work at the county/tribe but no longer need Security Liaison access, then submit the *"System Access Request"* in Minnesota Service Hub.

1. Check the Security Liaison Access box under Systems.

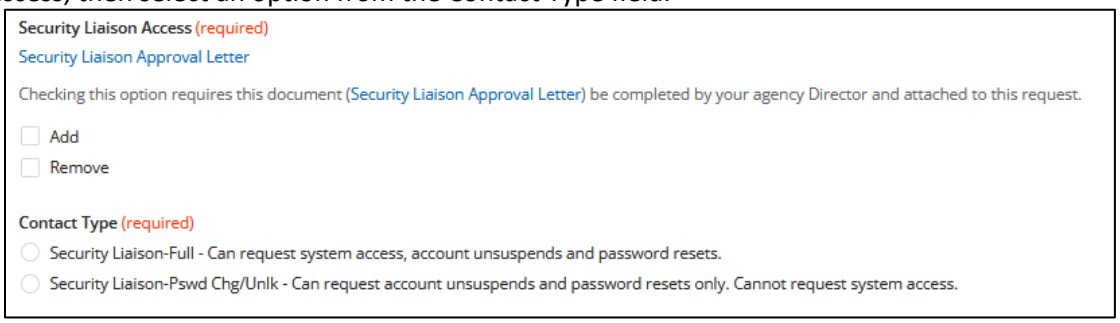


2. Click the Next button to continue.

3. Click on the Security Liaison Approval Letter link and email a copy of this letter to the Human Services Director at your agency. Please have the Director fill out the letter electronically and email it back to you. Attach a copy of the letter to the request when you submit it. Do not submit a scanned copy. If you have been authorized by your director to appoint new Security Liaisons, you do not need to include this letter with your request.



4. Check the Add or Remove box based on what changes need to be made under Security Liaison Access, then select an option from the Contact Type field.

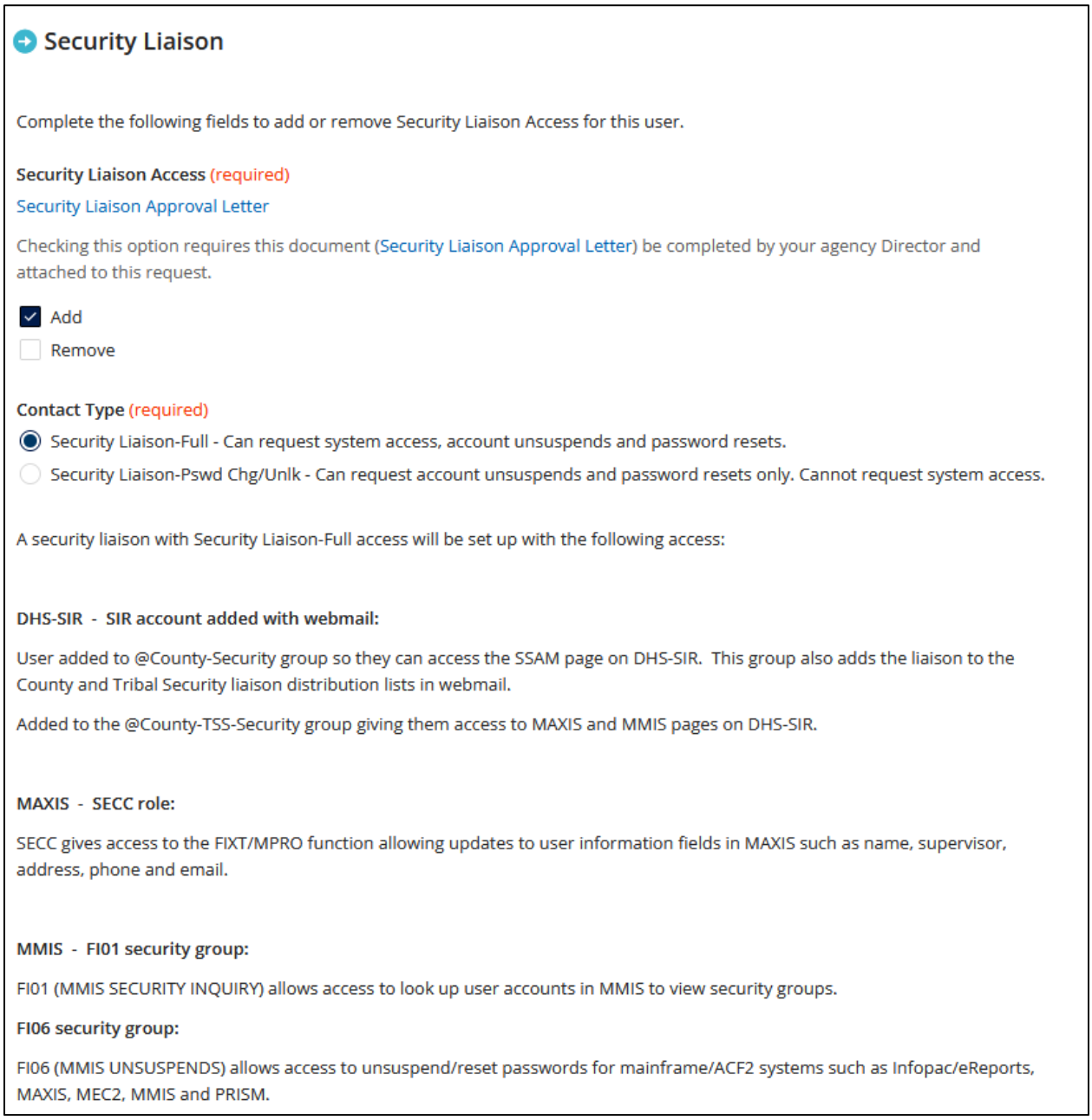


5. How will the requested Security Liaison access be used? Indicate in this field that the user still works at the county/tribe but no longer needs Security Liaison access.

6. Complete any remaining sections of the System Access Request, attach the completed Security Liaison Access letter from your Director and submit the request.

Security Liaison Access Summary of System Access Request Form

Below is an expanded view of the Security Liaison section of the System Access Request



Security Liaison

Complete the following fields to add or remove Security Liaison Access for this user.

Security Liaison Access (required)

Security Liaison Approval Letter

Checking this option requires this document (Security Liaison Approval Letter) be completed by your agency Director and attached to this request.

- [x] Add
- [ ] Remove

Contact Type (required)

- (•) Security Liaison-Full - Can request system access, account unsuspends and password resets.
- ( ) Security Liaison-Pswd Chg/Unlk - Can request account unsuspends and password resets only. Cannot request system access.

A security liaison with Security Liaison-Full access will be set up with the following access:

DHS-SIR - SIR account added with webmail:

User added to @County-Security group so they can access the SSAM page on DHS-SIR. This group also adds the liaison to the County and Tribal Security liaison distribution lists in webmail.

Added to the @County-TSS-Security group giving them access to MAXIS and MMIS pages on DHS-SIR.

MAXIS - SECC role:

SECC gives access to the FIXT/MPRO function allowing updates to user information fields in MAXIS such as name, supervisor, address, phone and email.

MMIS - FI01 security group:

FI01 (MMIS SECURITY INQUIRY) allows access to look up user accounts in MMIS to view security groups.

FI06 security group:

FI06 (MMIS UNSUSPENDS) allows access to unsuspend/reset passwords for mainframe/ACF2 systems such as Infopac/eReports, MAXIS, MEC2, MMIS and PRISM.

MNEIAM - Admin access in SMI:

Allows access to reset passwords for users in MNEIAM.

Minnesota Service Hub - People record added with Security Liaison-Full access:

Allows user to submit all SSAM forms (Off-board a User, SSAM General Inquiry, System Access Request, System User Maintenance, PRISM COAD Record, PRISM Block and Unsuspend/Password Reset).

Additional Systems Access

MEC²

☐ Yes

PRISM

☐ Yes

Is this user authorized to appoint new security liaisons? (required)

○ Yes

○ No

Each County/Tribe should have one primary and one backup liaison. If your County/Tribe does not currently have one designated primary and one designated backup liaison you can designate this person as such. If your agency already has people filling these roles, please do not designate another primary or backup.

Liaison Type (required)

Select

How will the requested security liaison access be used? (required)

(Also add Comments / Additional Instructions here)

What Access is Available to Security Liaisons?

A "Security Liaison" is an appointed contact who is authorized to manage access and related needs on behalf of his/her agency. Use this guide when requesting access.

NOTE: Security Liaisons are added to Security Liaison groups in SIR and to Security Liaison distribution email list. ***There is not a different set of Security Liaisons for each system.***

There are two Security Liaison types that primarily work with SSAM.

1. Security Liaison-Full
2. Security Liaison-Pswd Chg/Unlk

As a designated Security Liaison with Security Liaison-Full access, you will be given access to the following roles.

System	Will be Given Access To	Allows You To
DHS-SIR	Security Liaisons are added to Security Liaison groups in SIR and to Security Liaison distribution email list. There is not a different set of Security Liaisons for each system.	Gives you access to the SSAM page in SIR and content on other SIR system tabs. You will receive emails addressed to the Security Liaison distribution list.
MAXIS	SECC role	Gives you access to the following functions: FIXT/MPRO Function - Allows you to update user information fields in MAXIS such as name, supervisor, address, phone, and email. ROLE/ROLD Function – Look up a role to see what access it provides.
MMIS	FI01 and FI06 security groups **You must specifically log into FI01 and FI06 (not just your ACF^2 account) or after 90 days of non-use these security groups will be removed.**	Gives you access to the following: • FI01 (MMIS SECURITY INQUIRY) – allows you to look up user accounts in MMIS to view security groups – Using FI01 to View Security Groups. • FI06 (MMIS UNSUSPENDS) – allows you to unsuspend/reset passwords for mainframe /ACF^2 systems such as InfoPac/eReports, MAXIS, MEC^2, MMIS and PRISM. Here is a link to instructions - Unsuspend or Reset a Password with the MMIS FI06 Reset Tool.
Remedy OnDemand (RoD)	People record added with Security Liaison-Full Access	Sign in to Remedy OnDemand (RoD) **Security Liaison-Full Access** - submit all SSAM forms (Off-Board a User, SSAM General Inquiry, System Access Request, System User Maintenance, PRISM COAD Record, PRISM Block and Unsuspend/Password Reset). More information about RoD forms
MNEIAM	County/Tribal Admin Access	Gives you the ability to reset passwords for your users in SMI, ISDS-SMRT, and BOBI.

System	May be Given Access To Upon Request	Allows You To
PRISM	Can be assigned a SEC position within their county	Allows you to update some information in the user's COPM record.
MEC^2	M004 role - requires the training MEC^2 Home Page & Navigation TES260 and MEC^2 Inquiry TES261	This is the Security Liaison update role in MEC^2. Similar to the SECC role in MAXIS.

As a designated Security Liaison with Security Liaison-Pswd Chg/Unlk access, you will be given access to the following roles.

System	Will be Given Access To	Allows You To
DHS-SIR	Added to Security Liaison groups in SIR and to Security Liaison distribution email list	Gives you access to the SSAM page in SIR and content on other SIR system tabs. You will receive emails addressed to the Security Liaison distribution list.
MMIS	FI06 security groups **You must specifically log into FI06 (not just your ACF^2 account) or after 90 days of non-use these security groups will be removed.**	Gives you access to the following: • FI06 (MMIS UNSUSPENDS) – allows you to unsuspend/reset passwords for mainframe /ACF^2 systems such as InfoPac/eReports, MAXIS, MEC^2, MMIS and PRISM. Here is a link to instructions - Unsuspend or Reset a Password with the MMIS FI06 Reset Tool.
Remedy OnDemand (RoD)	People record added with Security Liaison-Pswd Chg/Unlk access	Sign in to Remedy OnDemand (RoD) **Security Liaison-Pswd Chg/Unlk access** - submit the Unsuspend/Password Reset request only. Cannot request system access. More information about RoD forms
MNEIAM	County/Tribal Admin Access	Gives you the ability to reset passwords for your users in SMI, ISDS-SMRT, and BOBI. Here is a link for the Security Liaison Administrator Guide for MNEIAM

Other Security Liaison Information

Mainframe rules are as follows:

- Passwords must be changed every 30 days
- After **45 days of non-use your account will be suspended**
- After **90 days of non-use your account will be removed** from the system without any notification to you

It is important for you to log into your accounts on a regular basis, change your password as needed and maintain your access to your accounts. Please add reminders to your calendar if you do not log in frequently (every 89 days) so you do not lose your access to systems.

County Security Liaison List

https://www.dhssir.cty.dhs.state.mn.us/SSAM/Lists/Security%20Liaisons/County.aspx

Tribal Security Liaison List

https://www.dhssir.cty.dhs.state.mn.us/SSAM/Lists/Security%20Liaisons/Tribes1.aspx

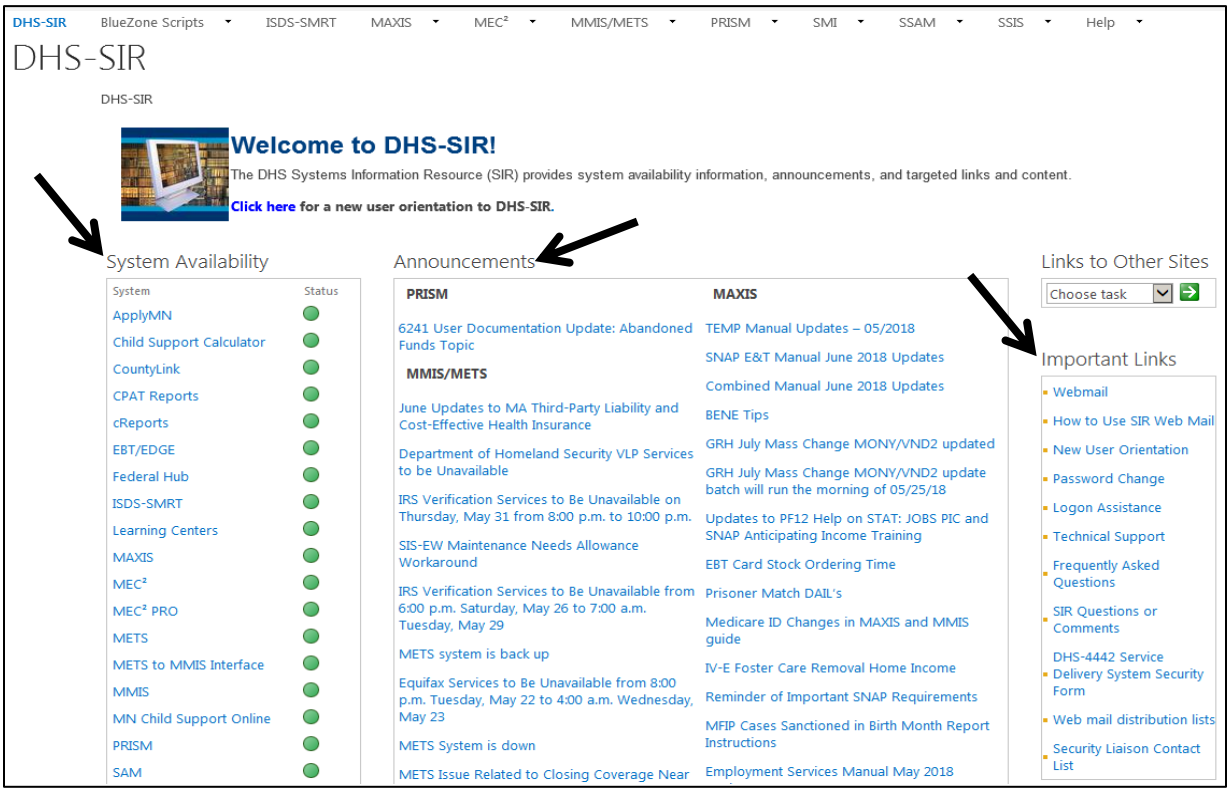
As a liaison, if you ever need system access or a password reset you will need to work through another liaison at your county or tribe as you cannot request these items for yourself.

Resources for Security Liaisons

There are many resources found on the DHS-SIR website https://www.dhssir.cty.dhs.state.mn.us. If you do not have access to SIR, please let us know.

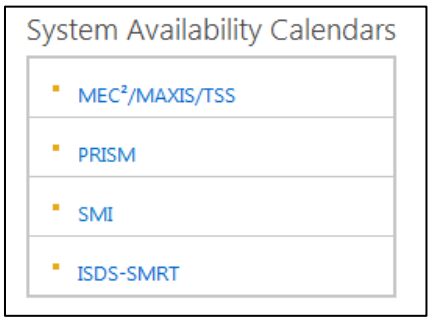
The main page of SIR provides system availability information, announcements, and important links.

SIR Website



The main page also has links to system availability calendars showing planned maintenance and down time.

System Availability Calendars

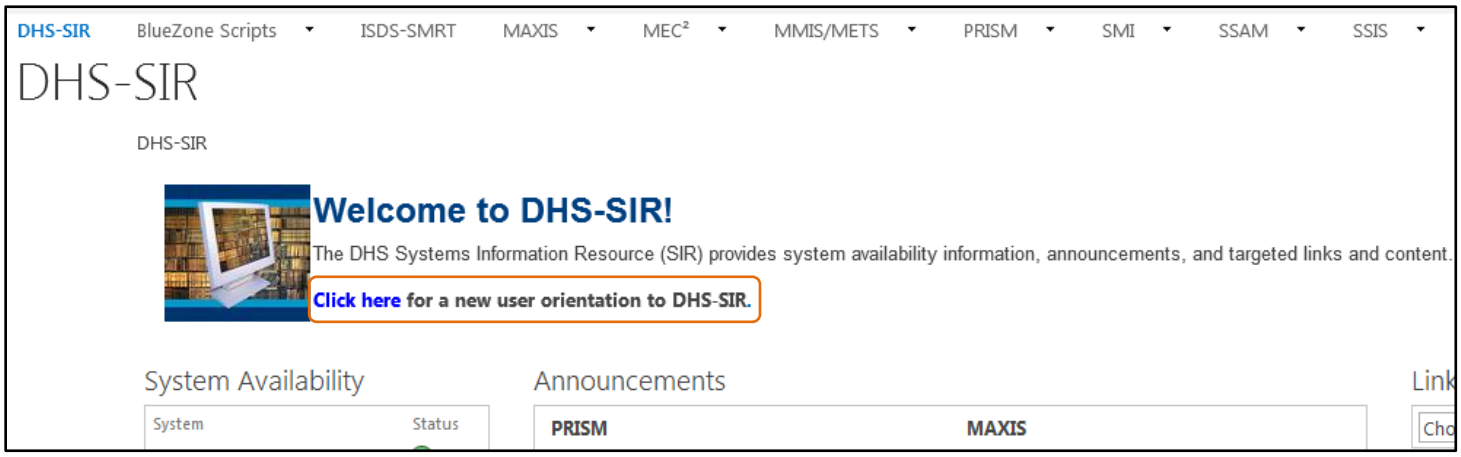


Announcements

You can click on announcements or systems in the System Availability list and set up email alerts to be delivered to your SIR Webmail account if you would like to receive notifications.

New User Orientation

To become better acquainted with the DHS-SIR website login to SIR and open the "new user orientation to SIR."

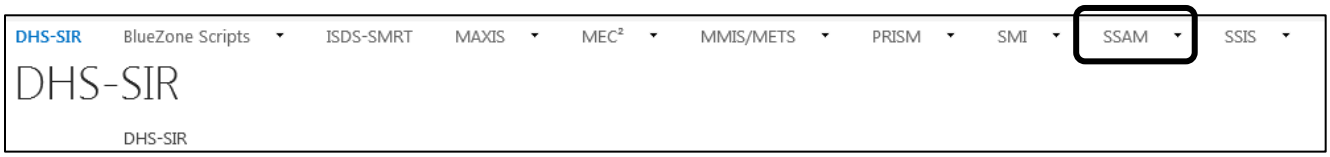


Navigation Bar with System Pages

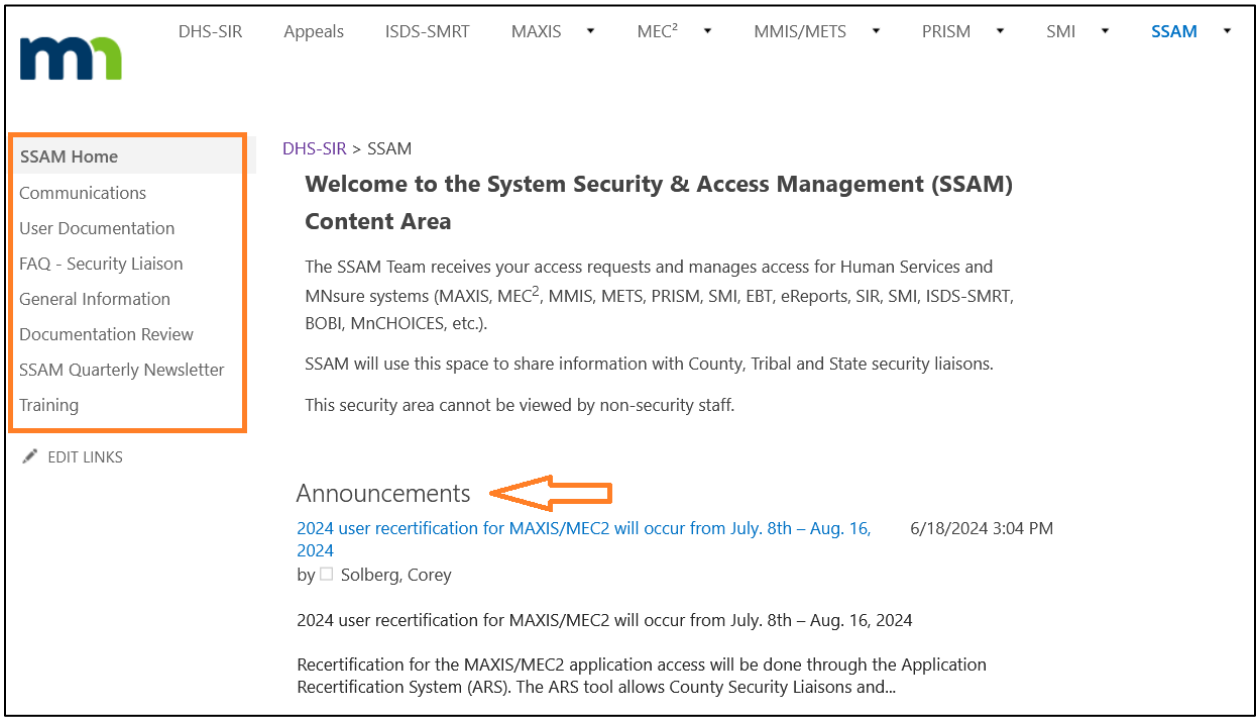
The navigation bar across the top of SIR displays tabs to access other system pages that contain more information regarding each area.

SSAM Page on SIR for Security Liaisons and Program Staff

The SSAM page on SIR is customized for Security Liaisons and is where we place resources designed for you.

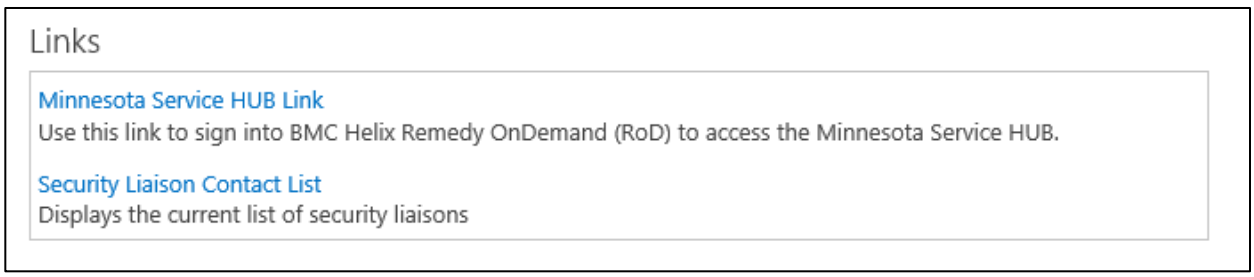


In the left column you will find links to user documentation, the SSAM Quarterly Newsletters, training information, etc. Announcements are posted prominently in the top center.



If you scroll down on the page, you will find a Links section with the following information:

Minnesota Service HUB Link
Security Liaison Contact List



Data Practices, Privacy Laws, and Regulations

Everyone with access to DHS and DCYF systems must understand their obligation to protect the private information contained in these systems. This is one of the major reasons that annual Security and Privacy training are required of all users utilizing DHS and MNsure owned systems.

Here are some links to Federal and State laws regarding data privacy and protecting IRS data.

These policies and laws that govern data practices and security including IRS regulations, Minnesota Government Data Practices Act (DPA), Minnesota Statues 13.46, and the Health Insurance Portability and Accountability Act (HIPAA).

Private data may be disclosed only under specific circumstances. Users that violate privacy rules/laws are subject to a number of sanctions ranging from disciplinary action to civil damages and federal or state prosecution.

Minnesota Data Practices Act

(Minnesota Statute 13.04, Subdivision 2 (45) https://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype+STAT_CHAP&year=2006&section=13. Private data may only be disclosed under specific circumstances. The Minnesota Data Practices act provides for disciplinary action for any government employee who knowingly violates the provisions of the Act. For state employees, the consequences range from a warning, to suspension, and, ultimately firing. Counties set their own disciplinary actions. Any persons, even those who are not employees, who willfully violate the provisions of the Act, can be charged with a misdemeanor.

Taxpayer Browsing Protection Act

Public Law 105-35 105th Congress, HR 1226 August 5, 1997. That law prescribes fines and imprisonment for violations and allows persons harmed to pursue civil damages. See http://www.unclefed.com/Tax-Bulls/1997/PI105-35.pdf any unauthorized disclosure of federal tax information must be reported to the Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) at: Treasury Inspector General for Tax Administration; PO Box 589, Ben Franklin Station, Washington, DC 20044-0589 (312) 866-0620 or 1-800-366-4484.

The Internal Revenue Service

(http://www.irs.gov/pub/irs-pdf/p1075.pdf) IRC Sec. 7431 and 7213 describe civil penalties/damages for unauthorized disclosure of information. Access to IRS data must be restricted to those who need it to do their jobs.

The Health Insurance Portability and Accountability Act

(HIPAA) includes penalties for inappropriate disclosure of PHI (protected health information) http://www.hhs.gov/ocr/privacysummary.pdf .

Minnesota Statutes 13.055 Disclosure of Breach in Security

https://www.revisor.mn.gov/statutes/cite/13.055 addresses notifying the individual if their privacy has been violated.

Minnesota Statutes 13.08 Civil Remedies

https://www.revisor.mn.gov/statutes/cite/13.08 the person damaged may bring an action against the responsible authority or government entity.

Some Systems Overview

ARS (Access Recertification System)
The Access Recertification System (ARS) is a tool in use since 2020, that makes it easier to recertify users access to several key DHS systems including MMIS, PRISM, MAXIS/MEC2, and soon to be MnCHOICES. Information is pulled in from various sources to identify users, supervisors, training status, and assigned roles so that training compliance, user roles, and need for continued access can be easily and thoughtfully verified in ARS. Recertification cycles are six weeks long and run once a year. If a user is not compliant or no longer needs access to the system, a ticket is sent to SSAM to disable access.

AVS (Asset Verification System)
AVS is a web-based service that provides information about accounts held in financial institution such as money market accounts, certificate of deposits as well as savings and checking accounts. AVS does not provide property information. The use of AVS is mandated by federal and state law to help identify unreported assets. Certain Medical Assistance (MA) and Medicare Savings Program (MSP) applicants and enrollees will use the AVS to help identify accounts the person has ownership of by using their name, date of birth, Social Security Number, and geographical location.

BOBI (Business Objects Business Intelligence)
BOBI is the new SAP platform that replaced BOEXI. It is a reporting and analytics business intelligence platform for DHS enterprise use. It delivers Crystal Reports and WebI (Web Intelligence) reports to both internal and external users.

EBT (Electronic Benefits Transfer)
Provides benefits to clients via Point of Sale (POS) terminals in grocery stores and public assistance cash benefits through Automated Teller Machines (ATMs) available through major banking networks. Done to meet federal Supplemental Nutrition Assistance Program (SNAP) requirement (adding cash benefit programs was optional); for purposes of efficiency (replaced paper Food Stamp coupons for all clients and cash warrant filing/handling for clients who chose to receive benefits through EBT); to reduce fraud (coupons could be marketed on the street); and, as a client service (could access benefits online, allowed mainstreaming). EBT passwords are specific only to the EBT system.

FASE (Fraud Application System Environment)
New system that replaced the PIN (Program Integrity Network) application. Gives fraud investigators, collection workers, quality control, and program evaluation staff streamlined access to customized views of multiple data sources through a single, secure portal. PIN accesses source system data from the Data Warehouse or from the source system, depending on the function of the data. PIN provides information from DHS Systems (MAXIS, MMIS and PRISM) as well as from MN Dept. of Employment and Economic Development, MN Dept. of Natural Resources, MN Dept. of Public Safety, Driver and Vehicle Services and Experian Credit Reporting. The SSAM team provisions RSA SecurID hardware tokens (key fobs) to provide two-factor authentication for this program to County and Tribal workers.

InfoPac/eReports
A mainframe report distribution system. Pre-defined reports on warehouse data can be run on a regular basis and displayed or printed in InfoPac. InfoPac Reports are normally administered by the source system that owns the data (E.g. MMIS, MAXIS or PRISM…).

ISDS (Integrated Service Delivery System)
One of four large modernization efforts currently underway at DHS. While ISDS will eventually include several subsystems, for now it includes one, the State Medical Review Team (SMRT) referral system, which was deployed at DHS on January 25, 2016. County deployment of the new SMRT referral system

will begin on March 21, 2016. SMRT conducts disability determinations for people applying for Medical Assistance (MA) or MA-related programs and services. SMRT currently receives referrals from county financial workers via fax. Since the SMRT referral system deployed on January 25, 2016, we have been entering those referrals into the new system. ISDS is accessed through SAM (System Access Management) Oracle Enterprise Identity Management.

MAXIS (Minnesota Access Information System)
Developed to provide automated eligibility results for families who require temporary financial assistance, housing, food, or medical assistance. The system design only allows for a limited number of users. Therefore, MAXIS has an established a policy which may result in denial of access. Users log into MAXIS with their ACF^2 login ID and password.

MDHS (Minnesota Department of Human Services) Menu
Allows the user to have more than one system up and running at the same time on their mainframe session. The user is able to toggle between systems. MDHS can be requested when two or more of the following systems are requested: MAXIS, MMIS, PRISM or InfoPac/eReports.

MEC² (Minnesota Electronic Child Care)
An online Java application created to improve the delivery of the Child Care Assistance Program (CCAP) in Minnesota. The system helps determine client eligibility, pays providers, supports program integrity and tracks child care expenses.

MEC² PRO (Minnesota Electronic Child Care – Provider Resources Online)
Provides access for child care providers to access and submit their bills for child care; integrated directly with MEC² for electronic billing. MEC² PRO streamlines processing, expedites provider payments, and eliminates mailing costs associated with billing--creating savings for counties, providers, and the State of Minnesota.

METS (Minnesota Eligibility Technology System)
The IT system formerly referred to as the new eligibility system or the MNsure IT system. A State of Minnesota system that addresses eligibility for health care coverage.

MMIS (Medicaid Management Information System)
Pays medical bills and managed care capitation payments for DHS-administered Minnesota Health Care Programs recipients, generates DHS program data for research and forecasting, assists in detecting medical fraud, and employs technological solutions to reduce costs and improve services for health care providers. Users log into MMIS with their ACF^2 login ID and password.

MnCHOICES
MnCHOICES is a comprehensive SAS product, supported by FEI Systems, and is Minnesota's person-centered assessment and support planning tool used by counties, tribal nations, and managed care organizations (MCO). A person of any age with a disability or anyone in need of long-term services and supports may request a MnCHOICES assessment and support – a planning process to help make decisions about their needs. MnCHOICES incorporates MnCHOICES assessments, managed care health risk assessment, and support plans associated with both assessments into one web-based application. The person's responses determine eligibility for several public programs including home and community-based services waivers and personal care assistance.

MNEIAM
MNEIAM is our identity management system. Identity management is the management of individual identities, their authentication, authorization, roles, and privileges within or across systems and enterprise boundaries with the goal of increasing security and productivity. METS, SMI, BOBI, and ISDS-SMRT systems are all managed within MNEIAM. Users log into MNEIAM to access all of these systems.

PayNearMe (PNM)
PayNearMe makes it easy and convenient for parents to pay their child support with cash by using PayNearMe at 22,000 trusted locations nationwide, including Casey's General Store, CVS Pharmacy, Family Dollar, and 7-Eleven. You'll need to provide your name and your ten-digit Minnesota child support participant number (also called MCI number) to obtain a PayNearMe PayCode. Child Support professionals can generate a barcode via the PNM Portal. The NCP can take the barcode to a payment location to make a payment.

To make a PayNearMe payment:

1. Get a new PayCode by going to PayNearMe.com/Minnesota
2. Go to any participating store, show the cashier your PayCode, and make a payment with cash
3. The Minnesota Department of Human Services is notified of your payment within 15 minutes. Your payment may take three to four business days to post to your child support account.

*A fee of $1.99 per transaction may apply.

PIN (Program Integrity Network)
PIN was replaced by FASE (Fraud Application System Environment) in 2020.

PRISM (Providing Resources to Improve Support in Minnesota)
A federally mandated system that supports the mission of Minnesota's child support enforcement program: "To benefit children through establishing paternity, establishing and modifying support orders, collecting support and promoting the means to do so." Users log into PRISM with their ACF^2 login ID and password.

SIR (System Information Repository)
A secure webmail and SharePoint system that provides users with current information about multiple DHS systems (PRISM, MAXIS, SMI, ISDS-SMRT, MMIS, METS, MEC^2, etc.)

SMI (Shared Master Index)
Serves multi-need persons and families through better coordination of services and reduces costs through more efficient administration. The SMI provides a search function to prevent duplicate client records across program areas and DHS/County/Tribal systems. This search function enables automated data matching of internal or external system data to DHS person records which allows for administrative efficiencies. It also brings together information from multiple systems into a single client/case profile view and streamlines interchange of information among state, county, and tribal systems. The SMI helps caseworkers, administrators, managers, and policymakers better understand the mix of services that have been (or are being) given to clients and families, as well as service results across programs and periods of time. SMI is hosted on MNEIAM, an Oracle Enterprise Identity Management solution.

SOLQ-I (State Online Query Internet)
An application that allows authorized State agencies real-time online access to the Social Security Number (SSN) verification service and, if permitted, retrieval of Title 2 and/or Title 16 data. SOLQ-I is accessed through the State Master Index (SMI).

VerifyMN
The Department of Human Services electronic verification tool collects client data from a variety of databases and displays the data instantly for use by county, tribal and state staff. VerifyMN aims to provide a single place to collect electronic data to verify client eligibility information for public assistance programs. VerifyMN uses the Shared Master Index (SMI) to connect to data sources and display information. VerifyMN connects with the Department of Employment and Economic Development (DEED) to display quarterly wage data. Unemployment Insurance data from DEED and data from the Social Security Administration is also available.

WebI (Web Intelligence) Reports
A BOBI (Business Objects Business Intelligence) application which is a web browser tool that allows users to perform analysis, produce formatted reports and distribute the reports on BO or export them to a PDF or Excel.

WMS (Waiver Management System)
The Waiver Management System (WMS) is an online tool that DHS developed. Lead agencies use WMS to manage costs for the following home and community-based disability waiver programs:

- Brain Injury (BI)
- Community Alternative Care (CAC)
- Community Alternatives for Disabled Individuals (CADI)
- Developmental Disabilities (DD)

The SSAM Team provisions RSA SecurID hardware tokens (key fobs) to provide two-factor authentication for accessing the Waiver Management System (WMS).

BMC Helix Minnesota Service HUB

BMC Helix Minnesota Service HUB, formerly Remedy OnDemand (RoD), is the IT Service Management (ITSM) software used at the state. February of 2018 marked the rollout of this software as we began to give County and Tribal Security Liaisons access to log into Remedy OnDemand (RoD) to access MNIT Mall in order to submit requests for their agency's staff. MNIT Mall was replaced with the Minnesota Service HUB early in 2021.

Minnesota Service HUB Link

Navigate to this link in your web browser to log into the Minnesota Service HUB

https://chi-rsso1.onbmc.com/rsso/start?bypass-auth=true&tenant=mn-itservices-prod&goto=https://mn-itservices-myit.us.onbmc.com/dwp

For more in depth instructions on logging into the Minnesota Service HUB please refer to the document MN Service Hub - Quick Reference Guide for Counties, Tribes and Managed Care Organizations. These documents are located on the SSAM page of DHS-SIR under User Documentation.

SSAM Forms in the HUB

The following forms are currently available to you in the Minnesota Service HUB:

- **Off-Board a User form**
- **PRISM Block**
- **PRISM COAD Record**
- **SSAM Access Request (state form)**
- **SSAM General Inquiry**
- **System Access Request (formerly the DHS-4442 form)**
- **System User Maintenance**
- **Unsuspend/Password Reset**

For more in depth information about forms please see An Overview of SSAM Forms for Counties and Tribes in Remedy OnDemand (RoD). This document is located on the SSAM page of DHS-SIR under User Documentation.

Requesting Access for Users

The legacy DHS-4442 form or Service Delivery System Request has been retired. This form has been modernized and is now called the System Access Request.

The System Access Request is available in the Minnesota Service HUB.

The System Access Request is used to add new access, modify existing access, or reactivate access to the following DHS Service Delivery Systems:

- AVS
- BOBI Reports
- Child Support Systems (including PRISM, Credit Bureau, DVS e-Services, OCSE Child Support Portal and PayNearMe)
- EBT/eFunds
- InfoPac/eReports
- ISDS
- MAXIS
- MDHS
- MEC^2
- METS
- MMIS
- MnCHOICES
- Security Liaison Access
- SIR
- SMI

When shouldn't I submit a System Access Request? (System User Maintenance Form and Off-Board a User Form)

- To request a new X1 or P9 login ID for a new employee for access to TrainLink (on CountyLink) submit the **System User Maintenance Form**.
- To request a change to user information such as name, address, phone number, supervisor, etc., submit the **System User Maintenance Form**.
- To terminate all access for a user or to temporarily suspend user access, submit the **Off-Board a User Form**.

System Access Request Requirements

When requesting access, it is important to remember the following:

1. Only System Access Requests submitted from appointed Security Liaisons with Security Liaison-Full access for each County/Tribe will be accepted.
2. Only requests submitted via the System Access Request in the Minnesota Service HUB will be accepted.
3. Users must have the Mandated Data Practices and Security Training and assessments with data specific and role specific modules completed - https://data-securitytraining.dhs.mn.gov/Account/Login
4. All MEC² users must complete MEC² Home Page & Navigation TES260 before access is granted. See the SIR system page for more information on training.

5. MAXIS formal training is required for all update access and must be completed within 90 days of access being granted
6. Ensure that a Staff Member Record exists in MnCHOICES before submitting the System Access Request.
7. Include a descriptive business reason in the “how will this system be used?” field on the request.
8. Liaisons cannot request their own access. Another liaison in your county/tribe will need to submit a System Access Request to modify or request new access on your behalf.
9. Enforce proper separation of duties.
    - Do not request security roles that conflict with each other.
    - Some role combinations (such as the Financial Worker plus Accounting) create separation of duty concerns and require County Director approval and a county risk mitigation and oversight plan.
    - Consult with SSAM staff if you have questions about role compatibility.
10. Request only the minimum level of access a user requires to do their job.

If the request meets the required guidelines:

- You should receive a response within 5 business days of receipt of all needed information.
- SSAM will send a response with the logon and password information through the HUB ticket to the Security Liaison who made the request.

Notification of Termination

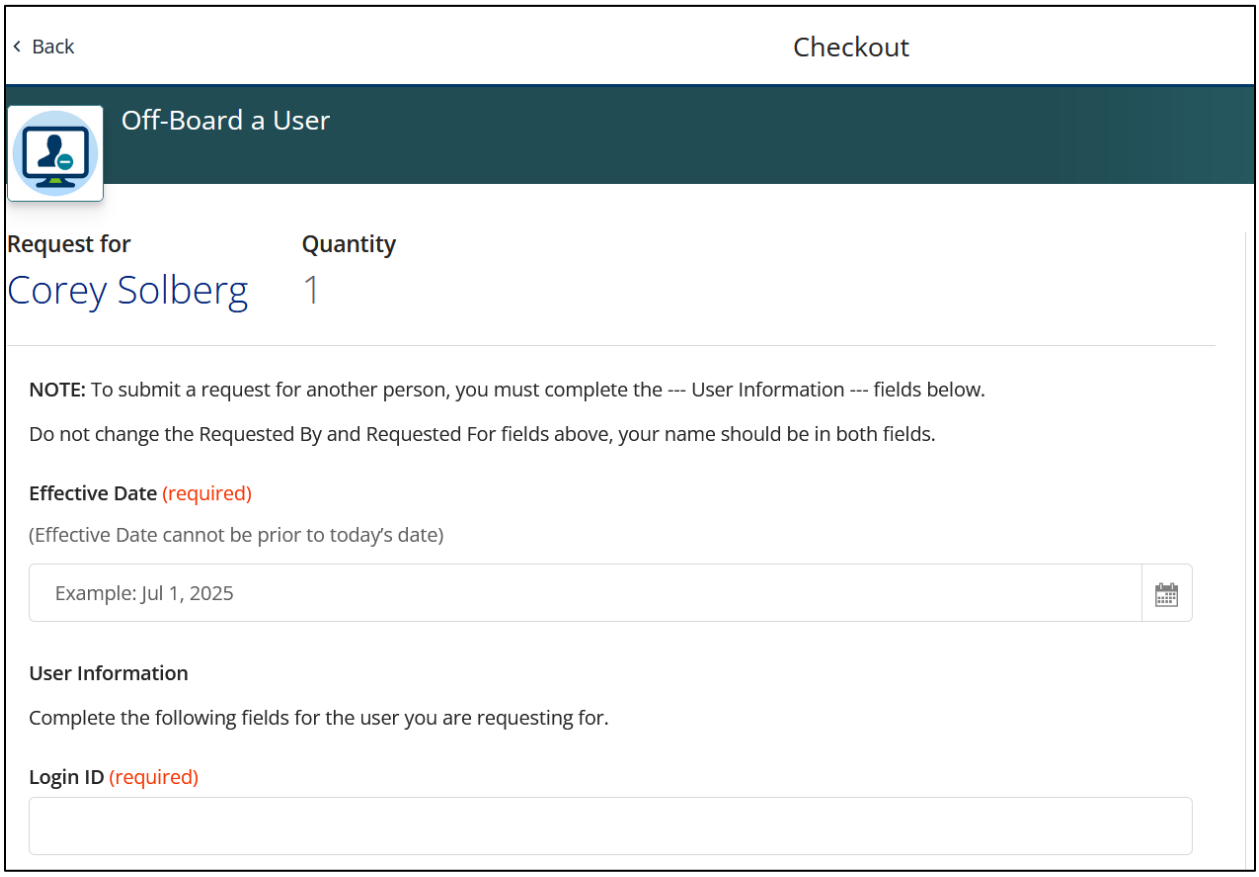
When a person is ending employment at a County or Tribe or if they will be out of the office for an extended period of time on a leave, please submit the **Off-Board a User** request in the Minnesota Service Hub.

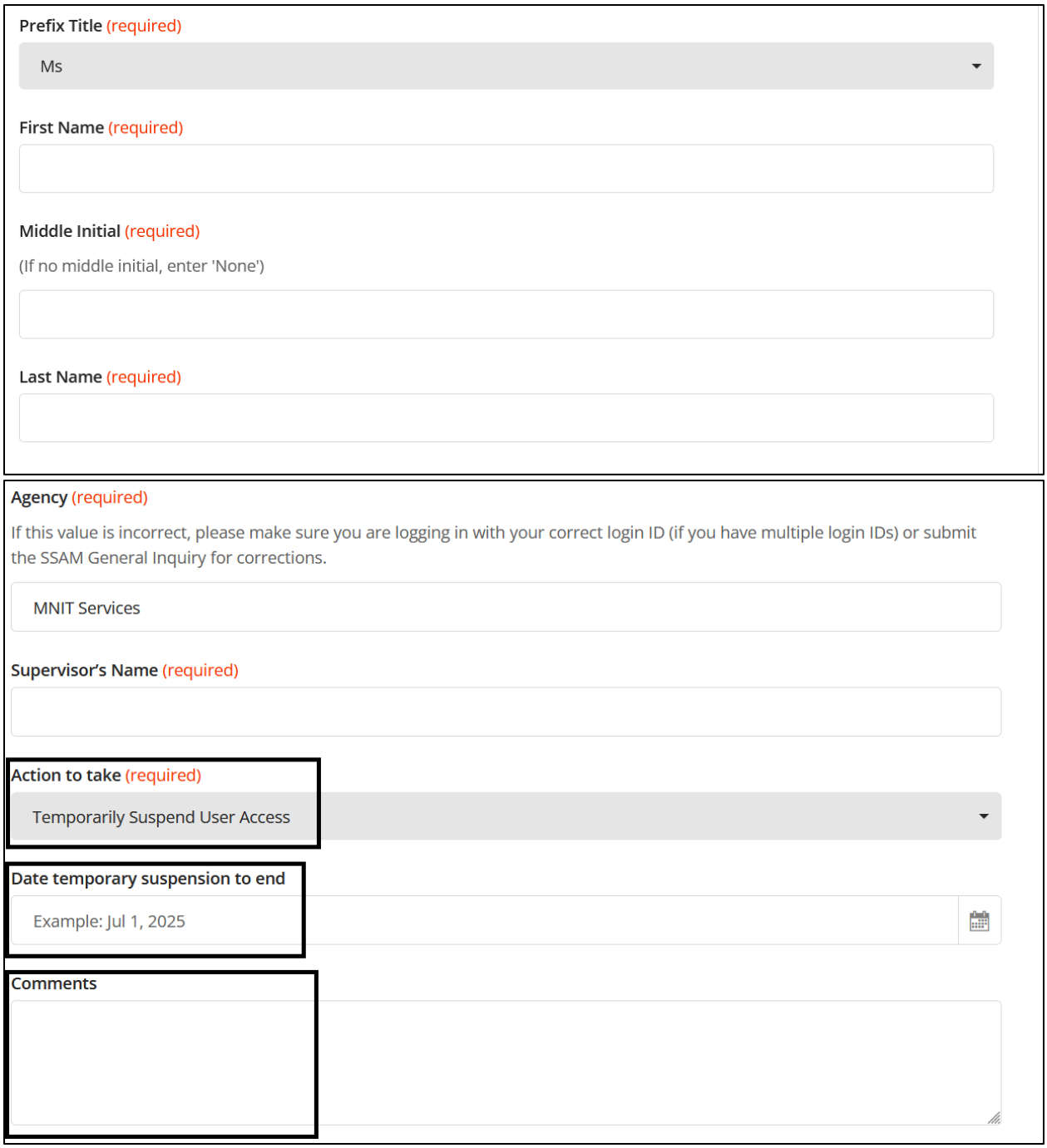
Requesting a Leave of Absence for Staff

A Leave of Absence (LOA) is considered when a person will be out for at least 30 days but no more than 6 months. This will help eliminate accounts from being removed for non-use. Systems affected by a LOA are MAXIS, MMIS, MEC^2, PRISM, Infopac, SIR, SMI (SOLQ-I), ISDS-SMRT, BOBI Reports, Credit Bureau, PayNearMe, DVS e-Services, MnCHOICES, EBT, and METS. If a user has EBT access and does not log in for 45 days the system automatically removes the access. For leaves lasting longer than 45 days EBT access will need to be requested and recreated upon the user's return.

To temporarily suspend user access, submit the Off-Board a User request in the Minnesota Service HUB.

- In the Action to take field choose the **Temporarily Suspend User Access** option
- Enter the expected return date in the **Date temporary suspension to end** field.
- Add any notes in the comments that will help us in completing the request.
- After submitting the request, record the request REQ number as you will need to include this number when you submit the System Access Request to reactivate the user's access upon their return.




Prefix Title (required)
Ms
First Name (required)
Middle Initial (required)
(If no middle initial, enter 'None')
Last Name (required)
Agency (required)
If this value is incorrect, please make sure you are logging in with your correct login ID (if you have multiple login IDs) or submit the SSAM General Inquiry for corrections.
MNIT Services
Supervisor's Name (required)
Action to take (required)
Temporarily Suspend User Access
Date temporary suspension to end
Example: Jul 1, 2025
Comments

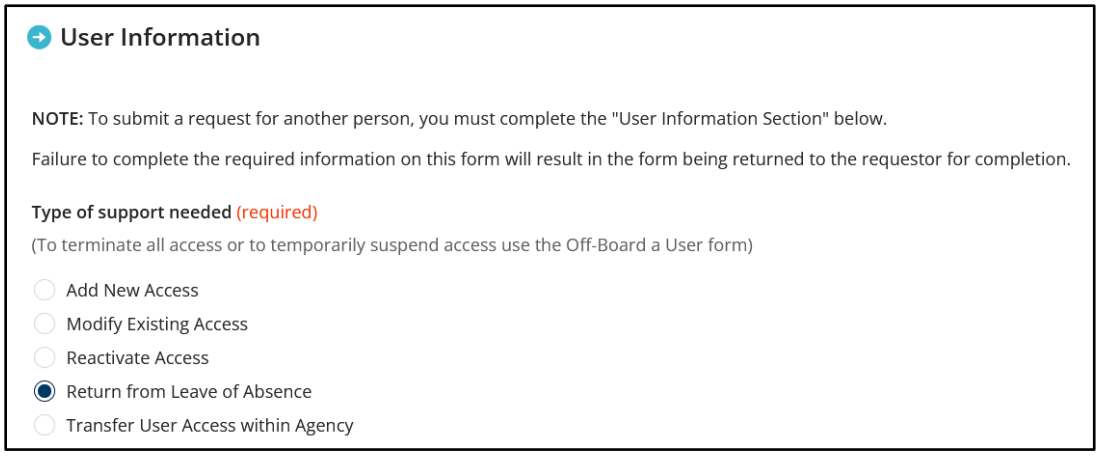
The SSAM team will do the following:

- Add an expire date to the user's **ACF²/mainframe** account. This suspends access to **MAXIS, MMIS, PRISM, MEC²** and **InfoPac**.
- Disable **SIR** account.
- Lock **Credit Bureau**. The account will be locked. This includes **EXPERIAN** and **EQUIFAX.**
- Disable **DVS/E-Services**.
- Disable PayNearMe
- Lock **MnCHOICES.**
- Disable **EBT.**
- Disable **AVS.**
- Disable **MNEIAM**. This suspends access for **SMI, BOBI reports, ISDS-SMRT,** and **METS.**
- Document in the request what systems were affected.

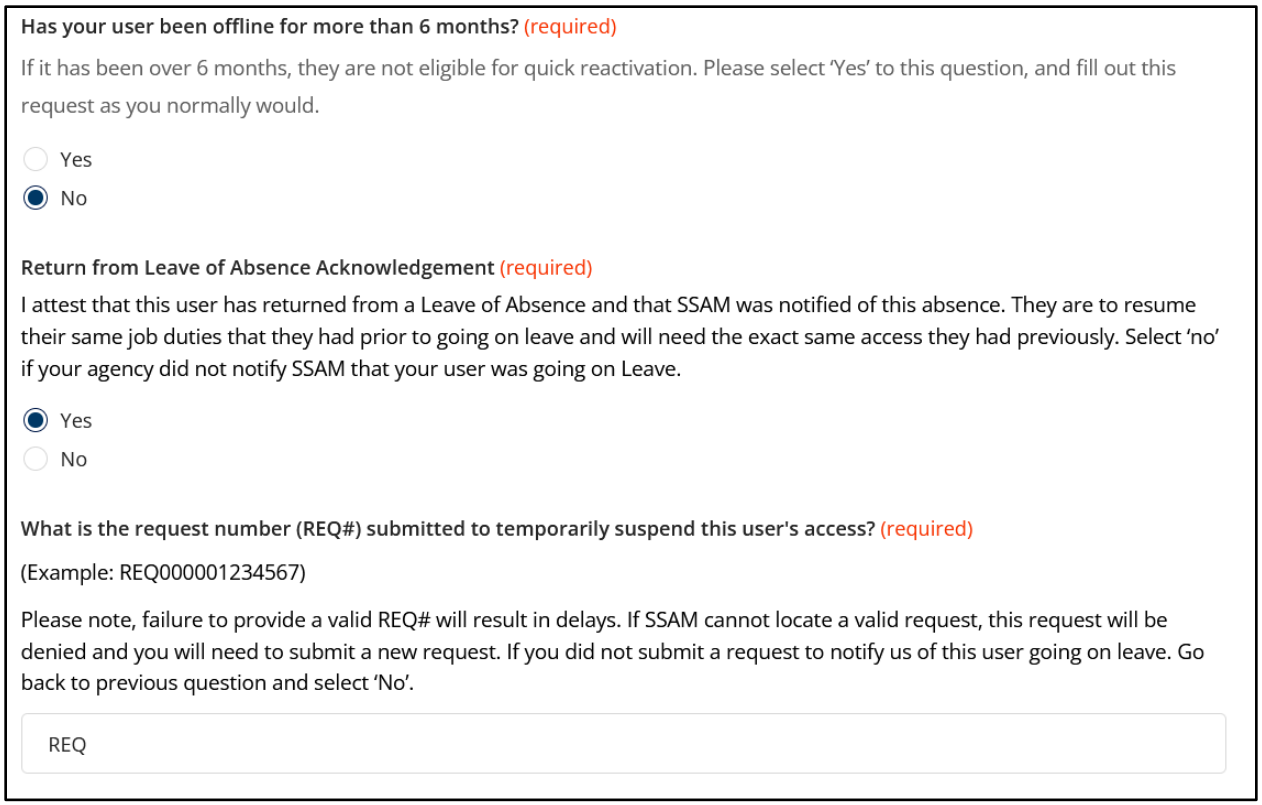
Reactivating Access for Staff Returning from a Leave of Absence

When a worker, for whom you submitted the **Off-Board a User Form** to temporarily suspend access, is about to return from leave, you will need to submit the **System Access Request** in the Minnesota Service Hub. Be certain to select the new option "Return from a Leave of Absence". System Access Requests can take up to 5 business days to process so please submit this request at least 5 days in advance of the worker's return date

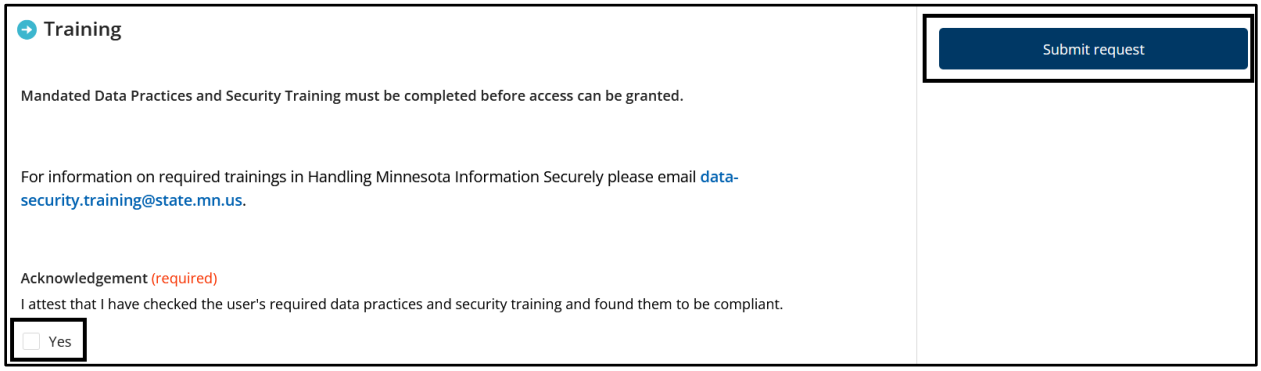
- In the Type of support needed field. Select "Return from Leave of Absence" option.



- Based on the responses to the new questions that appear below, the request may be eligible for a quick submission and not require you to select all the various systems.



- Acknowledge that the user is compliant with the Mandated Data Practices and Security training. You may now click "Submit Request".



Please note, that if SSAM cannot locate a valid temporarily suspend request. The current request will be closed, and notification will be sent to the Security Liaison explaining why. This will require a new System Access request to be submitted and be certain to select "No" for the Return from Leave of Absence Acknowledgement.

Training Requirements

Mandated Data Practices and Security Training

Required training courses have been created to increase compliance with data practices and security and meet federal training requirements for all users with access to DHS information and networks. Supervisors/managers are responsible for ensuring their reports—including staff, contractors, volunteers, and interns—have completed the required training on an annual basis.

There are 3 sets of role-based training modules. Your required modules are tied to the role you selected when you registered. The courses must be taken annually. The modules follow in order, and each has an assessment that must be passed. Each module has instructions for activating the courses and proceeding through the information and assessments.

NOTE: Over time, names can change and new courses may be required for certain users.
As of December 1, 2025, the list of potential training courses are:

1. **Core modules** – required for all for access to DHS information and networks
   Data Security and Privacy – OIS 11000
   How to Protect Information – OIS 1300024
   Managing Information Security – OIS 12000
   Security Awareness – OISSECA23

2. **Data-specific modules** – required for access to specific data types, based on role
   Protecting Everyone's Personal Information: Federal Tax Information (FTI) – OIS 14000
   Protecting Everyone's Personal Information: Social Security Administration Information (SSA) – OIS 15000
   HIPAA Compliance for Everyone: Protected Health Information – OIS 17000
   Payment Card Industry Data Security Standard Training --OISPCARD23

3. **Role-specific modules** – required based on role
   Data Protection for Supervisors – OIS 16000
   Data Security for County Staff and Assistors – OIS 19000
   Data Security for Help Desks and Network Administrators – OIS 20000
   Volunteers -- OIS 18000

   If you have any questions or concerns about the training, please send them to data-security.training@state.mn.us

   Each agency (County or Tribe) must identify at least one person to serve as a **course administrator**, with the ability to monitor compliance of your agency. Contact data-security.training@state.mn.us to set up administrative rights.

TrainLink

TrainLink and the System Access Request are unable to link to each other. These are two completely separate systems with no ability to "talk" to each other.

The link to TrainLink/Training News and Information/Income Maintenance is:
http://www.dhs.state.mn.us/id_007131

Once you are on this site if you click on Training Registration Procedures you will be given the steps on how to get a new worker "known" to TrainLink.

Here are the steps to follow:

Once you have a name and a start date for your new worker:

a. Submit a System User Maintenance form in the Minnesota Service HUB to request a new login ID and training access. Security will not begin until the start date of employment.
b. Contact Tracy Scott (tracy.k.scott@state.mn.us) or Health Care to reserve seats in the training classes that this new worker will need. Mary Omaas will also be helpful: mary.omaas@state.mn.gov.
c. Once you have the X1 ID, go to TrainLink and get the new worker "known" to TrainLink (there is a 2-day turnaround on this, but usually you will hear back the same day)
d. Register the new worker in TrainLink for desired classes
e. For questions of feedback, please contact:
   Tracy Scott, Instructional Design Training Team (IDTT) Supervisor
   Phone: 651/431-4020
   E-mail: tracy.k.scott@state.mn.us
   Or
   Mary Omaas
   Mary.omaas@state.mn.gov

MDHS (Minnesota Department of Human Services) Menu

MDHS is a menu that allows you to toggle between applications. MDHS is provided by MNIT Services and can be requested when the user has access to 2 or more mainframe systems (MAXIS, MMIS, PRISM or InfoPac). MDHS does not pertain to the MEC² Pro system. If a user will not be using MDHS or is waiting for MDHS access to be set up, the following methods can be used to log in.

For Contractors, County Staff, Tribes, Volunteers and Third Party Users:

If the user has previously taken the DHS Data Practices and Security Training, follow the steps in the Returning User list, otherwise, follow the steps in the New User list.

Returning User

1. Go to https://data-securitytraining.dhs.mn.gov/Account/Login
2. Enter your work email address to login.
3. Click "Login"
4. Enter your password
5. Click "Login"
6. Click "Settings" on the "home page".
7. Complete all required fields (indicated with an *) on the Registration page.
8. Click "Update" to be taken to your list of required courses.
9. Begin taking the courses and assessments.

New User

1. Go to https://data-securitytraining.dhs.mn.gov/Account/Login
2. Click on "Register" on the Login page.
3. Complete all required fields (indicated with an *) on the Registration page.
4. Click "Register" to be taken to your list of required courses.
5. Begin taking the courses and assessments.

To access MAXIS:

- For the **Production Region** the user must enter FM at the State of Minnesota screen, logon using their logon ID and password, and then enter FMPP on the next screen.

- For the **Inquiry Region** the user must enter FM at the State of Minnesota screen, logon ID and password then enter FMPI at the next screen.

- For the **Training Region** the user must enter CICSDT2 at the State of Minnesota screen, logon ID and password, and then enter FMTP at the next screen.

To access MMIS:

- For the **Production Region** the user must enter MNCICS1 at the State of Minnesota screen, logon using their logon ID and password, and then enter MW00 on the next screen.

- For the **Skills Region** the user must enter CICSDVA at the State of Minnesota screen, logon ID and password, and then enter MW00 at the next screen.

To access PRISM:

- For the **Production Region** the user must enter CICSPT4 at the State of Minnesota screen, logon using their logon ID and password, and then enter QQPR on the next screen.

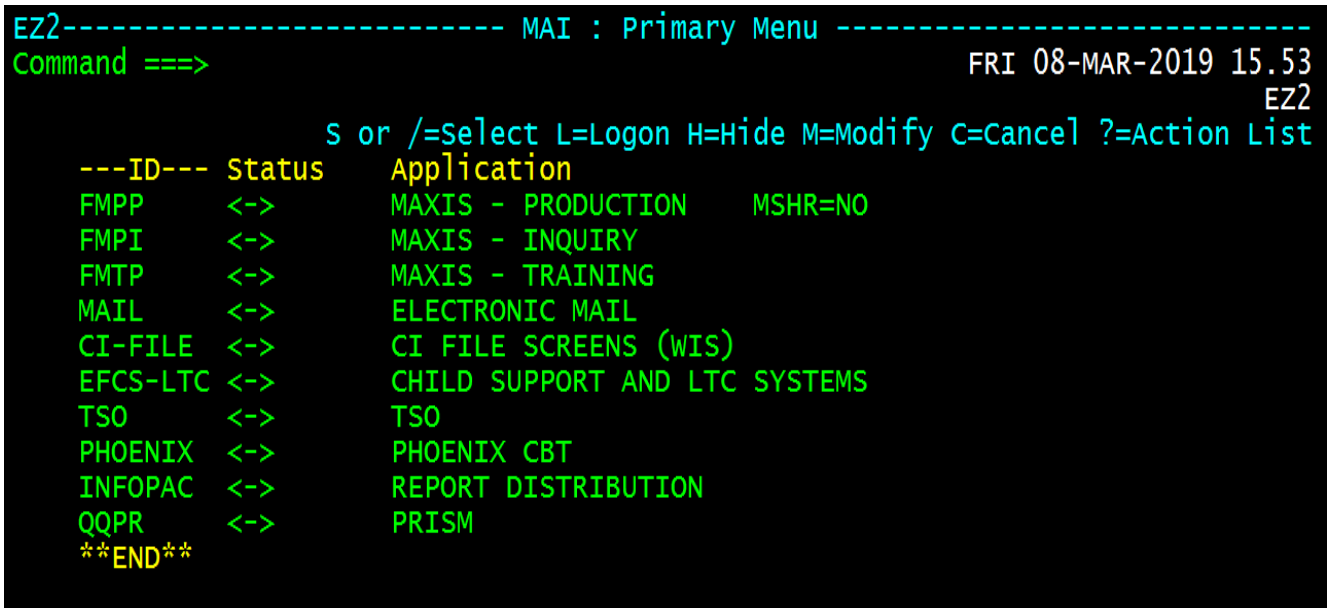
- For the **Inquiry Region** the user must enter CICSPT4 at the State of Minnesota screen, logon ID and password then enter QQPI at the next screen.

- For the **Training Region** the user must enter CICSDT4 at the State of Minnesota screen, logon ID and password, and then enter QQTP at the next screen.

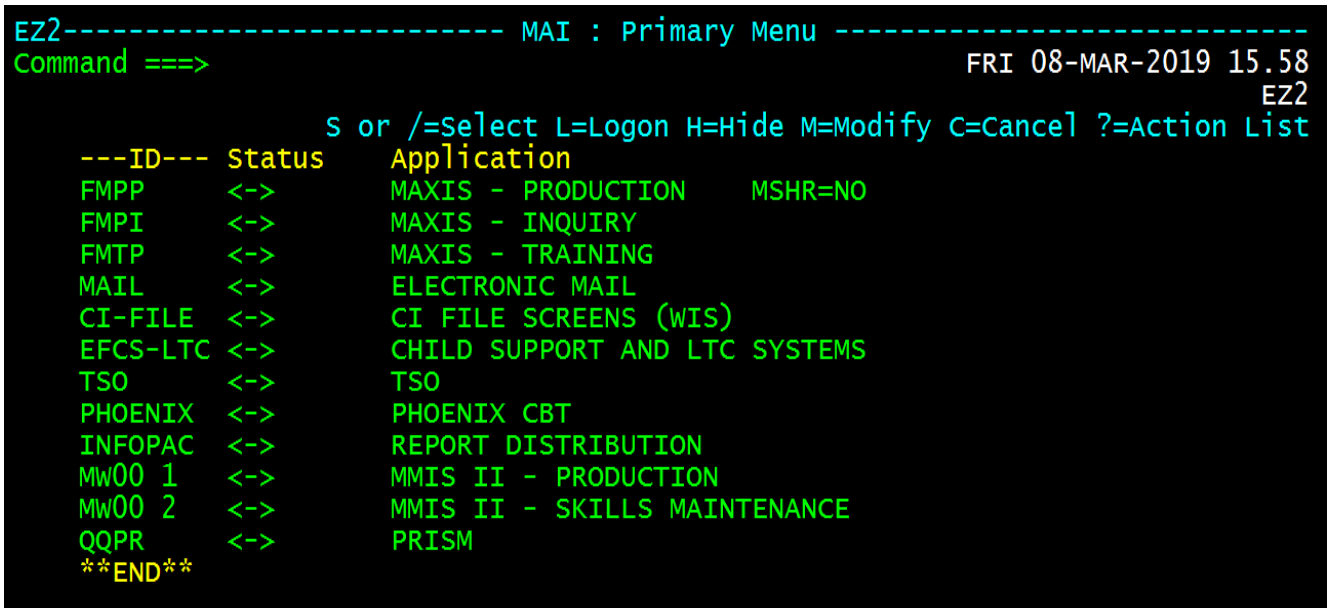
Adding MDHS Menu Permissions

When adding MDHS menu access these are 3 options for the setup. Depending on which menu the user needs the *Copy FROM User ID* field on the SSAM Access Request form should be populated with the logon ID of another user who currently has this same menu. Below is a screen shot of what each MDHS menu looks like.

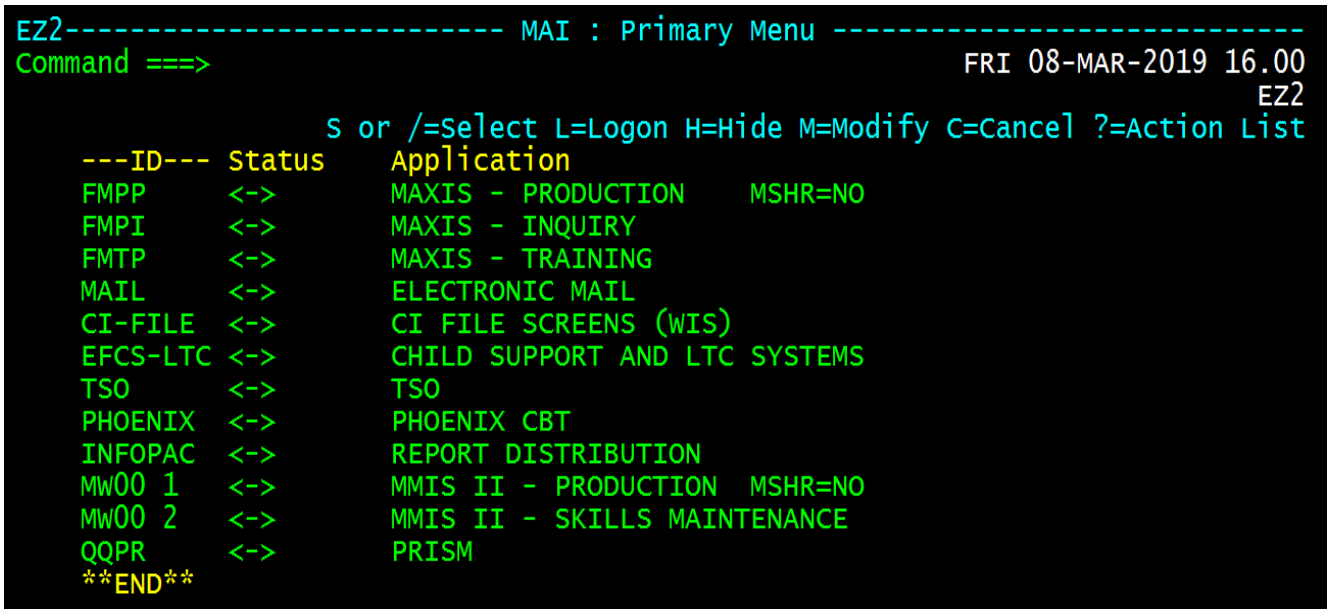
MDHS Menu A
(Session Model - MODDHS1)



MDHS Menu B
(Session Model – MODDHS2)



MDHS Menu C
(Session Model – MODDHS3)



Passwords

Unsuspending a logon/resetting a password

The Unsuspend Password reset form is supported by the SSAM team and the Enterprise Service Desk teams.

- SSAM will receive Unsuspend/Password Reset requests for AVS, e-Oscar, e-Services, EBT, MNEIAM (SMI, ISDS-SMRT, and BOBI), MnCHOICES, Minnesota Service Hub and SIR.
- Enterprise Service Desk will receive Unsuspend/Password Reset requests for ACF^2/Mainframe applications, MNEIAM(METS), and RSA Key Fob.

Users have one password for all mainframe systems: InfoPac/eReports, MEC^2, MAXIS, MMIS and PRISM. A password change completed in any of the above systems will change the password in all the above systems. Users can change a password at any time without waiting for 30 days to expire.

Users may have one password for several MNEIAM systems: SMI, BOBI, ISDS-SMRT, and METS. A please user may have multiple accounts in METS.

To request an unsuspend or password reset for:

- ACF^2/Mainframe (InfoPac/eReports, MAXIS, MEC^2, MMIS, PRISM)
- Asset Verification System (AVS)
- e-Oscar
- e-Services for Driver Information
- EBT
- MNEIAM – SMI, ISDS-SMRT, BOBI reports, and METS
- MnCHOICES (unsuspend only)
- RSA Key Fob (FASE/WMS)
- Minnesota Service HUB
- SIR

Log into the Minnesota Service HUB to submit the Unsuspend/Password Reset request.
NOTE: The Unsuspend/Password Reset queue is monitored Monday through Friday between 7:00 am and 4:30 pm and has up to a 2-hour response time.

If the user is experiencing difficulties logging in or receiving error messages, please submit the "SSAM general inquiry" request and select the "Receiving error message(s)" option.

Password standards for mainframe systems

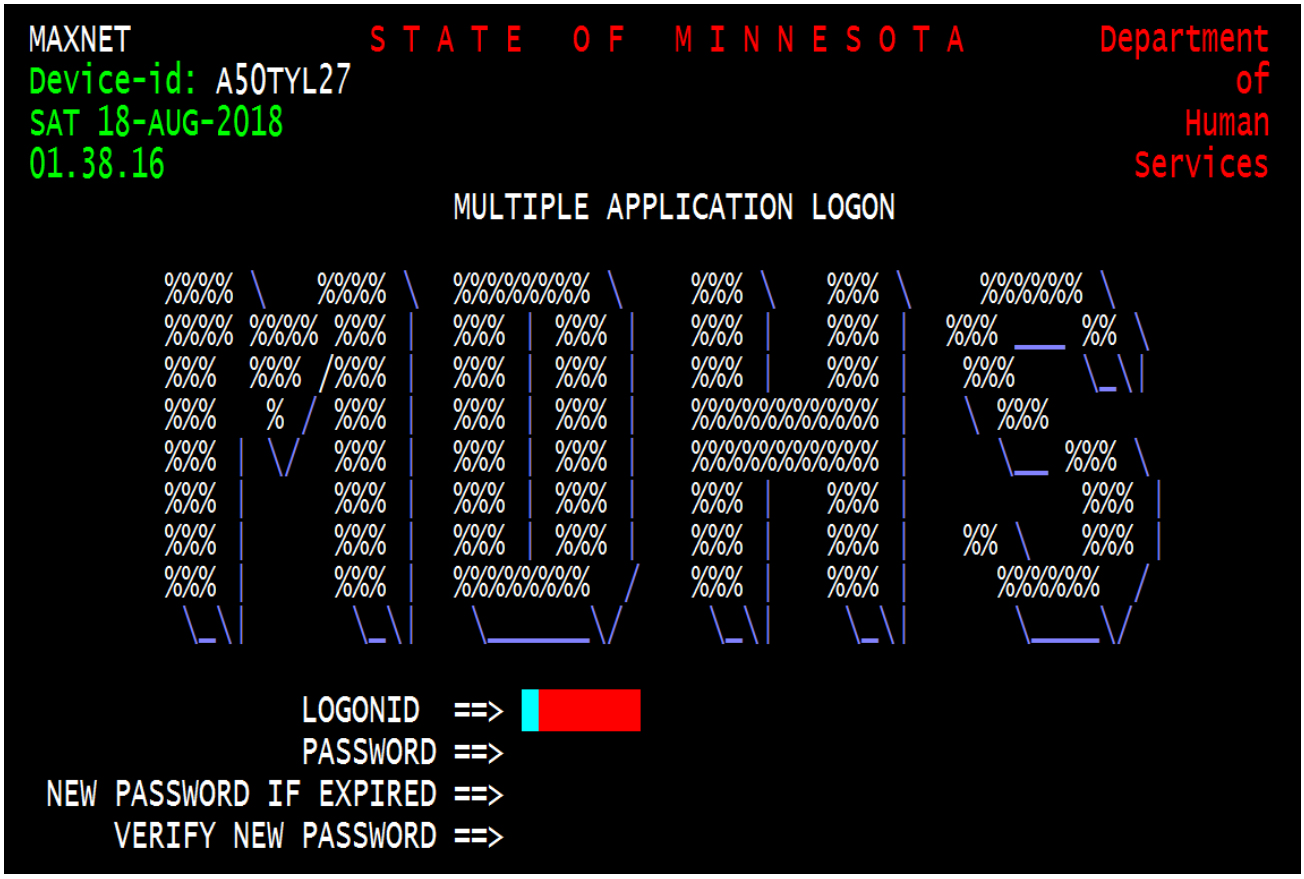
Mainframe passwords requirements:

- Passwords must be exactly eight (8) characters long.
- Passwords must contain at least 1 alpha character.
- Passwords must contain at least 1 numeric character.
- Passwords must contain at least 1 of the following special characters: * $: = - ! . % ? @ # _ &
- The special character cannot be the first or last character of the password.
- Passwords must be retained for a minimum of 5 days.
- Passwords must be changed every 30 days.
- Passwords cannot contain 2 of the same characters in a row (ex: r@bbit35 would not be accepted).
- Passwords cannot be reused for at least 24 password cycles (changes)

Changing Temporary Passwords

The user will need to change the temporary password the first time they log into the mainframe. Follow these steps if logging in through MDHS:

- LOGONID ==> type in your X1 logon ID
- Press the Tab key
- PASSWORD ==> type in the temporary password that you were given
- Press the Tab key
- NEW PASSWORD IF EXPIRED ==> type in a new 8 character password
- Press the Tab key
- VERIFY NEW PASSWORD ==> type in your new password again
- Press the Enter key



Follow these steps if logging directly into a region on the mainframe:

- LOGONID: ==> type in your X1 logon ID
- Press the Tab key
- PASSWORD: ==> type in the temporary password that you were given
- Press the Tab key
- NEW PASSWORD: ==> type in a new 8 character password
- Press the Tab key
- (enter twice) ==> type in your new password again
- Press the Enter key

The message Password Successfully Altered displays

Know the Difference between a Suspended and Expired Password

Know the difference between 'Suspended' and 'Expired' passwords. Have the user clarify the message they are receiving.

- If the message indicates their password is 'Expired' it means the temporary password assigned by DHS has not been changed.
- If the message indicates the password is 'Suspended', you must submit the Unsuspend/Password Reset form to have the account unsuspended.

Other Information about Mainframe Passwords

- Temporary passwords are good for 4 weekdays but not over the weekend.
- If a temporary password has not been used after 4 weekdays or by Sunday night, the user ID will be suspended.
- If the person is not starting employment until Monday, please let us know so we can put an active date on the ACF^2 record so it will be ready for them to use on Monday.
- Incorrect passwords are counted throughout the day
- Users will be prompted to change their password every 30 days
- After 45 days of non-use the user will be suspended on the system
- After 90 days of non-use the user will be removed from the system without notification to user or Security Liaison.
- The system keeps track of your password history. You must use 24 different passwords before the first password can be reused again.

Password Standards for DHS-SIR

SIR doesn't timeout so if you include opening SIR and SIR Webmail in your morning routine, it will remain available on the lower taskbar of your browser window throughout the day.

- As of early 2025, users are required to reset your SIR password every 90 days.
- In 2025, a new piece of software will remind users of their deadline to change their password and send countdown reminders along with a link to the Password Change page.
- You can also change your SIR password by clicking on the Password Change link under Important Links on the DHS-SIR home page. See instructions in the next section.
- Passwords need to be a minimum of 8 characters and include:
    - At least 1 capital letter (A through Z)
    - At least 1 lower case letter (a through z)
    - At least 1 number (0 through 9)
    - At least 1 special character (* $: = - ! . % ? @ # _ &)
- It cannot contain your logon/user ID or parts of it
- The system keeps track of your password history so you cannot change your password to the one you used last time.
- You'll be suspended if you enter your password incorrectly 5 times in 15 minutes.
- You will not receive a suspended message. Instead, a blank window will display. After a 15 minute wait you can try logging in again.
- SIR allows you to attempt to authenticate your password 5 different times for a total of 25 times before SIR will lock you out for the day.
- After being locked out for the day you may wait and try again the next day if you are confident that the password you are using is correct. Otherwise, contact your Security Liaison to request a password reset for you.

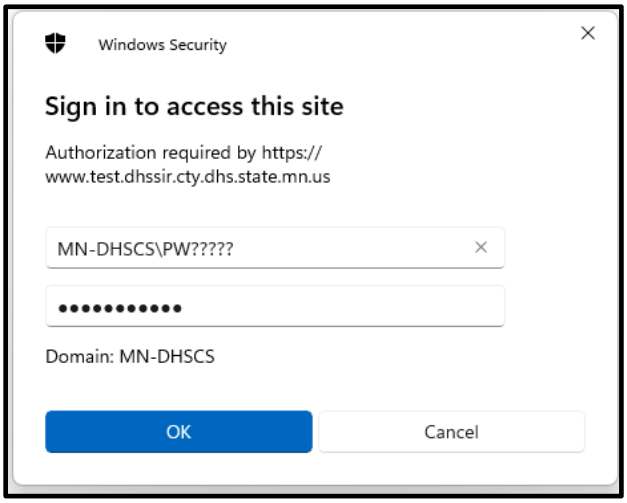
SIR Logon Process

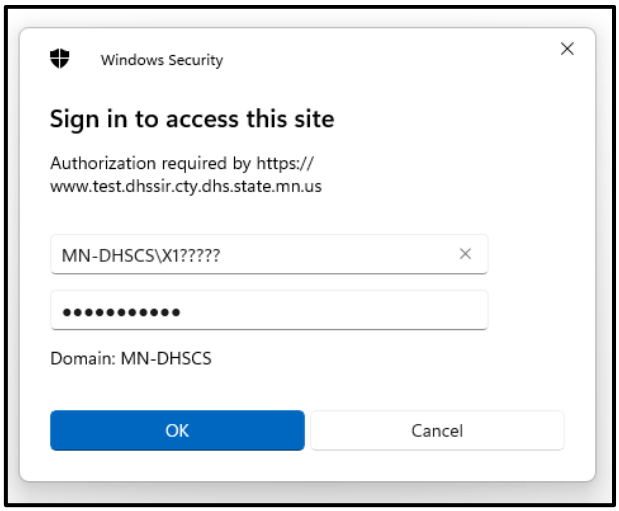
For improved security, SIR users must manually type the domain name in front of their User ID (as of October, 2024.)

To Logon, type in: MN-DHSCS\Your User ID:

1. Navigate to the DHS-SIR website in your browser - https://www.dhssir.cty.dhs.state.mn.us
2. **Type in domain: MN-DHSCS**
3. **Insert a backslash (\ )** after domain and before User ID
4. User ID = continue to **use your same User ID** (PW, X1)
5. Hit OK (or Submit if that's what shows in your county)

Examples with PW and X1 numbers below:





Remember To Use the New Logon Process

Please follow the logon instruction to avoid getting locked out/suspended in SIR. Without the correct process, a user will get three tries and then be locked for 45 minutes. They will then get another three tries to logon correctly. If not successful logging in correctly after the second three tries, the user account will be suspended, and a Security Liaison will need to request an unsuspension.

How To Unsuspend Your Account

1. To unsuspend a SIR user account or to reset a SIR password, contact the assigned Security Liaison (designated by the county or tribal nation) for assistance.
2. **Security Liaisons:** Follow the same process routinely used to reset passwords and unlock and unsuspend accounts in SIR. If needed, follow the SSAM Escalation Process to move the request to the highest priority.

Password Reset for SIR

Password Reset Required Every 90 Days

Users are now required to reset their SIR password every 90 days. In 2025, a new piece of software will remind users of their deadline to change their password and send countdown reminders along with a link to the Password Change page. Meanwhile, users will receive an email notice and reminder to reset their password with a link to the Password Change page.

If a user does not reset their password within the designated 90 days, their account will be suspended by SSAM. Users have another 30 days to reset their password—if they do not, their account will be deleted.

Watch for alerts about this new password reset requirement and any software update announcements.

Please remember to alert your Security Liaison to put in a Leave of Absence request for any extended absence.

Password Change Page
Users can change their SIR password when needed by clicking on the Password Change link under Important On the right side of the SIR home page under Important Links click on Password Change.

At the SIR Password Change page:

- Enter your temporary/current password in the Old Password field.
- Enter a new password in the New Password field.
- Retype the new password in the Retype New Password field
- Click the Change Password button

Go out of SIR and then back in to make sure the new password works for both the SIR website and your SIR web mail. ***For security, please do check the Remember my Password box***.

Unsuspend/Reset a Password with the MMIS FI06 Reset Tool

The FI06 security group in MMIS is available to County and Tribal Security Liaisons who have a MMIS account. This tool can be used to unsuspend accounts or reset passwords for mainframe/ACF^2 systems such as InfoPac/eReports, MAXIS, MEC^2, MMIS and PRISM. These systems all use the same password.

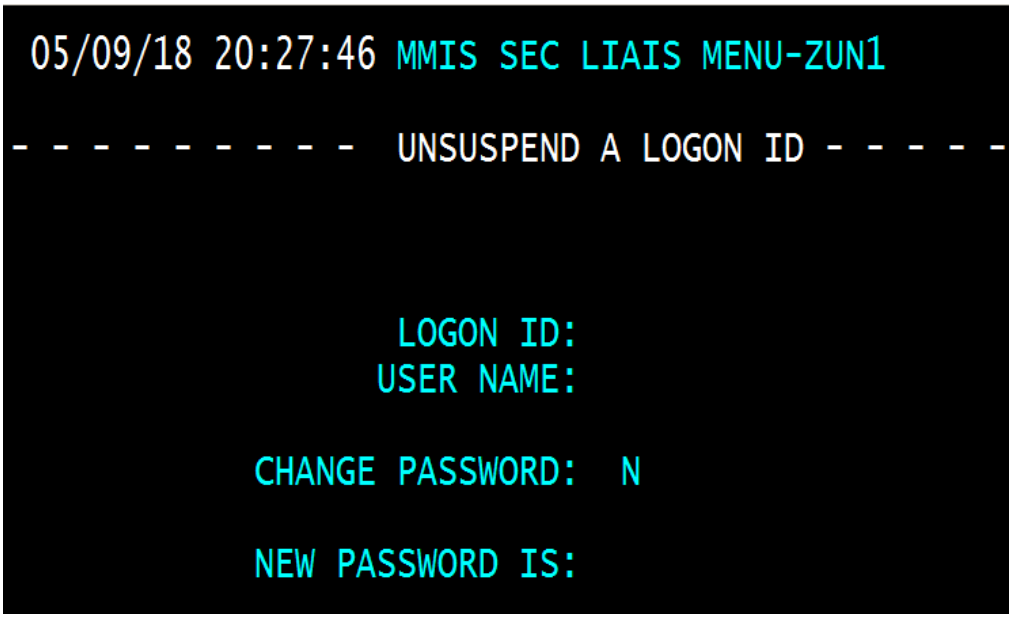
A job runs to process (or synchronize) the unsuspend/password resets that you enter. Once your action has been confirmed you will need to wait for a sync before the unsuspend/password reset goes into effect. This unsuspend job runs:

- 7 days a week
- Between 6:00 am and 6:00 pm
- On the hour and every 15 minutes thereafter (6:00 am, 6:15 am, 6:30 am, 6:45 am, 7:00 am, 7:15 am, 7:30 am…6:00pm)

For example, if you use this tool to submit an unsuspend/password reset at 8:55 am, it will be processed during the 9:00 am job.

Quick instructions
When you sign in to MMIS Production, Enter **MWZB** (instead of MW00).

You will see this panel.



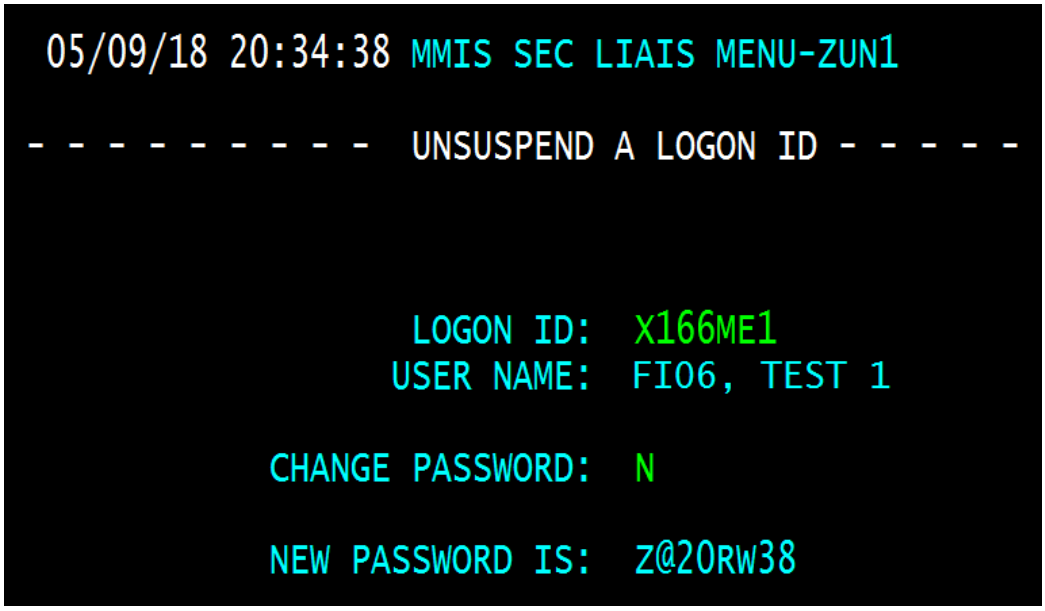
We will use the test IDs X166ME1 and X166ME2 in our examples.

Unsuspend with No Password Change
For an unsuspend with no password change follow these steps:

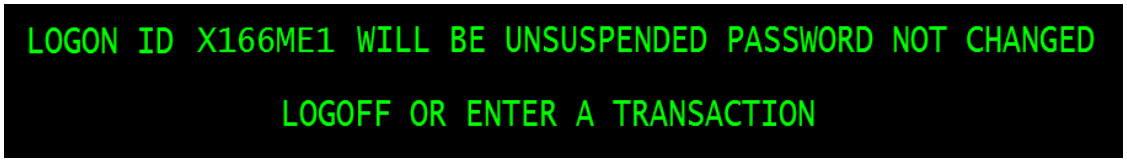
1. Type in the **LOGON ID**
2. Press the **ENTER** key

The USER NAME field will populate as will the NEW PASSWORD IS field.

3. Leave the '**N'** in the **CHANGE PASSWORD** field
4. Ignore the new password in the **NEW PASSWORD IS** field

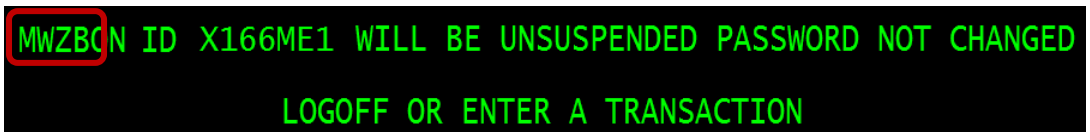


5. Press the **F3** key and you will see this message

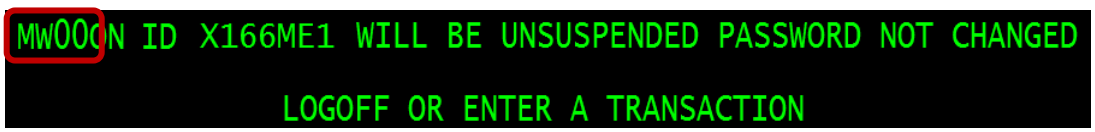


6. Once your action is confirmed, please let the user know about the delay or wait for the next unsuspend job to run before you notify the user that that they have been unsuspended.

Type **MWZB** and press the **ENTER** key if you have more accounts to unsuspend or reset.



Type **MW00** and press the **ENTER** key if you would like to go to MMIS production.



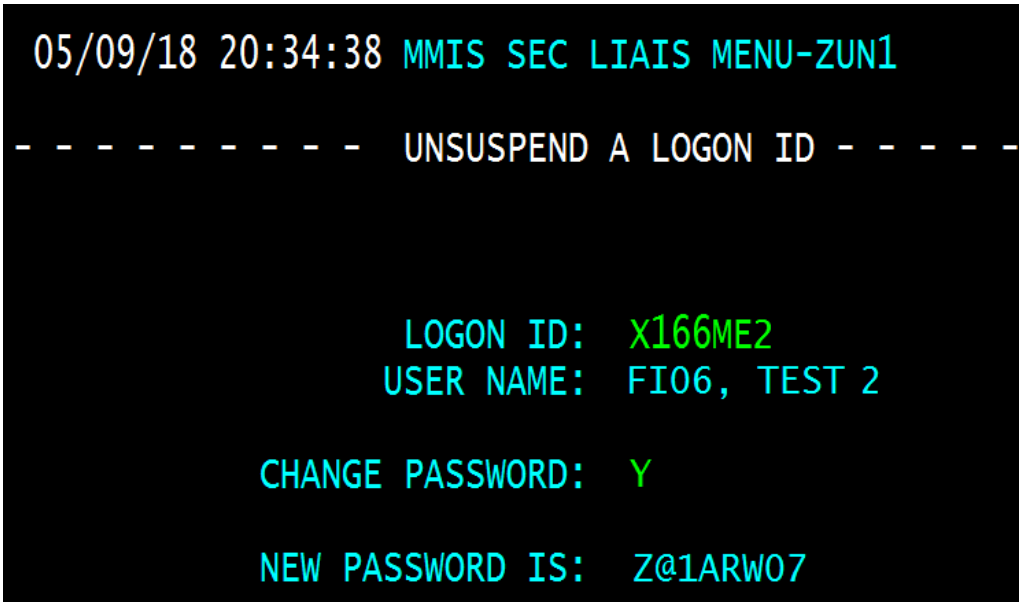
To exit, type **LOGOFF** and press enter.

Password Reset
For a password reset follow these steps:

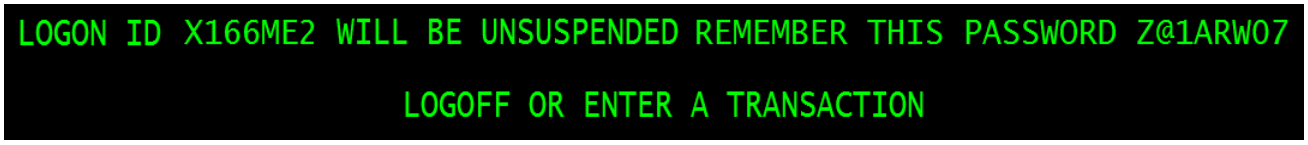
1. Type in the **LOGON ID**
2. Press the **ENTER** key

The USER NAME field will populate as will the NEW PASSWORD IS field.

3. Type '**Y**' in the **CHANGE PASSWORD** field
4. Press the **ENTER** key



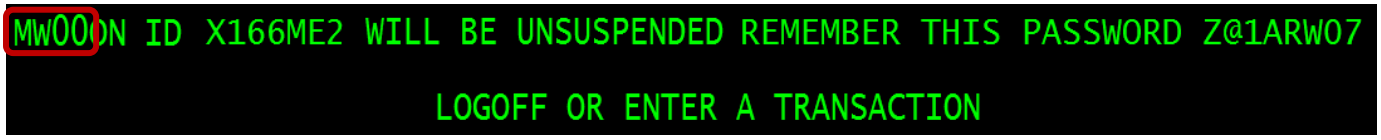
5. Press the **F3** key and you will see this message



7. Transaction complete, make note of the password.
8. Once your action is confirmed, please let the user know about the delay or wait for the next unsuspend job to run before you notify the user of their new password.

Type **MWZB** and press the **ENTER** key if you have more accounts to unsuspend or

Type **MW00** and press the **ENTER** key if you would like to go to MMIS production.



To exit, type **LOGOFF** and press enter.

Error Messages
There are a few error messages that you may encounter while using the MMIS FI06 reset tool.

If you type in your own logon ID, you will receive this message.

You will also receive an error message if you try to unsuspend a user from a county/tribe other than the county/tribe you are a liaison in.

If you see the message shown below, the logon ID is not on the file. The unsuspend/password reset will need to be submitted via the Unsuspend/Password Reset Request in the Minnesota Service HUB.

MNEIAM Password Standards, Resets and Unsuspends

MNEIAM Admin Portal
Portal to manage applications based in MNEIAM. Click here to reset user passwords for SMI, ISDS-SMRT, and BOBI Reports.

MNEIAM Administrators Guide
Instructions for Security Liaisons on resetting passwords for systems that run off of MNEIAM. Can be used to reset user passwords for SMI, ISDS-SMRT, and BOBI Reports.

EBT/eFunds Password Standards

EBT/eFunds rules for a strong password are:

- Minimum 8 characters; maximum 14 characters
- Must contain both upper and lower case letters
- Must have at least one number character/symbol
- May have a maximum of 3 repeating characters (same characters next to each other)
- The previous 10 passwords cannot be used
- The user will be locked out if they enter the password incorrectly 3 times in a row

Your EBT Password will expire every 45 days.

The system will issue password expiration warnings 5 days prior to expiration reminding the user to select a new password.

If your EBT User ID has not been used for 90 days, the system deactivates the User ID.

MAXIS Access

MAXIS Inquiry Access

As a Security Liaison, it is important to know the differences in the INQUIRY roles so you can request the correct access for each position. The INQR role includes notes data and IEVS (IRS) data. When a user has access to IEVS data, they MUST sign a non-disclosure oath. **This oath is now located on-line (no printing and signing is required)**, and **users will be denied access if they do not electronically sign it**.

MAXIS Inquiry Users Messages
There are two messages received from the MAXIS initialization modules

1. **PLEASE LOGON TO TRNG ONCE TODAY TO RECORD YOUR MAXIS USAGE**
   If 45 days have passed since an inquiry user has logged on to the Training Region, the MAXIS system gives them this message: **PLEASE LOGON TO TRNG ONCE TODAY TO RECORD YOUR MAXIS USAGE**. The MAXIS system records a last logged on date so we can track who is no longer active.

2. **PLEASE USE TRAINING REGION FOR THIS PANEL. PF3 TO END**
   MAXIS gives a reminder for the certification/oath panel. The certification/oath needs to be completed annually for HIPAA. It is presented in inquiry, but does not allow the user to fill it out in inquiry, they need to log into the training environment. MAXIS system gives this message: **PLEASE USE TRAINING REGION FOR THIS PANEL. PF3 TO END**

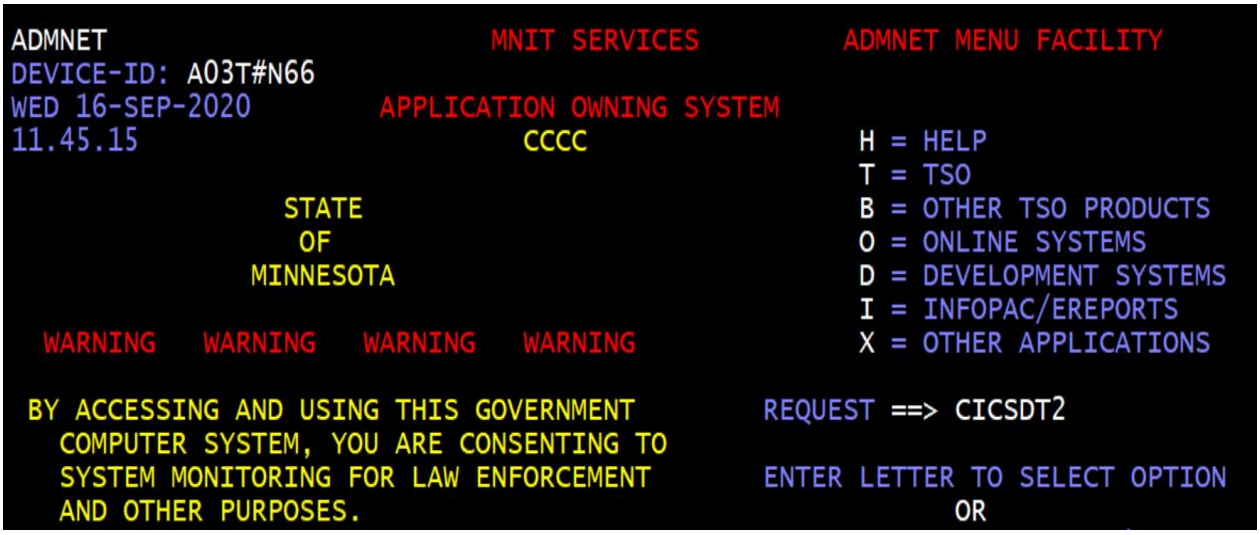
All Inquiry users need to do the following the first time they log in to use the system:

- Log into the Training Region (CICSDT2) on the State of MN screen
- Enter LOGON ID and PASSWORD and change the password if it is a temporary password
- Type FMTP and press ENTER

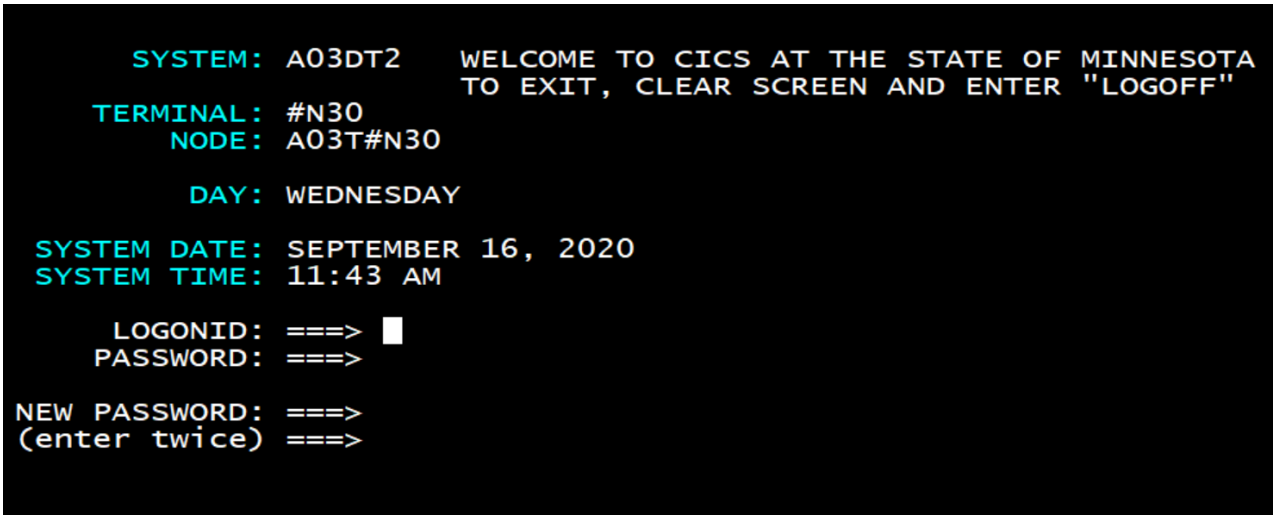
And then complete the above at least once during the day when they use their MAXIS access.

Instructions for electronic signature of the nondisclosure oath for INQUIRY USERS:

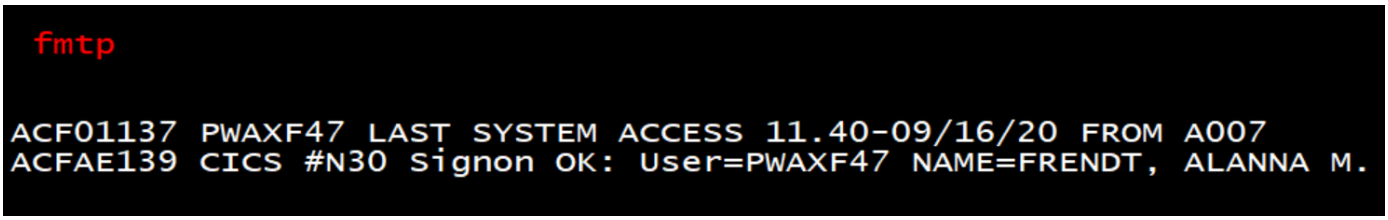
1. Log out of everything, including MDHS.
2. From the STATE OF MINNESOTA screen, log into CICSDT2 by typing CICSDT2 and pressing ENTER



3. Enter LOGONID and PASSWORD, press ENTER



4. Type FMTP and press ENTER



5. Flag the Oath with a “Y” and press ENTER
6. Log out
7. From the STATE OF MINNESOTA screen, log into the Inquiry Region by typing FM and pressing ENTER
8. Enter LOGONID and PASSWORD, press ENTER
9. Type FMPI and press ENTER

The user should see the SELF panel at this time. They can continue to use FMPI, or they can logout and log back in using MDHS.

MAXIS Update Access

MAXIS is required for any user who will have any type of update authorization including Financial Worker, IPAM, Accounting and Fraud roles.

- Update access can be requested for up to 90 days prior to training.
- If the new user does not receive training within 90 days, the logon will be automatically denied Update access after 90 days has passed.
- Always identify the type of training and the date (requested or confirmed) that the user is scheduled for.

The new user must attend formal DHS training within 90 days of application. Contact Train Link/Pathlore for training enrollment information. If a user attends training for IPAM, ACCT, ACC2, CCOL or Financial Worker and does not already have the role in production, submit a System Access Request in the Minnesota Service HUB to have the new role added.

Examples of a Conflict of Interest:

The user cannot have the ACCT or ACC2 role and the Financial Worker (FINE) role.

- Having the user approve eligibility and issue a check is not a good security practice.
- Enforce the separation of duties in the roles assigned to each user.
- Confirm that each user has the least access possible to do their assigned job.
- Roles should be assigned to users on a “need to know” basis.

Re-adding a MAXIS User

When a former employee is re-hired by the county, SSAM will add the person back to the MAXIS system after receiving the System Access Request.

If the person has been off the system for more than 1 year and an Update role is requested, the person must attend formal DHS training within 90 days.

When an Inquiry role is requested, the Mentor must re-train the user if a user has been off the system for more than 1 year.

When your county hires a worker from another county, and that worker has had Update access into MAXIS and has used it within 1 year, you must submit a System Access Request, indicating the previous county logon.

Inter-County Transfer (ICT) Logon IDs (MAXIS and SIR)

Each county has a unique ICT logon ID.

These logons begin with X1, followed by the county number and the letters ICT.

These logon IDs are used to transfer cases between counties.

Someone in the county is responsible for checking email messages in the SIR system for this logon ID.

- The ICT is controlled by the county.
- The county determines who can use this ID.
- The user logs on with the ICT logon ID and MAXIS password in MAXIS to do what is needed in the MAXIS system.
- To read and/or send web mail for the ICT account you would need to log into SIR using the ICT logon ID and SIR password.
- Distribution Lists are not created for ICT logon IDs

POOL/HOLD IDs (Case Banking)

POOL or HOLD IDs have also become known as Case Banking IDs.

To request a new Bank/Hold/Pool login ID, submit the SSAM General Inquiry form in the Minnesota Service HUB.

HOLD IDs: This group is used to define the "holding file logons". Some counties have chosen to setup logons that are used to simply hold closed cases or other unique types of cases.

HOLD IDs pertain to things/items, it is an identifier:
EXAMPLES: Inactive Cases, CAF1 Cases (not assigned a worker), Closed Cases, Deceased, Pending, etc.

These IDs do not receive mail.

POOL IDs: This group contains the "pooled caseload logons". The pooled logon holds active cases and distribution lists can be used in sir web mail with that pool ID.

EXAMPLE OF USE: The workers will work on a case and then transfer it back to the pooled ID in order for another worker to have the case.

Pooled IDs pertain to people/teams that have access to the ID and hold an active caseload for a team.

If you have questions on how Case Banking teams are being used, please contact Tracy.K.Scott@state.mn.us

See below regarding distribution lists for Team/POOL IDs.

Team/POOL IDs, SIR Webmail Access and Distribution Lists

- Distribution lists need to be setup for Team/POOL IDs (Initial set up is done by SSAM staff, maintenance of the distribution list is done by the Security Liaison or assigned staff in the county, see below for instructions on maintaining distribution lists)
- If the assigned staff is not a Security Liaison, please inform us of who the person is that we can accept changes from.
- Team/POOL IDs do not have access or passwords to the SIR system
- The users that make up the team/pool ID logs onto SIR Webmail as themselves using their own logon ID
- Any email that is sent to the team/pool ID distribution list (Ex: X1team@cty.dhs.state.mn.us) in SIR Webmail will be sent to each of the team members.
- For distribution list we need the following information:
    - Name of the distribution list you wish the user(s) to be added to (generally is the same name of the team)
    - Name of the user(s)
    - Logon ID of the user(s)

Technical College Student User (MAXIS) { TC “TECHNICAL COLLEGE STUDENT USER” \f C \l “1” }

MAXIS access for a Technical College Student Intern is coordinated between the Technical School Instructor, the County, and the DHS Technical College Coordinator.

The DHS Technical College Coordinator is Tracy Scott (651.431.4020, Tracy.K.Scott@state.mn.us

The DHS Technical College Coordinator sends the Student Intern form to SSAM.

SSAM assigns a County logon ID with the FINU security role.

SSAM sends the new logon ID, e-mail code and password to the appropriate County Supervisor, Security Liaison, and the DHS Technical College Coordinator.

The MAXIS Security Liaison should e-mail SSAM when the intern’s supervisor believes the intern is ready to have eligibility approval security.

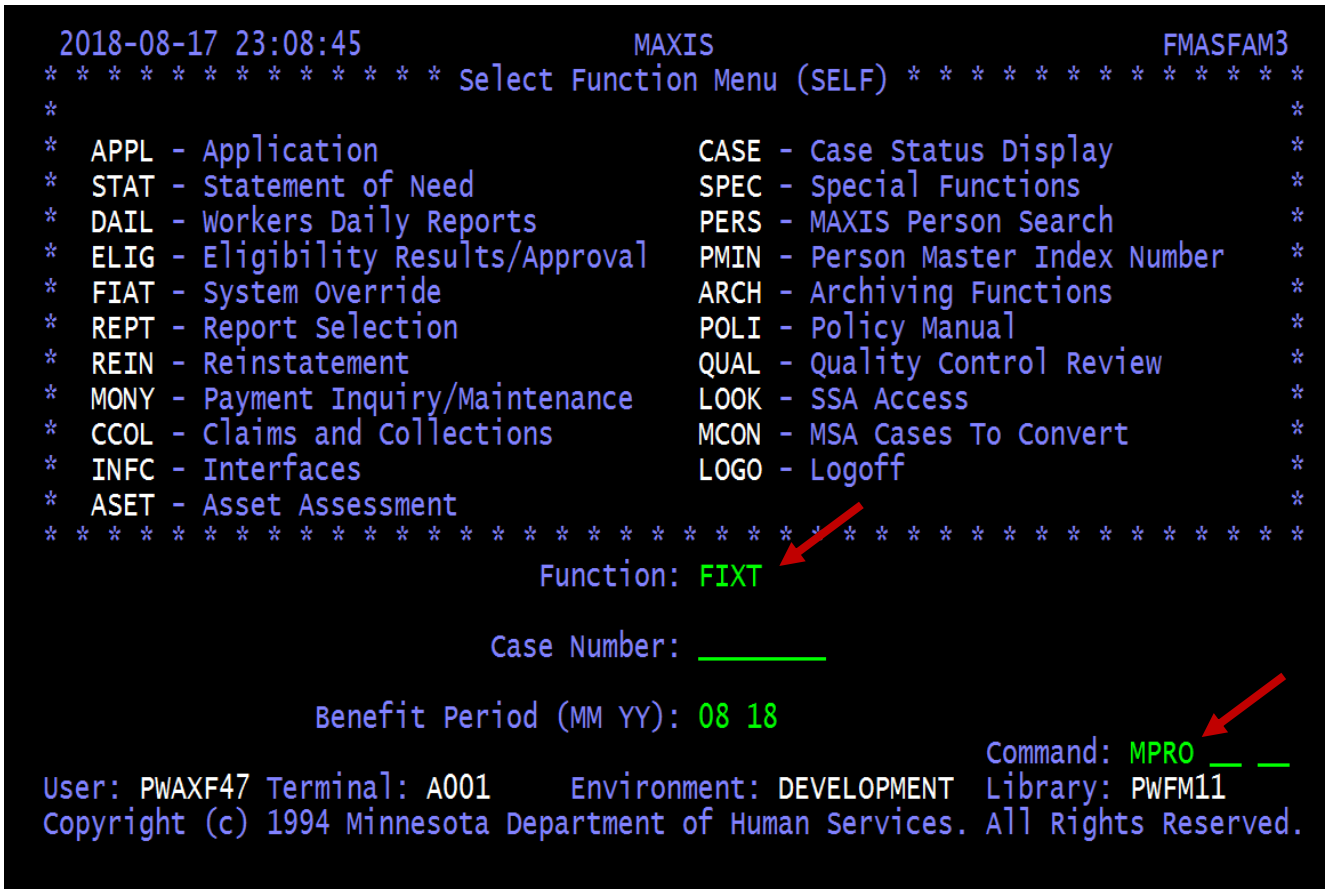
FIXT/MPRO Function

You will have users who must have modifications made on their security profile. You can make many of these changes using **FIXT/MPRO.** The function is used for both MAXIS and MEC² information.

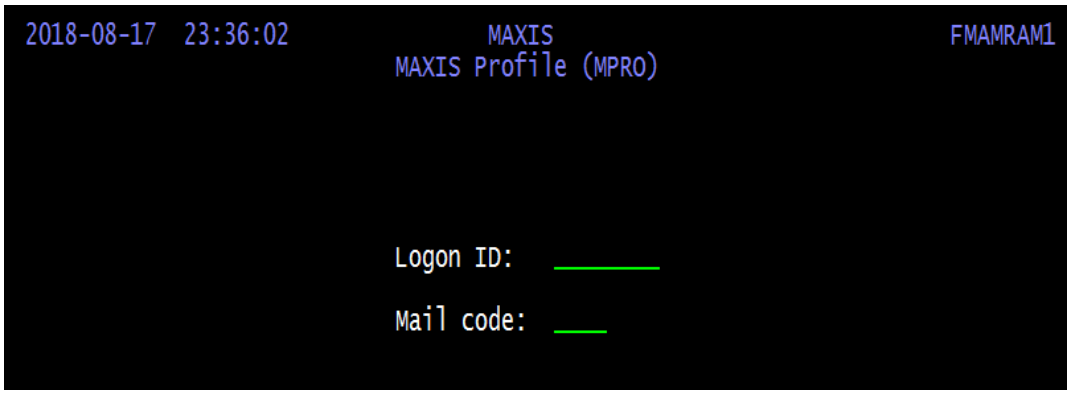
Log into MAXIS Production

From the Select Function (SELF) Menu

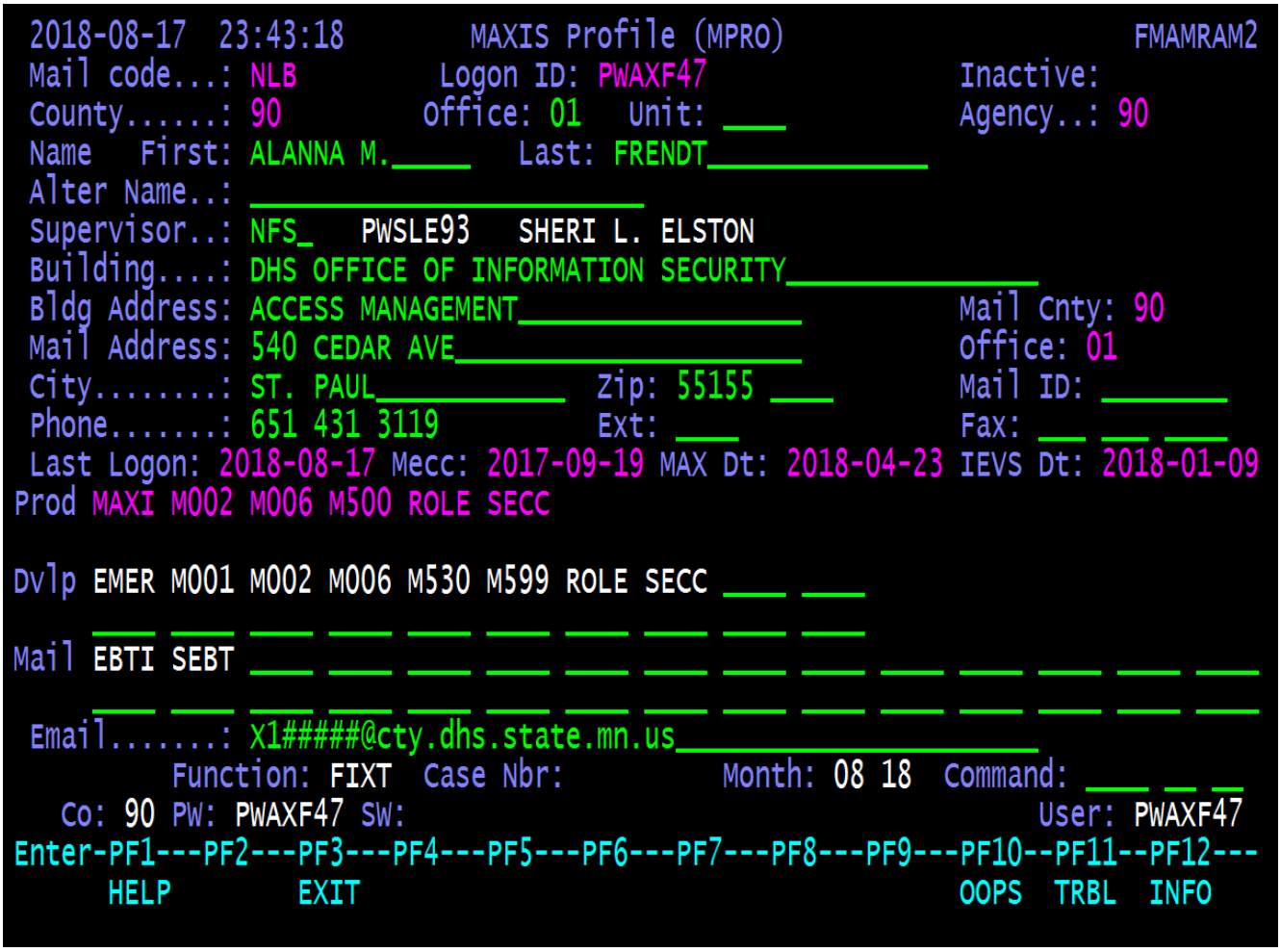
- Type **FIXT** on the Function line
- Type **MPRO** on the Command line
- Press the Enter key (Transmit)



- Enter the user's logon ID or mail code and transmit



The MAXIS Profile (MPRO) screen display



The fields in green above are the fields that can be modified. Here is a list of the fields:

- Unit
- First Name
- Last Name
- Alternate Name (when filled in this is the name that appears on notices)
- Supervisor (must locate the mail code ID for the supervisor, can be looked up on REPT/USER screen)
- Address Information
- Phone
- Fax
- Email Address (this is the SIR email address X1#####@cty.dhs.state.mn.us)

If you make changes to the person's name, please notify the SSAM team by submitting the **System User Maintenance** form in the Minnesota Service HUB so that all security databases and systems can be updated. The form has a Request Change to User Information option with a checkbox for Name Change.

Fields that you will not be able to modify through the FIXT/MPRO function:

- Mail Code
- Logon ID
- Inactive field
- Servicing Agency
- User's production roles and e-mail groups
- Last Logon Date (the last date the user logged onto the MAXIS system)
- MAXIS Date (last date of signing the MAXIS Oath)
- MEC² Date (the last date user signed onto the MEC² system)
- IEVS Date (last date of signing the IEVS Oath)
- Fields used for EBT printing, issuing cards and return of cards are the County field (next to the Region field) and Office. Security Liaisons do not have the authority to update these fields; only SSAM can make the changes.
- Fields used for MAXIS mailing checks, notices and return address.

The Mail County and Office (under MAIL County) are used for printing/issuing of checks, etc.

In the event of a mass change (your office moves and everyone in the county now has a new address), do not make these changes one user at a time. Notify SSAM and a mass change can be done.

Make sure your Inquiry user's log on at least once every 30 days to keep their user ID's active. Please see section on Inquiry User's and Inquiry Messages for more information.

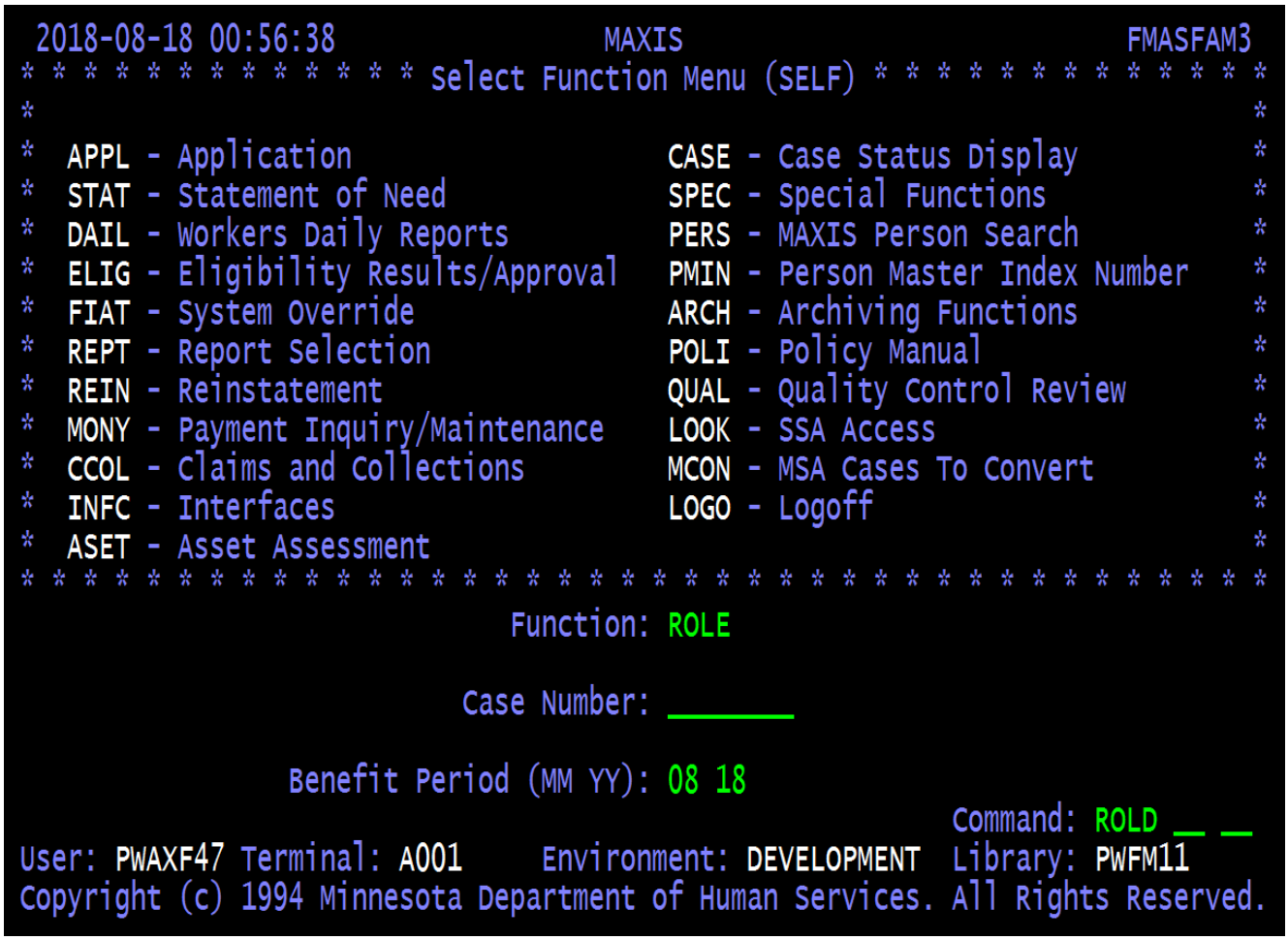
ROLE/ROLD Function for MAXIS and MEC²

To see what type of access a role has follow these steps:

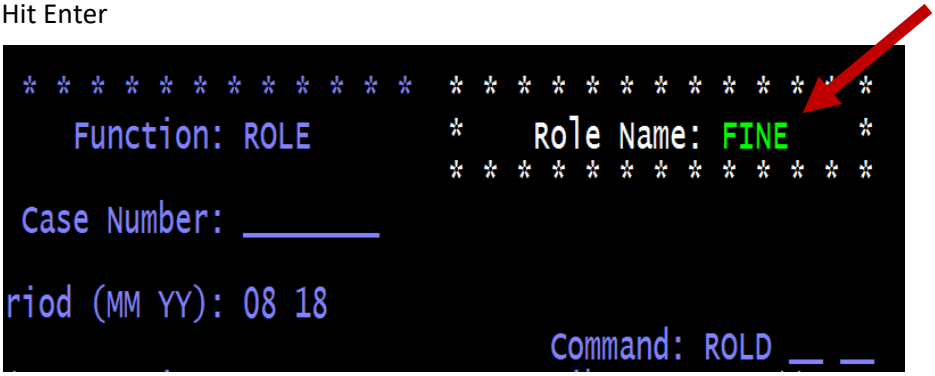
Log into MAXIS Production

From the Select Function (SELF) Menu

- Type **ROLE** on the Function line
- Type **ROLD** on the Command line
- Hit Enter

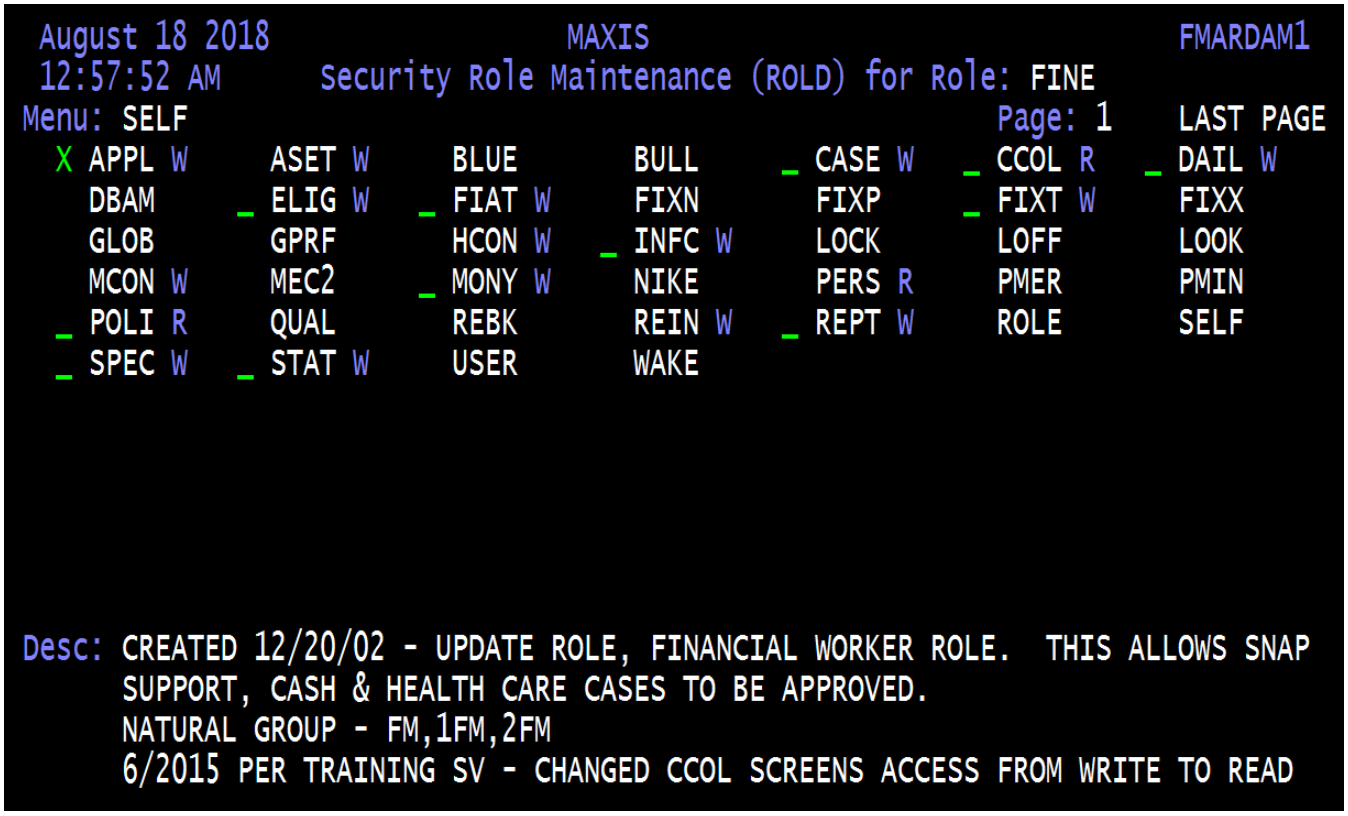


- Type the Role Name you wish to view
- Hit Enter

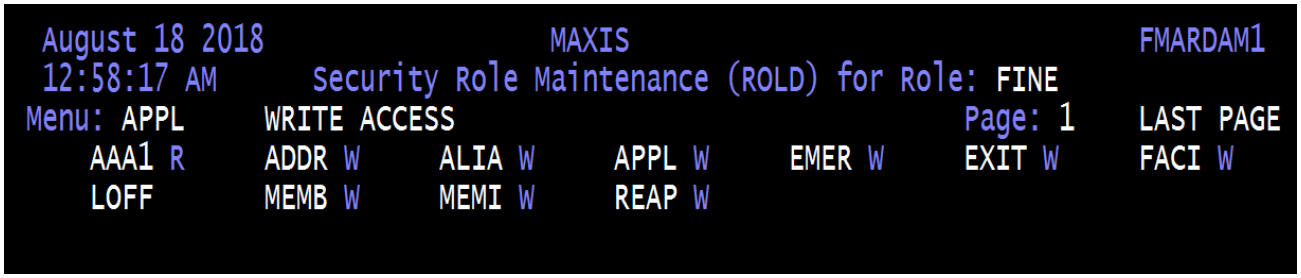


The next screen will show you what functions this role can (R) read or (W) write to

- Place an ‘x’ on the line in front of the screen name
- Hit Enter



The screen will display what functions can be accessed below the item you selected.



There may be another screen showing the next set of screens that can be accessed. Additional screens have a line where you can place an ‘x’ to view more information on the role.
The ROLE/ROLD panel works for both MAXIS and MEC² systems.

Blocked and/or Privileged Cases

Access Requirements
Occasionally a county needs to have a case blocked. MAXIS/MEC² has several "privileged" codes that can be applied to a case, and will prevent unauthorized access. ***For assistance with a case block please send a request to the TSS (MAXIS) Help Desk and they will forward the request to the staff person authorized to set these codes.***

Submit a TSS Help Desk Request form found on SIR under either MAXIS or MEC² pages.

The following codes pertain to both MAXIS & MEC²

CODE 1: can only be accessed by the user's primary county, equal to that of the case.

CODE 2: can be accessed only by the case worker, or case worker's supervisor, a secondary worker and that person's supervisor, and authorized state personnel.

CODE 3: Can only be viewed by authorized state personnel.

CODE 4: Foster Care Case. Can be accessed only by the Case Worker; a secondary worker; the supervisors of either worker; a person who has a mentor role and a primary county equal to that of the case or the MAXIS/MEC² Help Desk.

A special role can also be requested for MAXIS and MEC² staff needing to see foster care cases in their county.

- FOST is the role needed in the MAXIS system
- M598 is the role needed in the MEC² system.

Interfaces with MAXIS and MEC² Systems

Interface means the sharing/sending of information from the MAXIS or MEC² systems to have that information updated on the receiving system.

An interface with another system can alleviate the need to have access to both systems, for information from these systems are being sent over and are updated on the receiving system.

MAXIS and/or MEC² systems interface with the following systems:

PRISM (Child Support System)
Work Force One (WF1- DEED)
MMIS
SSIS (4E Foster Care)
SMI
Licensing
Data Warehouse
Disqualified Recipient Subsystem (DRS)
TOP – Treasury Offset Project
MCE – Minnesota Collection Enterprise – Department of Revenue
Department of Finance (via CITA)
Department of Treasury
U.S. Bank
EBT – Electronic Benefits Transfer – eFunds
PARIS
SSA (Social Security Administration)

County Instructions on Maintaining Distribution List(s)

These instructions include steps for county staff who have security to change enrollment of staff to distribution lists. It is important to log into the Minnesota Service HUB and submit the SSAM General Inquiry form to modify a SIR Web Mail distribution list. This will send a request to SSAM staff informing them of the changes. SSAM will update SIR Active Directory with your changes and the new user(s) will begin receiving SIR Web Mail for the team.

SSAM staff will need to establish the initial SIR Distribution List(s). Once that has been created the designated person(s) in the county will then take over and follow the below instructions.

Notify SSAM staff of who will be maintaining the distribution list or if there are any changes in staffing. This ensures that the correct access is set up for these individuals in SIR Active Directory.

- Log onto SIR and click on the Web Mail Distribution Lists link in the Important Links box.
    - Select the Distribution List you wish to edit (E.g. Click on MAXIS)
- Scroll down to locate the distribution list
- Double click on the list
- To ADD a new user, click on the NEW dropdown for a New Item
    - On the User name field, enter the worker's X1#
    - On the Full name field, enter first than last name
    - On the County name field, enter county
    - Click OK
- To CHANGE a user, click on the User name (X1#) link
    - Click on the EDIT Item link on tool bar
    - Make your changes
    - Click OK
- To DELETE a user, click on the User name (X1#) link
    - Click on the DELETE Item link on tool bar
    - User will be removed
    - Click OK
- Once you have completed your changes, log into the Minnesota Service HUB and submit the SSAM General Inquiry form to modify a SIR Web Mail distribution list.

This will send a request to SSAM staff informing them of the changes. SSAM will update SIR Active Directory with your changes and the new user(s) will begin receiving SIR Web Mail for the team.

DHS-SIR Webmail System

The SIR Webmail system is a common, secure, single communication platform for users of DHS major systems: MAXIS, PRISM, MMIS, SMI, and MEC². Each county worker will have a secure Outlook email address in SIR mail that can be used to send or receive secure mail. County workers will no longer have to depend on DHS to maintain distribution groups. SIR Outlook mail provides an easy way to maintain distribution lists to communicate with groups of people. See section on POOL/HOLD/Case Banking.

Your SIR mail address is your X1 number followed by @cty.dhs.state.mn.us.

This address will be displayed on the REPT/USER panel in MAXIS and the MEC² User window and the Associated Case Worker Information window in MEC².

To gain access submit the System Access Request form.

It is important to access SIR and your SIR Webmail daily since communications from DHS and other county workers are sent to this secure email address.

- For instructions on how to change your SIR password see How to Change Your SIR Password
- If users do not have access to SIR pages needed, please submit the SSAM General Inquiry request to request access.

SIR Web Mail Distribution List - How to View List of Users

If you need a Distribution List set up, see POOL/HOLD IDs (Case Banking) Section.

To View SIR Distributions List:

Go to the main page of SIR;

- On the right-hand side of the page, there is a link titled: Web Mail Distribution Lists click on that link.
- Under the title of Distribution Lists, you will see MAXIS or MEC² or PRISM; click on the area you want to view.

In this example we will select the MAXIS area:

- Click on MAXIS
- You will now see a list of the Distribution Lists used by MAXIS staff

Example: SUPR distribution list

Double click on the SUPR name/list and it will show you the staff that is in the list.

SIR Webmail Access, Passwords and Team ID's

How does a team/pool ID use SIR Webmail?

- Distribution List needs to be setup for Team/POOL/Case Banking IDs
- Team/POOL/Case Banking IDs do not have access or passwords to the SIR system
- The users/workers of the team/pool ID logs onto SIR Webmail as themselves using their own logon ID
- Any email that is sent to the team/pool/case banking ID distribution list (Ex: X1team@cty.dhs.state.mn.us) in SIR Webmail will be sent to each of the team members.
- For distribution list, the following information is needed:
    - Name of the distribution list you wish the user(s) to be added to
    - Name of the user(s)
    - Logon ID of the user(s)

How to use the Address Book in SIR Webmail

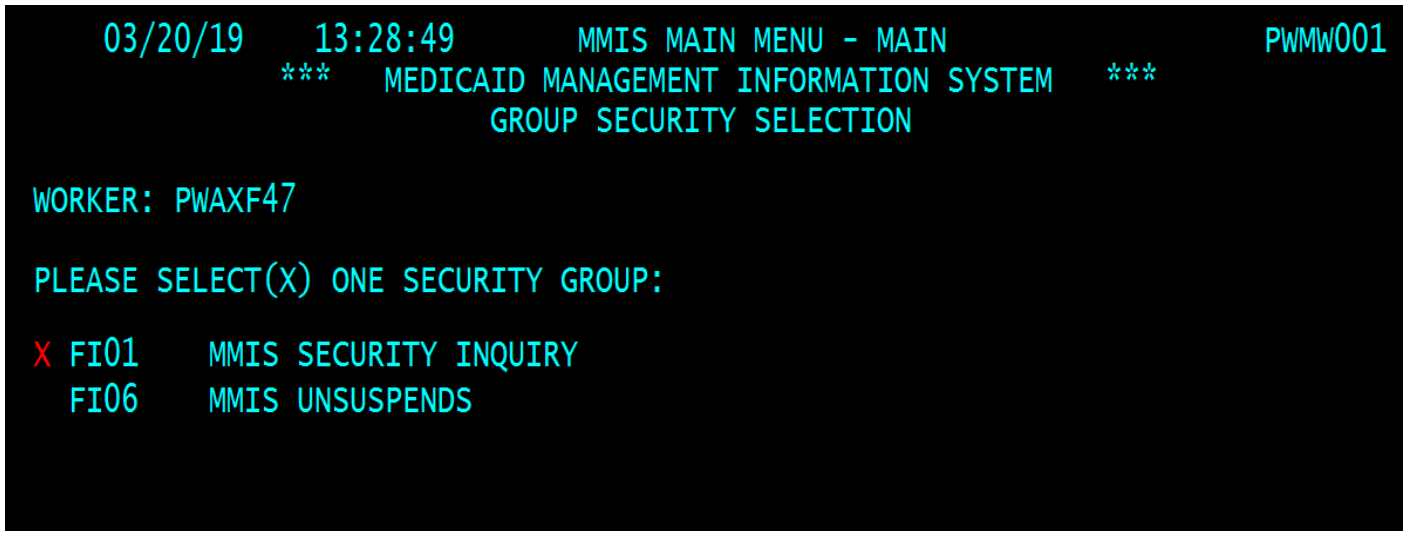
- To locate the Address Book in SIR Web Mail, locate the icon of an open book in the tool bar.
- Click on the book and it will open up the search panel.
- If you know the logon ID, you can type the ID in the ALIAS field and click on the FIND button in the lower right-hand side of the window under the CITY field.

  OR
- Type in the user's last name in the DISPLAY NAME **or** LAST NAME field and click on the FIND button to locate them.
- Once you have found them; highlight the name, by clicking once on it, and then click on the button NEW MESSAGE. This will open up a blank email for you to use.
- If you double-click the user name, it will display the properties of that user.
- Once you are in an email, you can hover your mouse over the user name and this will let you view the actual email address for that user.
- If you wish to add another user to this email; click on the TO button and the address book search panel will open and again type in the user name or logon ID in the appropriate fields. See above for details.
- Type in your message that wish to send and once completed, click on the SEND button located in the upper left-hand side of the email.

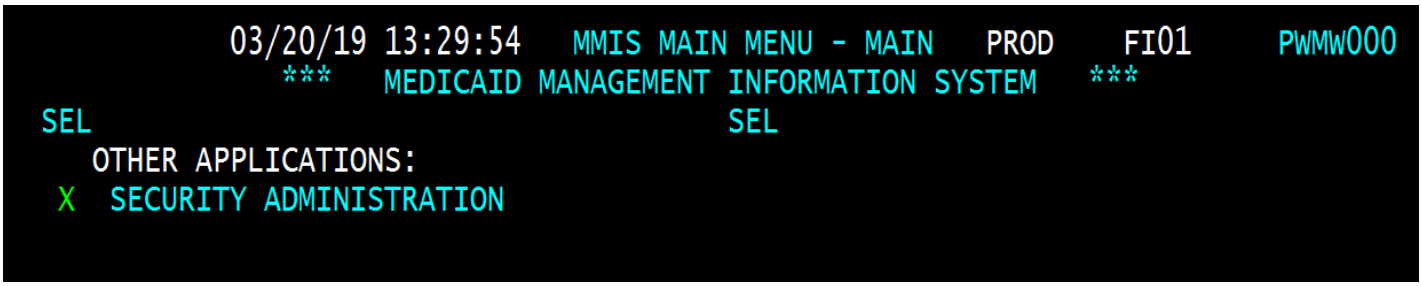
Using FI01 (MMIS SECURITY INQUIRY) to look up user accounts in MMIS to view security groups

As a Security Liaison with Security Liaison – Full access you should have the FI01 security group in MMIS. This group allows you to look up user accounts to see what security groups they have. Follow these instructions to view security groups in MMIS.

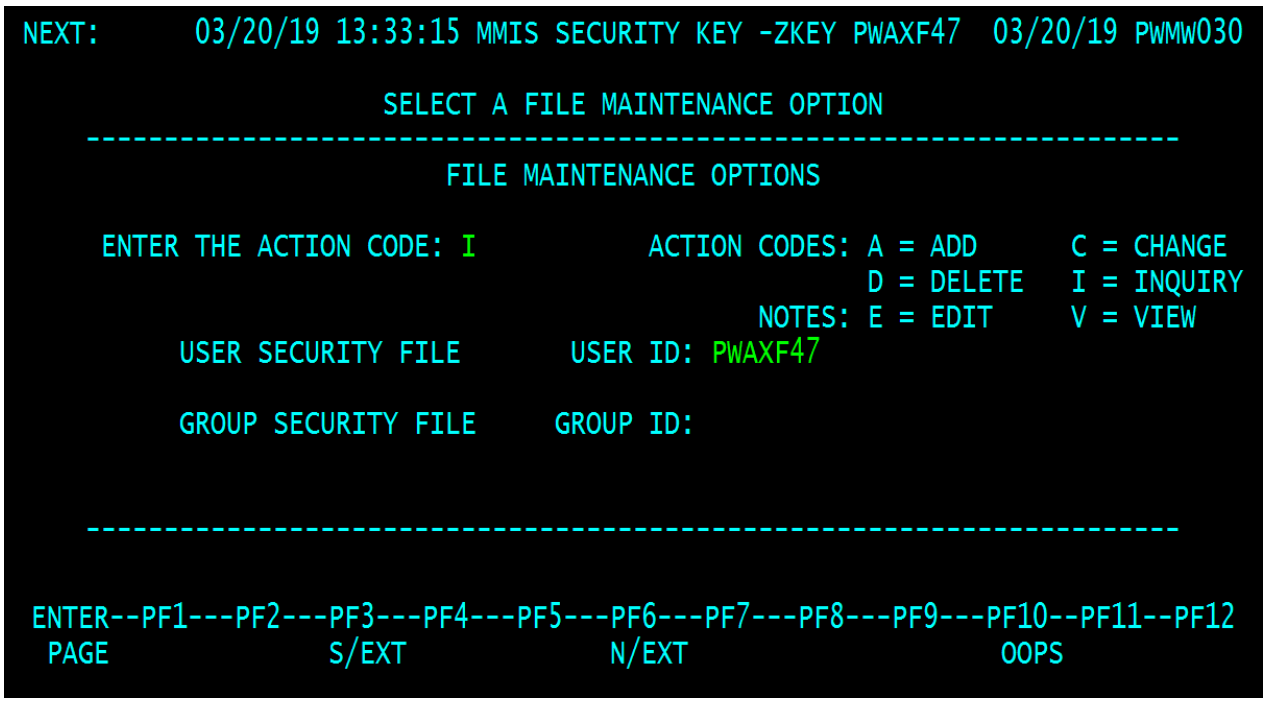
- Log into MMIS Production through MDHS
- If you do not have MDHS then log into the MMIS Production Region by:
  - entering MNCICS1 at the State of Minnesota screen
  - logon using your logon ID and password
  - then enter MW00 on the next screen
- Read the MMIS Security Banner and Press the ENTER key to continue
- Place an "X" next to FI01 MMIS SECURITY INQUIRY and press the ENTER key



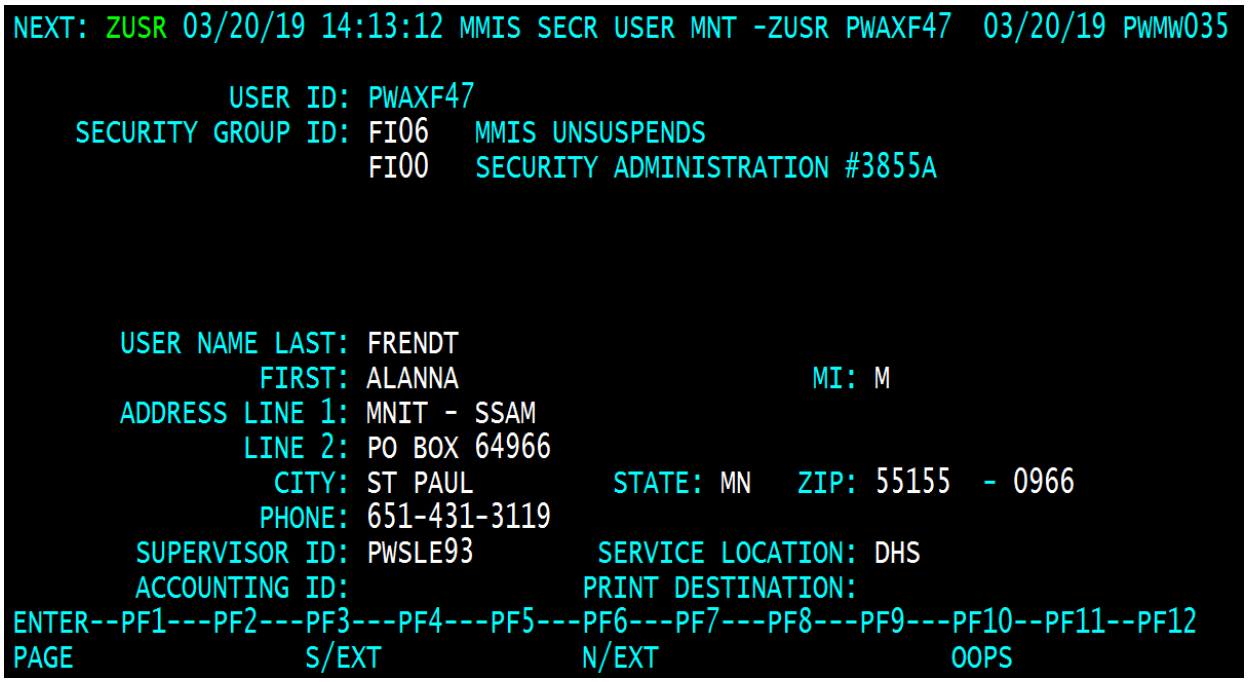
- Place and "X" next to SECURITY ADMINISTRATION and press the Enter key



- Enter ‘I” for Inquiry as the action code and enter the User ID that you would like to look up then press the ENTER key



- The user account will come up and you will be able to view the user’s security groups



- Press PF3 to Exit

MnCHOICES Overview of Access Management

MnCHOICES Delegated User Management Administration Model

The MnCHOICES application uses a delegated user management administration model. This means that at the Lead Agency, there are users that can manage other users' access on behalf of their agency. This is unique to MnCHOICES and is described in this section of the Security Liaison Handbook.

A user's access to Agency specific data is based on the Organization and Location they are assigned. In MnSP, this was referred to as the Agency Combination, which was comprised of the Lead Agency (Organization) and Delegate Agency (Location). What makes MnCHOICES different, is that users may have one or more roles within an Organization/Location assignment. There are two roles that a user may have that allow management of staff records.

These roles are managed exclusively by the Lead Agency Security Admin or the Lead Agency Supervisor.

Lead Agency Supervisor: Among their access privileges, they are granted the authority to modify attributes of existing staff records (phone, name, etc.). They can manage existing staff records location assignment and roles, as well as modify or remove existing Location assignment and roles. They cannot create staff new staff records or modify their own access.

Lead Agency Security Admin: This user may create and modify staff records, and setup the Location assignment and roles the user will need. This user is responsible for adding new Staff records to their organization prior to submitting the System Access Request to activate the account. They cannot modify their own access.

> ***NOTE: SSAM will only assign the Lead Agency Security Admin role if your organization does not have one currently.***

Some users may work as delegate workers for other Lead Agencies. For each organization/location assignment, a user will have a corresponding staff record. If they have three Organization/Location assignments, they will have three staff records. Each staff record may be granted its own set of roles depending upon each Lead Agency's needs.

SSAM System Security and Access Management for MnCHOICES

Staff records are linked to MnCHOICES System Accounts. A user may have one or more staff record—however, they will only have one System Account. Setup and management of System Accounts is handled exclusively by the SSAM team. SSAM will activate a new system account for a new user. If the user already has an active staff record with another lead agency, SSAM will link the new staff record to the corresponding System Account.

Other responsibilities that SSAM has includes verifying completion of MNCH8010 and adding credentials for Certified Assessors. SSAM also modifies system accounts when name, phone or email need to be updated.

SSAM can assist with modifications on the staff record, although Lead agencies are expected to manage their users. Please note SSAM cannot modify who the supervisor is on the Staff Record. Lead Agency Supervisors and Lead Agency Security admins must manage this.

Roles and Responsibilities Specific to Granting Access to MnCHOICES

1.Responsibilities of Lead Agency Specific to MnCHOICES

The Lead Agency must follow the process below to ensure requests for access can be completed when a System Access request is submitted. Failure to follow this process will result in delays and the request could even be closed. If the request is closed, SSAM will state specifically what needs to be completed. Once the issue is corrected by the Lead Agency, the Lead Agency Security Admins may request that the Security Liaison submit a new request for access.

***2.*Responsibilities of Lead Agency Security Admins Specific to MnCHOICES access request process**

Lead Agency Security Admins are required to complete the following before the Security Liaison may submit a System Access request. Once this has been completed, they should notify the Security Liaison.

1. Check for an existing staff record and create a new staff record if one does not exist.
2. Add the phone number and check the Primary box.
3. Add the email and check the Primary box.
4. Add the Location assignment.
5. Assign role(s) the user may need.

3.Responsibilities of Security Liaison Specific to MnCHOICES access request process

1. Before filling out the request, ensure that the Lead Agency Security Admin has completed setting up the Staff record.
2. Check user security training compliance in Handling MN Information Securely.
3. Fill out the System Access request form user information details.
4. Select the MnCHOICES from the list of available systems.
5. If the user is a certified assessor and will be fulfilling those duties for the Lead Agency. Ensure the user has completed the MNCH8010 course in Trainlink. Answer 'Yes' to the Certified Assessor question and provide the Trainlink ID in the corresponding box. *Please note that this value may be different from the X1 or PW logon ID.*
6. Include a descriptive business reason in the "how will this system be used?" field on the request.
7. Attest that the user has completed their security training on Handling MN Information Securely
8. Once all the required fields are filled in, Submit the request.

4.Responsibilities of SSAM Specific to MnCHOICES access request process.

1. Verify all the information submitted and validate the System Access request.
2. Ensure the data entered on the staff record is accurate according to what is provided on the System Access request.
3. If the request states that the user is a Certified Assessor, SSAM will verify completion of MNCH8010 on Trainlink and setup the credentials on the Staff Record.
4. Verify that the user has an assigned Location and at least one role assigned. If they are a Certified Assessor, and the system had removed the role due to lack of valid credentials, SSAM will add the Certified Assessor role. *SSAM will not assign other roles, however the Security Liaison will be notified if this step was missed by the Lead Agency Security Admin.*
5. Activate a new System account or link an existing account.
    - If the user does not have a System Account, when SSAM activates the staff record, the system will create a new System Account and send the user the onboarding email. This email expires within 7 days.
    - If the user does have an active System Account, this is due to another active Staff Record with a different Lead Agency, SSAM will Link the new Staff record to the existing System

Account. In this scenario the user will not receive an email from the application, however upon their next login, they will be able to select the new Organization/Location option.

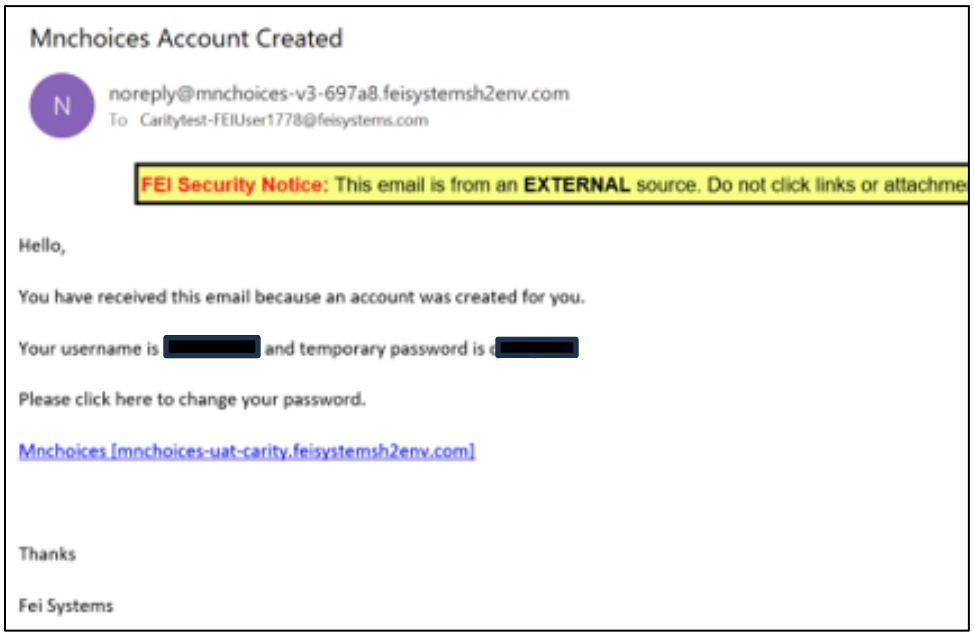
6. SSAM will send a communication to the Security Liaison indicating that the request was completed.

Emailed notifications from the MnCHOICES application relating to system access.

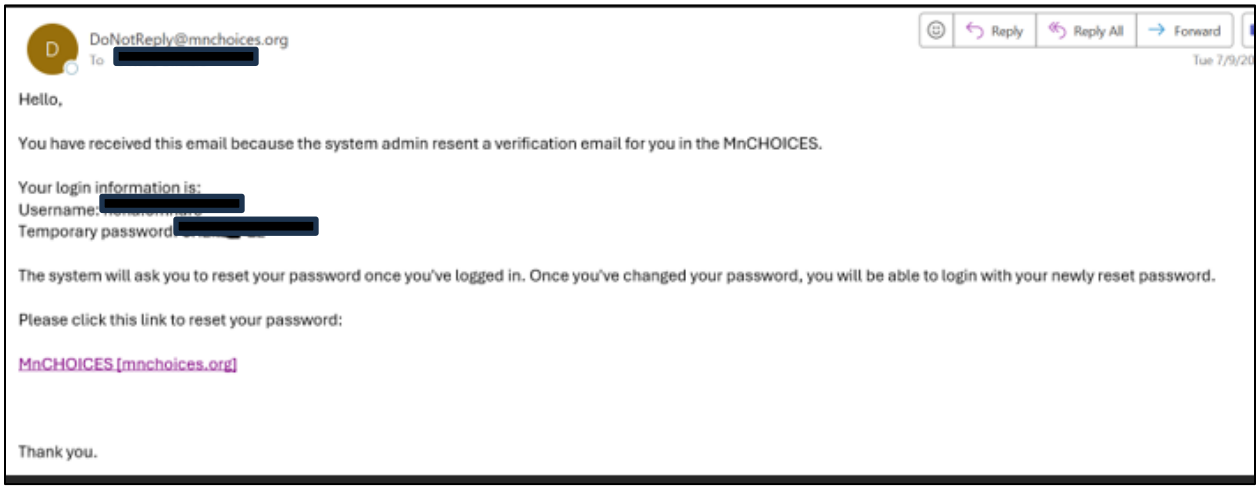
MnCHOICES will email the user for a few different scenarios. Examples of the common notifications relating to System Access are shown below.

1. When a user clicks on “Reset My Password,” this code expires within 1 hour.

2. SSAM links a staff record to a system account by using Create Account. The password in this notification expires within 7 days.



3. When SSAM resends a verification email, the system will resend the original onboarding email. The password in this notification expires within 7 days.



4. When SSAM updates the email address on the System Account, the password in this notification expires within 7 days.

From: <DoNotReply@carity-notification.feisystemsh2env.com>
Date: Thu, Jul 11, 2024, 4:04 PM
Subject: MnCHOICES System Account Verification
To: <[redacted]>

Hello,

You have received this email because the system admin changed the email for you in the MnCHOICES.

Your login information is:
Username: [redacted]
Temporary password: [redacted]

The system will ask you to reset your password once you've logged in. Once you've changed your password, you will be able to login with your newly reset password.

Please click this link to reset your password:

MnCHOICES [mnchoices-uat-carity.feisystemsh2env.com]

Thank you.

Infopac Reports/eReports

Infopac Reports are also known as eReports.

eReports (Infopac) is not available to all county staff. eReports (Infopac) gives access to reports used by specific people in the county.

Infopac/eReports can be requested via the System Access Request. You will need the Name/Number of the report(s) and the Printer ID to request reports.

BOBI Reports (Formerly BOEXI/TSS Reports/MEC² Reports/CPAT)

The TSS Reports System contains on-line reports for the MEC² County Users.

- TSS Reports information is available on SIR on the MEC² page. The link, called TSS Reports Information & Delegated Security Information, is located in the MEC² Content Areas of the page under the Security Information Section.
- The TSS BOEXI/Crystal Reports Master List is a documents that lists each report that is available. The list includes the report name and a description of the report. A link to the list is available on SIR on the MEC² page. It is located in the MEC² Content Areas of the page under the MEC² Reports Section.
- Training instructions are in the MEC² User Manual located under MEC² Links on SIR on the MEC² page.
- Direct questions on how to use the system to the MEC² Helpdesk or submit the TSS Helpdesk Request form found on SIR under the MAXIS or MEC² pages.

TSS Reports Tips:

- To locate a report in Info View, use the "SEARCH TITLE" on the Header Panel; for an example you will enter the report number FN100 and click the arrow to search for the report.
- In the top bar right hand corner of the page will show how many pages there are in the folder, the user can click the page number to proceed to the next page to view more reports.
- **CPAT** Reports are CSED/PRISM Reports
- Users have one password for the following systems: BOEXI (TSS Reports), CPAT and SMI. When you change the password, it changes it for all of the systems.

Security Access:

- To obtain access please submit the System Access Request.
- Security Liaisons cannot submit their own requests for access
- If a user is not a MAXIS or MEC² user, SSAM staff needs to be notified in order to set up a record of the user in our files.
- Some Security Liaisons now have the ability to add users to TSS Reports. If your county has delegated security, the liaison will not need to submit a request form to SSAM. For delegated security option check out: TSS Reports Information & Delegated Security Information under MEC²/Security page.

3 ways to view the reports:

1) A link on the MEC² IP on-line system to the reports is located at the bottom on the page in the system.
2) The direct link to the site, URL: https://creports.dhs.mn.gov/InfoViewApp/logon.jsp
3) On the SIR MEC² page there is a link on the right-hand side of the page under MEC² Links.

CPAT Reports: For unsuspends/password resets contact your Security Liaison as they can reset this password for you in SAM.
TSS Reports: For unsuspends/password resets contact your Security Liaison as they can reset this password for you in SAM.
System availability: Check the DHS-SIR Home page. TSS Reports is listed on the left-hand side of the page under System Availability along with several other systems.