TAC REMINDERS 2024

WHAT TRAINING FIELD SERVICES OFFERS

- UCJIS INQUIRY
- NCIC ENTRY
- QUARTERLY TRAINING
- SPECIFIC TRAINING IN-PERSON OR VIRTUAL AS REQUESTED

WHAT TRAINING FIELD SERVICES OFFERS

- E WARRANTS
- PUBLIC SAFETY ALERTS (AMBER, EMA, SILVER, AND BLUE ALERTS)
- NIBRS AND/OR USE OF FORCE
- AUDIT

BCI HAS FINGERPRINT READERS

- BCI AFIS has approximately 80 fingerprint readers that are bluetooth enabled
  - These are capable of doing quick ID and electronic citations
- If your agency would be interested in using these devices, please see Nicole Borgeson here at the conference or contact AFIS

TAC SPECIFIC REMINDERS

USERS VS NON-USER

- Users are someone that directly access the UCJIS system

- Non-access users-someone that receives information but does not have direct access to the system
  - All agency Administration **must** be setup as at least a non-access user, not as a non-user on the account of that ORI
- Non users-someone that does not have access to UCJIS
  - Don’t forget, your IT must be added to your ORI

AGENCY AGREEMENTS

If there is an administration change within your agency, we will need the following updated agreements:

- Agency Criminal Justice Agreement
- New ROA Agreement signed by the new administration (email Ofa Vaisima for more the information)
  - ovaisima@utah.gov
- Always use the most updated versions

AGENCY AGREEMENTS

What forms are sent to CIC and what forms are sent to your FS rep?

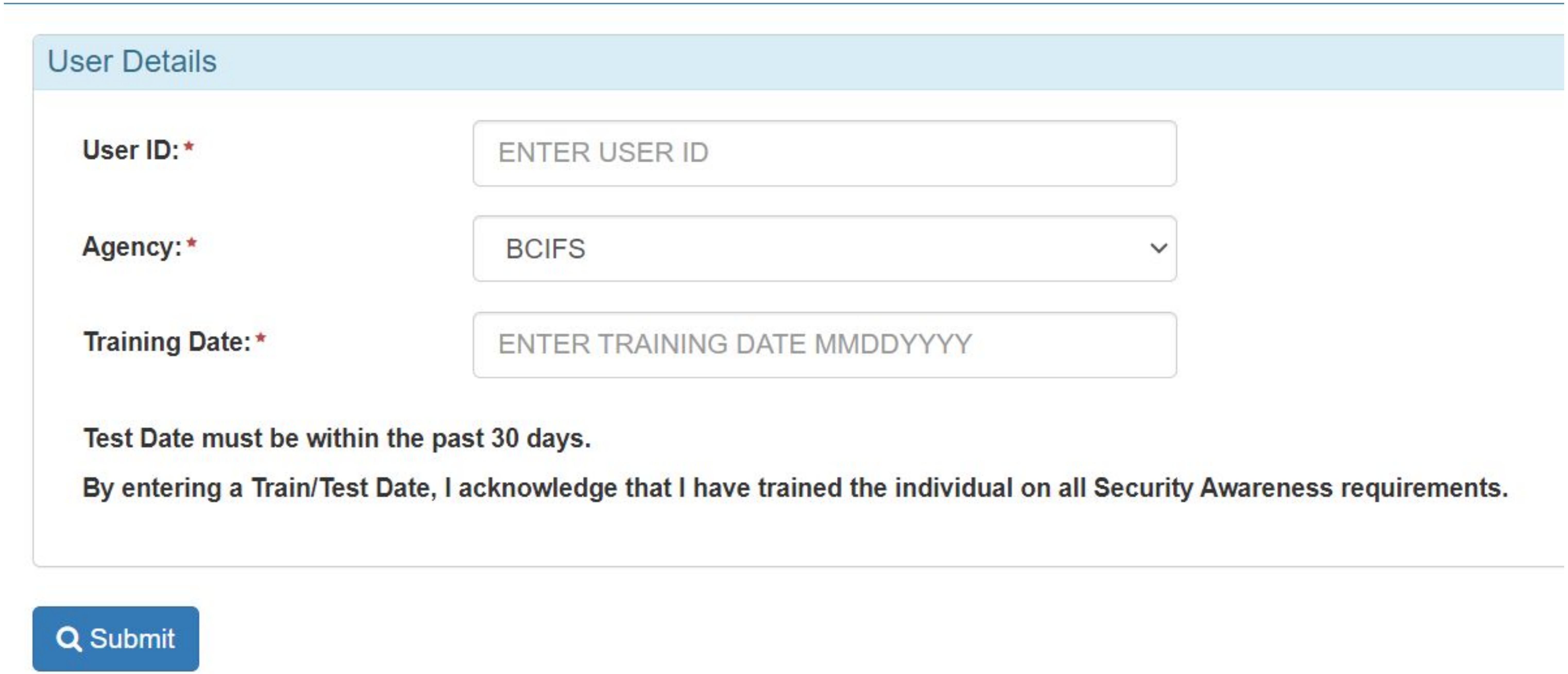
- Any google form such as user setup forms get sent to CIC
- The following forms need to be emailed to your FS rep -
  - Security agreements
  - Training and testing agreements
  - Hit confirmation agreements
  - All agreements **MUST** be updated versions found on the TAC website (outdated versions will not be accepted)

FINGERPRINT BILLING CODES

- When sending fingerprints in to BCI that they must be sent under the proper billing code
  - Agencies should be using billing code **B1019**
  - If fingerprints are sent to BCI by mail, please add "Attn: CIC"

Security Awareness Training (SAT)

- This is a new transaction you will use to update the security awareness training
- Security awareness training must be completed every year
- The SAT transaction will allow you to update that training
- If it expires, the user will not be able to log into UCJIS
- Shows when you run the REPT transaction
- TACs and Alt-TACs will have their security awareness training updated by their Field Service Representative



User Details

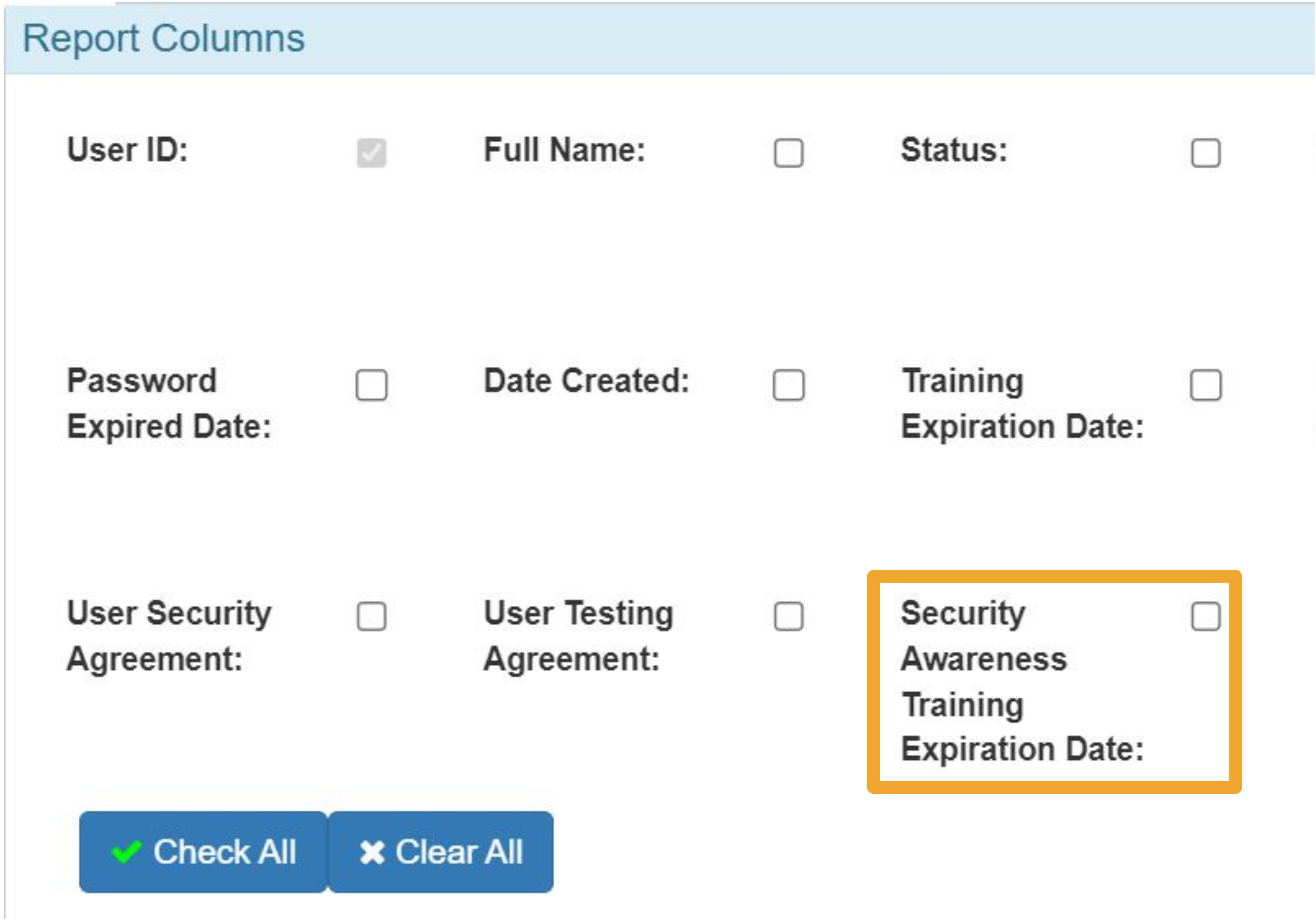
User ID:* ENTER USER ID

Agency:* BCIFS

Training Date:* ENTER TRAINING DATE MMDDYYYY

Test Date must be within the past 30 days.

By entering a Train/Test Date, I acknowledge that I have trained the individual on all Security Awareness requirements.



Report Columns

User ID:	☑	Full Name:	□	Status:	□
Password Expired Date:	□	Date Created:	□	Training Expiration Date:	□
User Security Agreement:	□	User Testing Agreement:	□	Security Awareness Training Expiration Date:	□

TAC TEST

- Available after TAC Conference
- Due October 31st
    - If you are a TAC or ALT TAC representing multiple ORIs, please put each individual ORI on your TAC test
- Don’t forget to email your certificate of completion to your Field Services Representative

HIT CONFIRMATION AGREEMENTS

- If you are not a 24/7 agency, there must be someone to respond to hit confirmations after hours
- You must have a hit confirmation agreement in place with a 24/7 agency
  - For example a 24/7 dispatch agency
- The agreement must state the days and times the agency will be responding to all hits on behalf of your agency
- Make sure this is kept on file and also send it to your FS rep

AGREEMENTS

- If agreements are sent in by mail, it may take longer to process
- The best way is to scan and email them to your Field Services rep
  - We can accept electronic signatures

AGREEMENTS

- Agreements should be sent to BCI by a TAC or ALT TAC and not the individual user
- When sending in a security agreement, make sure it is the correct type of agreement (user/non access user/non user)

PASSWORDS

- Passwords have previously been exactly 8 characters
  - As of 1/1/25 this will change, per CJIS Security Policy
- Passwords will be changing to require more than 8 characters
- There will be a reminder sent in December

RESETTING PASSWORDS

- When a TAC or Alt TAC are not available to reset a password users should call the UCJIS Help Desk
  - (801)965-4446

EMAIL ADDRESSES

- Personal emails should not be added to new UCJIS accounts when they are created
  - Individual work email should be used
    - Ex: gmcneil@utah.gov
- Avoid using group emails
- In the past, UCJIS information or eWarrants have been sent to personal email addresses associated with UCJIS accounts

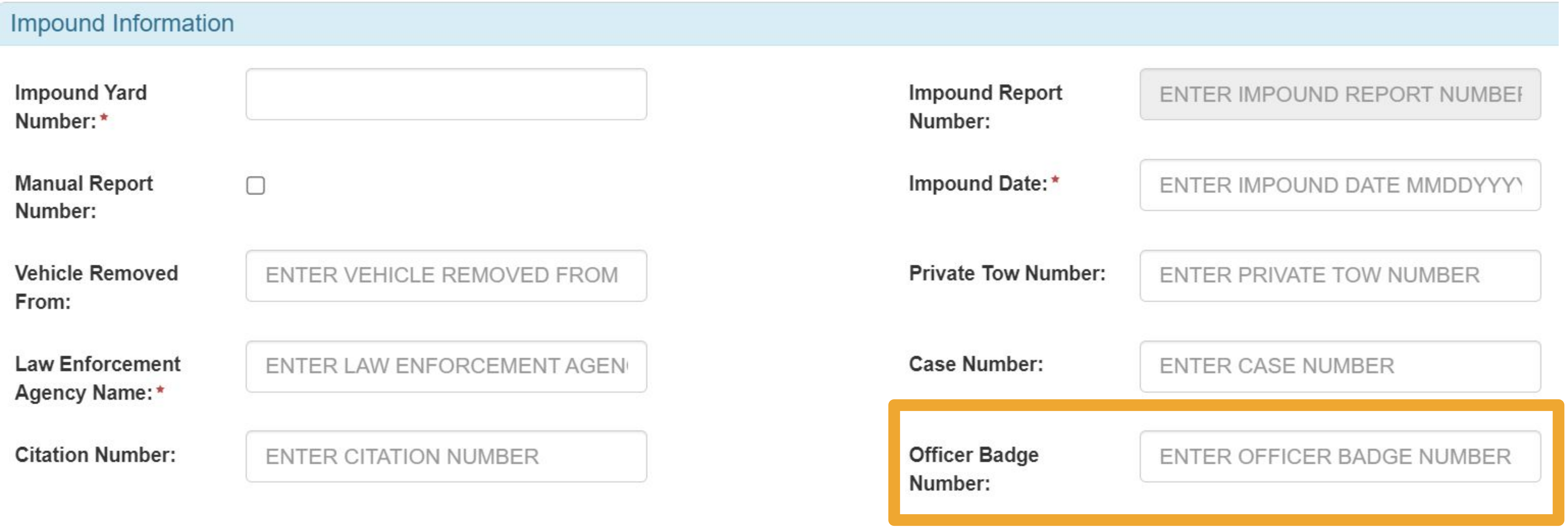
LOGS TRANSACTION

- All agencies are encouraged to run LOGS once a week
  - It does not matter if it is a law enforcement agency, prosecutor, court, or vender
  - BCI TAC responsibilities manual 9.0 Internal Agency Audits By TACS
- Watch for:
  - Improper purpose codes
  - Vague or incorrect auditing purpose
  - Common or famous names
  - Suspicious times and dates users are running things (misuse)
    - Ex: Employee works M-F, 8-5 but is running transactions on a Saturday evening

GENERAL REMINDERS AND UPDATES

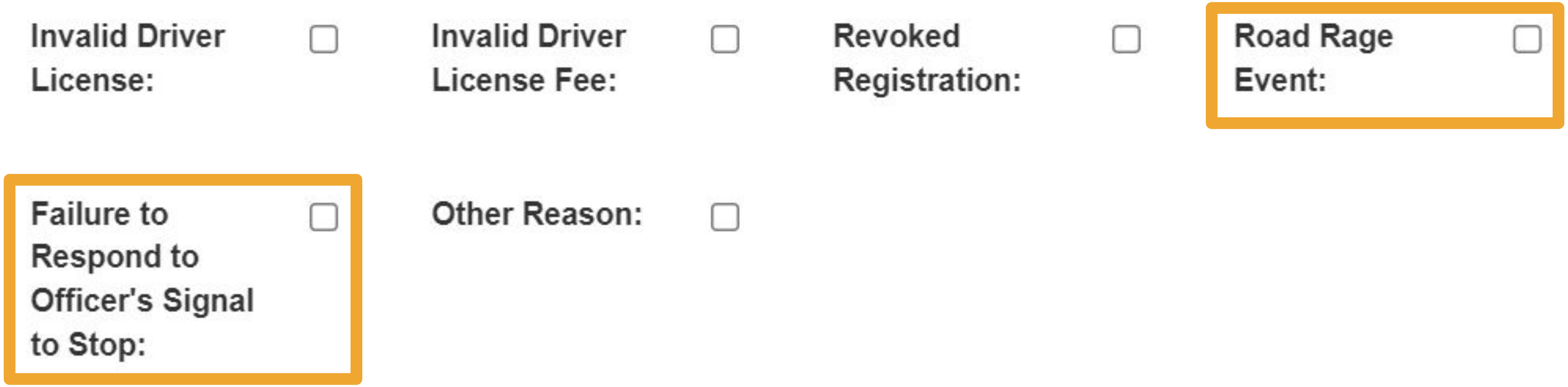
ENTER IMPOUND - EIMP

- New fields on the EIMP screen
  - Road rage
  - LEO stop
  - Officer badge number



Impound Information

Impound Yard Number:*		Impound Report Number:	ENTER IMPOUND REPORT NUMBE
Manual Report Number:	□	Impound Date:*	ENTER IMPOUND DATE MMDDYYY
Vehicle Removed From:	ENTER VEHICLE REMOVED FROM	Private Tow Number:	ENTER PRIVATE TOW NUMBER
Law Enforcement Agency Name:*	ENTER LAW ENFORCEMENT AGEN	Case Number:	ENTER CASE NUMBER
Citation Number:	ENTER CITATION NUMBER	Officer Badge Number:	ENTER OFFICER BADGE NUMBER



Invalid Driver License: □

Invalid Driver License Fee: □

Revoked Registration: □

Road Rage Event: □

Failure to Respond to Officer's Signal to Stop: □

Other Reason: □

JAIL REIMBURSEMENT - JRLL

- JRLL - Jail Reimbursement
- This is to replace the current process the jails go through when they house an inmate on behalf of the prison or other correctional facility
- Previously submitted to CCJJ on an Excel spreadsheet
- Now inside UCJIS
- More information will be provided by CCJJ and DTS

MEDICAL MARIJUANA

UCA 26B-4-202

(9)(C) A law enforcement officer who uses the database used by law enforcement to access information in the electronic verification system for a reason that is not administration of criminal justice is guilty of a **class B misdemeanor**

In summary MMJL misuse now matches UCA 53-10-108 to be a Class B Misdemeanor

UCJIS ERRORS

- UCJIS Help Desk - CIC
- When reporting any error that you are receiving during an NCIC entry or modify, please provide the UCJIS Help Desk with the following:
    - A screenshot of the actual error
    - A screenshot of the screen you are trying to enter with the information that you are entering

RECORD MANAGEMENT SYSTEM (RMS)

- May be used to store UCJIS information
- Must meet CJIS standards and policies
- Anyone using an RMS system must be set up as a user or non-access user and must be set up on that agency’s ORI because of the sensitive information stored within the system

DISSEMINATION FROM UCJIS

- Not allowed to disseminate UCJIS information to:
  - City mayor
  - Fire department or EMT (unless they have proper UCJIS access and authorization to receive the information)
    - Ex: arson investigator
  - City council member
  - Legislator or representative of the legislature
  - Civilians
  - Attorney that refuses to get access to UCJIS (must be an authorized recipient)
  - Coaches/rec center employees

RIGHT OF ACCESS (ROA)

When renewing your ROA Contract **OR** initially becoming a ROA provider, agencies must submit the following:

- ROA Provider Information Sheet
  - This will provide BCI with your agency's information for the BCI website and will also provide BCI with the contact information for your agency regarding ROAs

RIGHT OF ACCESS (ROA)

- ROA Contract
  - The contract must be signed and submitted to BCI before your agency can run ROAs
    - Use purpose code P
- The contact information for the ROA POC is for BCI use only. We will not share that with the public
- Questions?
  - Contact Ofa Vaisima
    - ovaisima@utah.gov or (385)499-1421

UNIFORM CRIME REPORTING (UCR)
USE OF FORCE

- During the most recent FBI NIBRS Audit, the FBI found that many agencies are classifying Larceny and Fraud offenses incorrectly. Remember to always match your case/incident to the best definition possible for each offense before selecting the catch-all category
- Both NIBRS and UCR reports are due by the 16th of each month. If your agency does not have Use of Force incidents to report, a Zero Report must be entered

UNIFORM CRIME REPORTING (UCR)
USE OF FORCE

- For Use of Force permissions or to verify who in your agency has access, please contact Alex Martinez
  - mmartinez@utah.gov
- Please review the monthly validations to ensure your NIBRS and Use of Force data are being reported correctly
  - UCR validations are sent out monthly
  - Use of Force validations are sent out bi-monthly

ENDANGERED MISSING ADVISORY (EMA)

EMA transaction

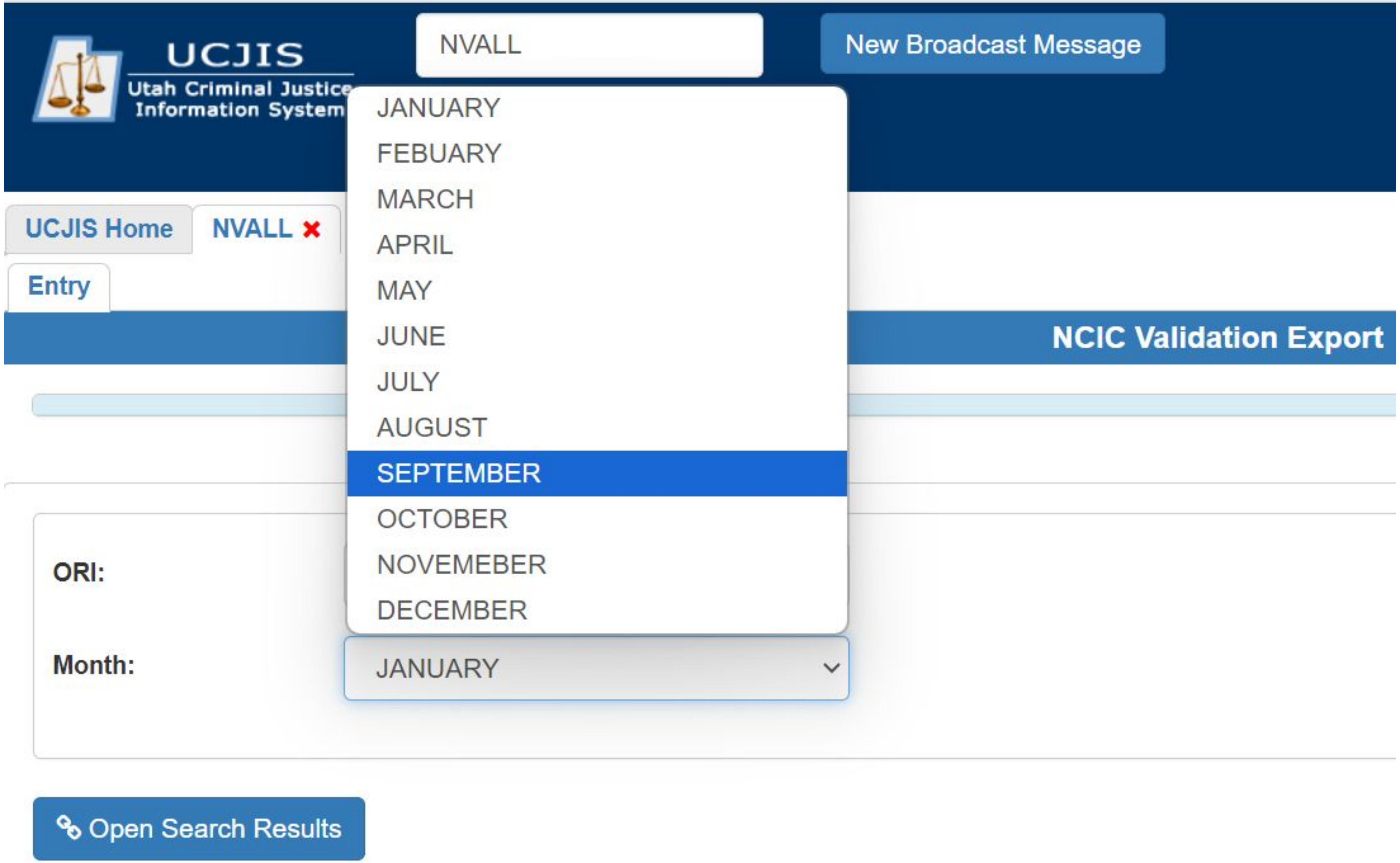
- Is the person believed to be in danger due to:
  - Age
  - Health
  - Mental disability (such as autism or alzheimer's - could be a Silver Alert)
  - In the company of a potentially dangerous person
  - Any other factor that may put the person in peril such as:
    - Internet enticed, missing college student, or overdue traveler or hiker

ENDANGERED MISSING ADVISORY (EMA)

- Entering a qualifying missing endangered person into NCIC will not issue an EMA
    - First enter the missing person, then use the EMA transaction to issue the alert
- BCI offers training on the EMA as well as all other alerts for agencies that are authorized to activate alerts
- If you would like to schedule training, contact:
    - Ofa Vaisima oviasima@utah.gov or
    - Alex Martinez mmartinez@utah.gov

NCIC VALIDATIONS - NVAL

- No more SFTP server
- New way you will access your monthly validations
- This transaction was not granted automatically
  - If you do not have access, contact CIC or your FS Representative to get the permission granted
- May pull validations up to one year prior



NCIC Validation Export

ORI:

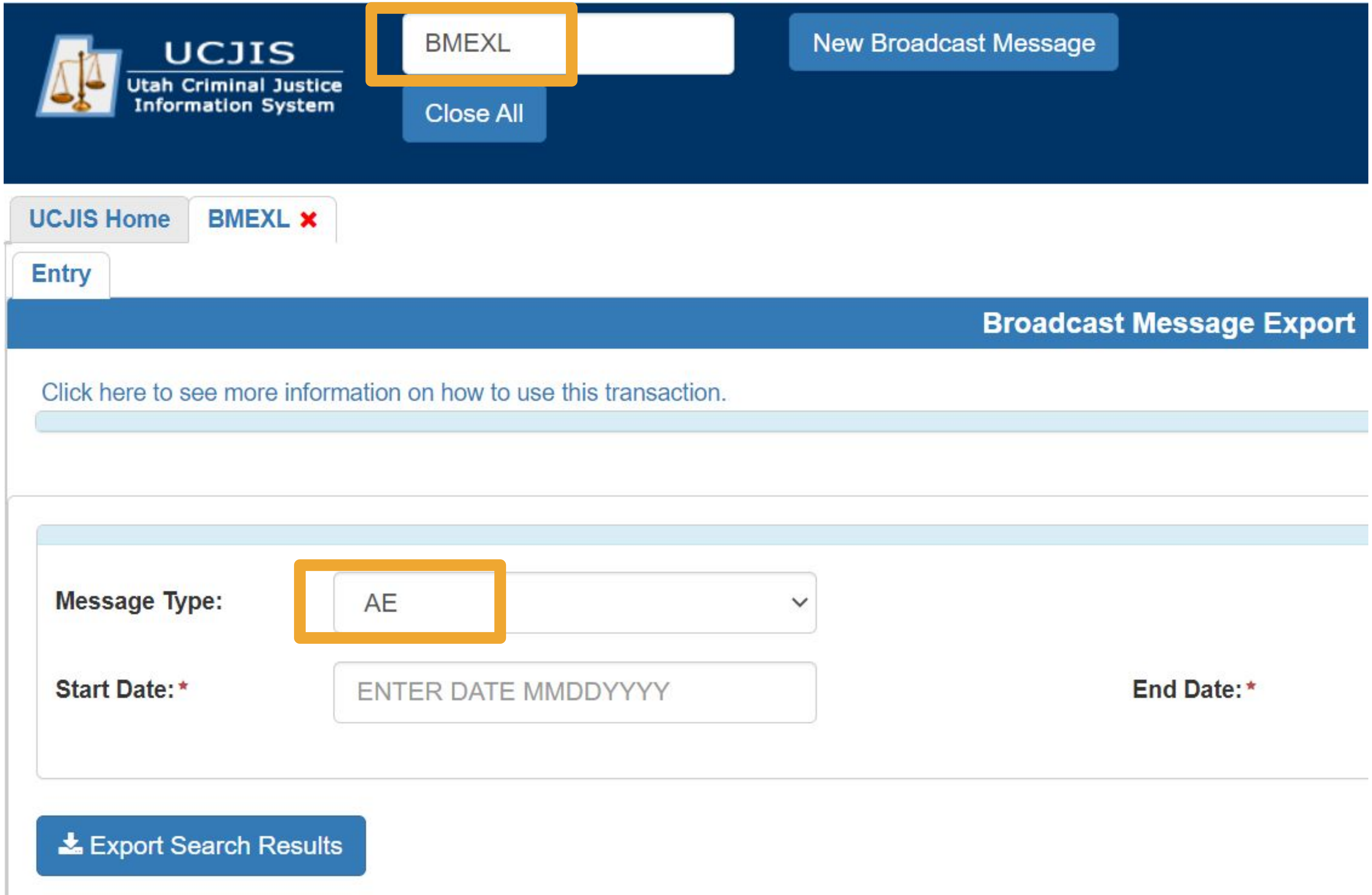
Month: JANUARY

AUTO EXPUNGEMENTS (AE)

- Agencies should be watching broadcast messages for all AE messages
- Logs will only go back 21 days
  - To go back any further use the BMEX transaction
- If you have any questions regarding AE you can contact the BCI Expungements section
  - autoexpungements@utah.gov

EXPUNGEMENT BROADCAST MESSAGES - BMEX

- This transaction is a message export
    - The transaction allows agencies to pull past broadcast messages regarding auto expungements (AE) and expungements (EX)
        - It will only pull AE and EX messages
    - You can limit it by searching for a specific date range
    - Results go as far back as January 2022



BMEXL

Broadcast Message Export

Click here to see more information on how to use this transaction.

Message Type: AE

Start Date:* ENTER DATE MMDDYYYY

End Date:*

NCIC VIOLENT PERSON FILE (VPF)

The Violent Person File was designed to alert law enforcement officers that an individual they are encountering may have the capacity for violence against law enforcement

NCIC VIOLENT PERSON FILE (VPF)

An entry into the VPF should be made when at least one of the following criteria has been met:

- Offender has been convicted for assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement
- Offender has been convicted of a violent offense against a person to include homicide and attempted homicide

NCIC VIOLENT PERSON FILE (VPF)

- Offender has been convicted of a violent offense against a person where a firearm or weapon was used
- A law enforcement agency, based on its official investigatory duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community
- Questions?
    - Contact NCIC at (304)625-3000
    - NCIC Manual (TAC web site)
    - BCI will also pass along additional training

AGENCY AUDIT FINDINGS

- Common findings from agency audits that were conducted by the Field Services reps this audit cycle
- A new audit cycle will start after this TAC conference
- Incorrect date of theft (DOT) or date of last contact (DLC)
- Agreements not being submitted in a timely manner (Security Agreements or Testing & Training Agreements)

AGENCY AUDIT FINDINGS

- NCIC miscellaneous (MIS) field: Description of scars, marks and tattoos are not being added to this section
  - Aids law enforcement in identifying missing or wanted persons
- All NCIC entries must have supporting documentation.
  - Documentation must be on file and available in order to maintain the entry in NCIC
- Up-to-date hit confirmation agreements
- Missed hit confirmation requests

AGENCY AUDIT FINDINGS

- Background checks for ride alongs are being ran with purpose code P
  - Should be purpose code C
- Not having a formal SWW and NCIC validation policy in place
  - If your agency has the potential to have a felony warrant placed under your ORI, you are required to have a NCIC validation policy

AGENCY AUDIT FINDINGS

- NCIC records are not being packed with all information available
  - The better the record is packed, the greater potential of a hit
- Vague audit purposes. “Investigations” or “criminal” should not be used
  - Case number, citation number, or an incident number

AGENCY AUDIT FINDINGS

- Release of firearms
  - Use purpose code “F”
    - Not purpose code “C”
  - UCA 77-11a-402(2) requires law enforcement releasing a firearm to submit a Firearms Release Form to the Brady section to make sure the individual is not a restricted person
  - The form can be found on the BCI website under the Brady tab, law enforcement tab
  - Questions?
    - Contact the Brady Section
      - (801)965-GUNS(4867)
      - bcibrady@utah.gov

ORDERING FINGERPRINT CARDS

- Fingerprint cards must be ordered directly from the FBI
- Link on following slide
    - FD-249 Criminal cards (white card/red ink)
    - FD-258 Applicant cards (white card/blue ink)
- Questions
    - Contact BCI AFIS Section
        - dpsafis@utah.gov

https://forms.fbi.gov/cjis-fingerprinting-supply-requisition-form

NCIC ENTRIES

- NCIC entries automatically list your agency's primary phone number. This number is provided by agencies on their yearly ORI Validation Forms. If this number is incorrect, please contact your FS rep to update it. This number needs to be a number within your agency, it cannot be the phone number for an agency who handles your hits or dispatches for you
- Agencies who aren't 24-hour and have an agreement in place with a 24-hour agency must place instructions in NCIC entry (MIS field) on who to contact after hours. This can be the phone number of the ORI handling after hour hits or their ORI

UTAH CRIMINAL HISTORY (UCH)

Citations

- BCI records must have a legible fingerprint, the charges listed, and the correct court of next appearance. Without a fingerprint, we cannot verify who the criminal history belongs to or properly create a new history
- If your subject is NOT booked into jail and a citation is submitted without a print, the charge(s) **CANNOT** be added to UCH. Please keep this in mind when issuing a citation. Lack of a fingerprint will also result in the citation being sent back to your agency

UTAH CRIMINAL HISTORY (UCH)

- UCA 53-10-207(2) requires declinations and fail to file decisions to be forwarded to BCI “within 14 working days”
- Declination/Fail to File Form
  - https://ucjis-tac.utah.gov/wp-content/uploads/sites/38/2022/08/BCI-REQUEST-FORM.pdf
- BCI will contact you for information to update the disposition if we never received information

UTAH CRIMINAL HISTORY (UCH)

- To add or remove charges or information from Utah Criminal History, please use the Change Request Form on the TAC webpage
  - https://ucjis-tac.utah.gov/wp-content/uploads/sites/38/2022/08/BCI-REQUEST-FORM.pdf
- Questions?
  - BCI Records Section
    - bcirecords@utah.gov

UTAH CRIMINAL HISTORY (UCH)

- Training available
  - Fingerprints
  - Suspense File
  - Utah Criminal History
  - Citations
- Contact Erin Paulsen
  - epaulsen1@utah.gov

UTAH CRIMINAL HISTORY (UCH)

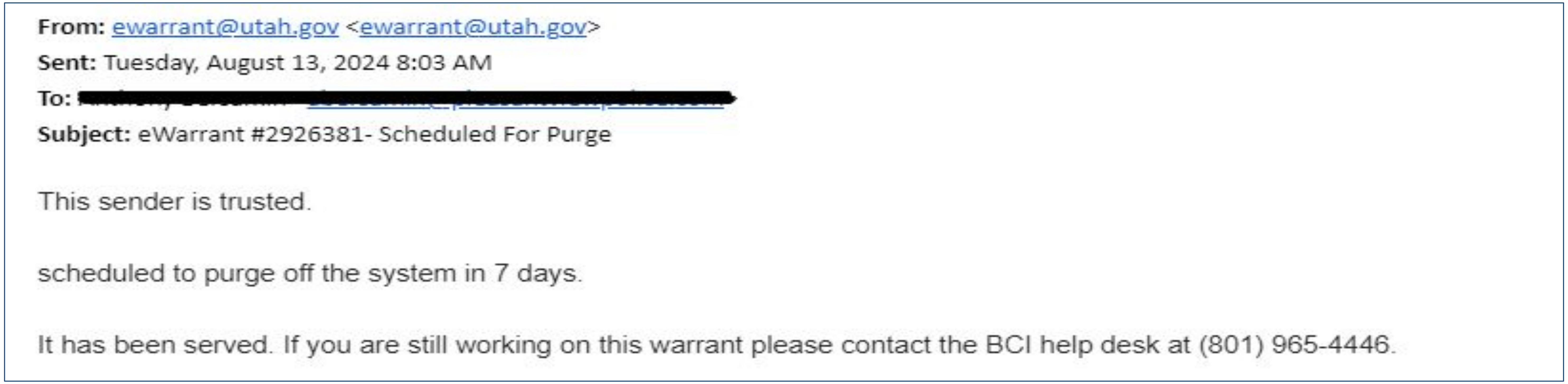
- Fingerprinting on new charges - if you add more charges at a later time, fingerprint them again if they are still in custody
- If you want charges under one OTN or they are not in custody, send BCI info through a Change Request Form
  - https://ucjis-tac.utah.gov/wp-content/uploads/sites/38/2022/08/BCI-REQUEST-FORM.pdf
  - Include related OTN(s)

REJECTED CITATION EMAIL

Contact the Administrative Office of the Courts (AOC) and let them know the best email address for these rejection notifications

EWARRANTS

- eWarrants (all types) will now receive a "Scheduled for purge" email
  - This email will be sent if an eWarrant has been served or has met its expiration date



From: ewarrant@utah.gov <ewarrant@utah.gov>
Sent: Tuesday, August 13, 2024 8:03 AM
To: [redacted]
Subject: eWarrant #2926381- Scheduled For Purge

This sender is trusted.

scheduled to purge off the system in 7 days.

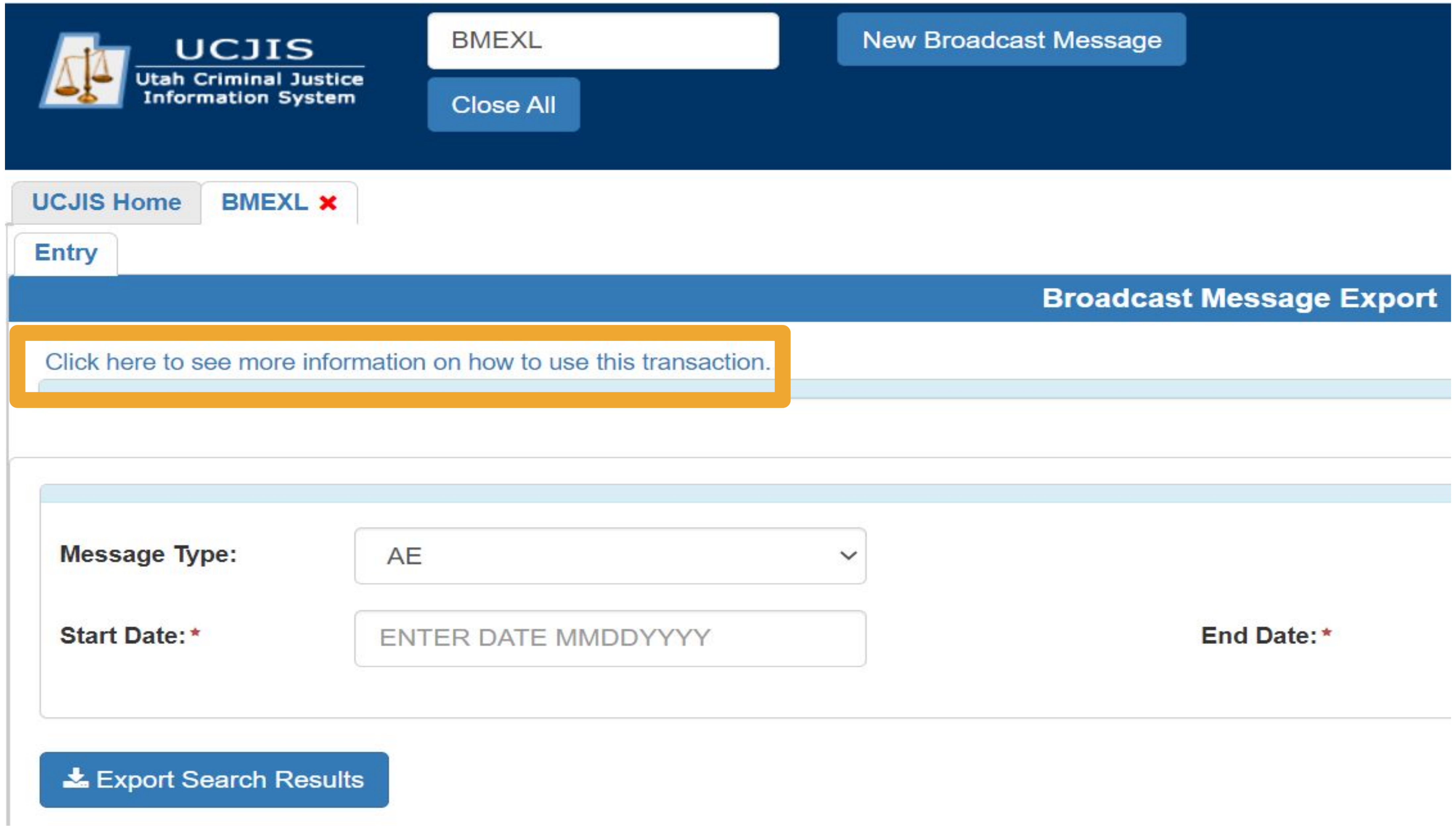
It has been served. If you are still working on this warrant please contact the BCI help desk at (801) 965-4446.

PROTECTIVE ORDERS

- Courts are responsible to validate protective orders using the MPO transaction
- Utilize all available files to make sure the record contains all available information
    - CORIS
    - UCJIS
- Remember to properly clear or cancel the PO
    - XPO - cancel
    - CPO - clear

UCJIS ON-SCREEN HELP

- Mini presentations
- Embedded on transaction screens in UCJIS



Message Type: AE

Start Date:* ENTER DATE MMDDYYYY

End Date:*

CRASH AND CITATIONS

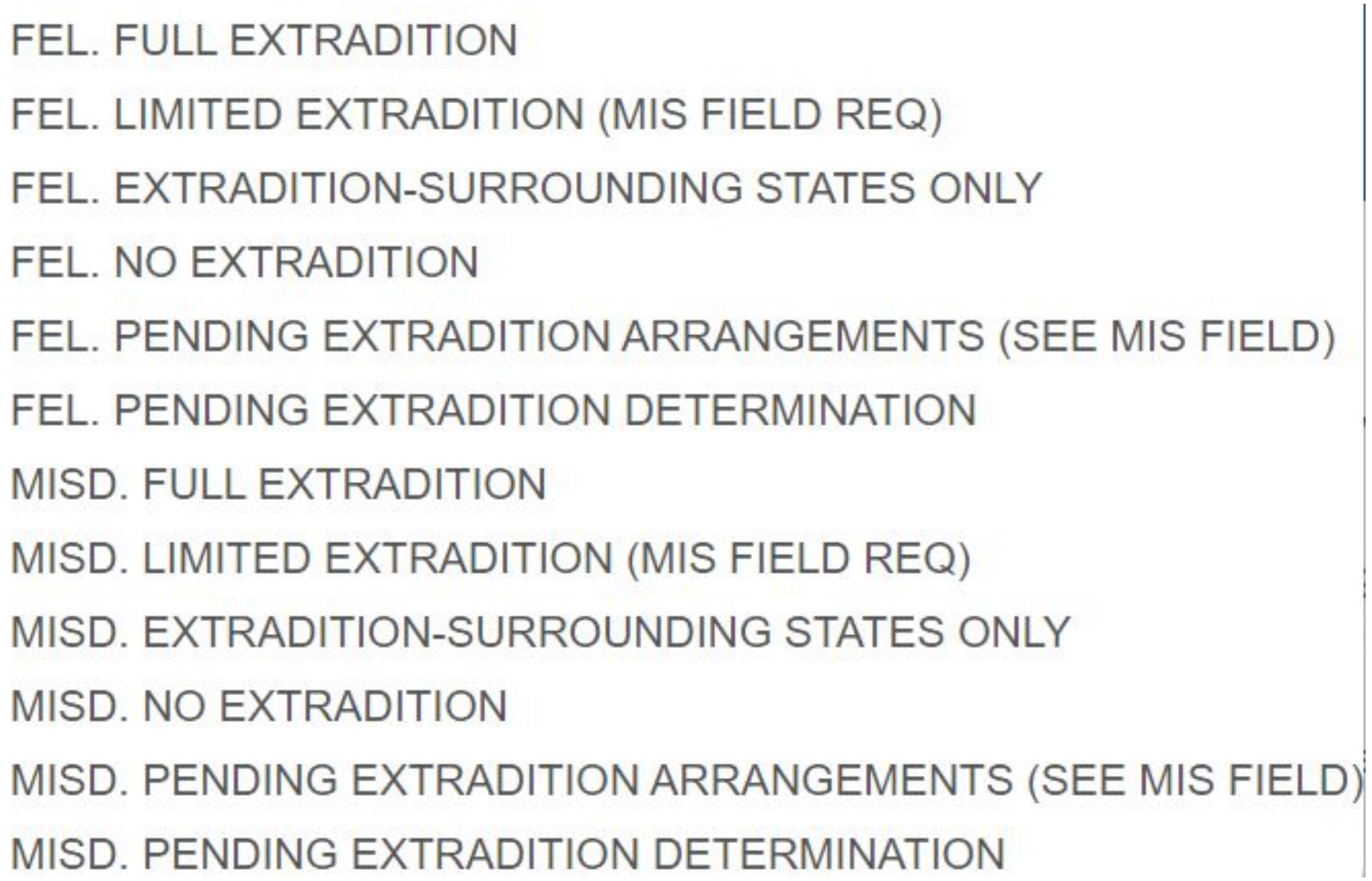
- If there are any questions concerning crash and citations you can get more information at this website
  - https://highwaysafety.utah.gov/crash-data/crash-entry-help/
  - Contact Barbara Freeman at the Utah DPS Highway Safety Office
    - (801)783-7250
    - bafreeman@utah.gov

CUSTODIAL (JAIL) FACILITY VISITORS

- When an individual is turned away from visiting someone in a correctional facility due to a warrant, criminal history, etc.
    - They should not be told to call BCI to find out why
        - BCI cannot give that information out over the phone
    - They can request a copy of their Utah Criminal History either in person at BCI or by mail
    - They can also check for warrants on bci.utah.gov

Extradition

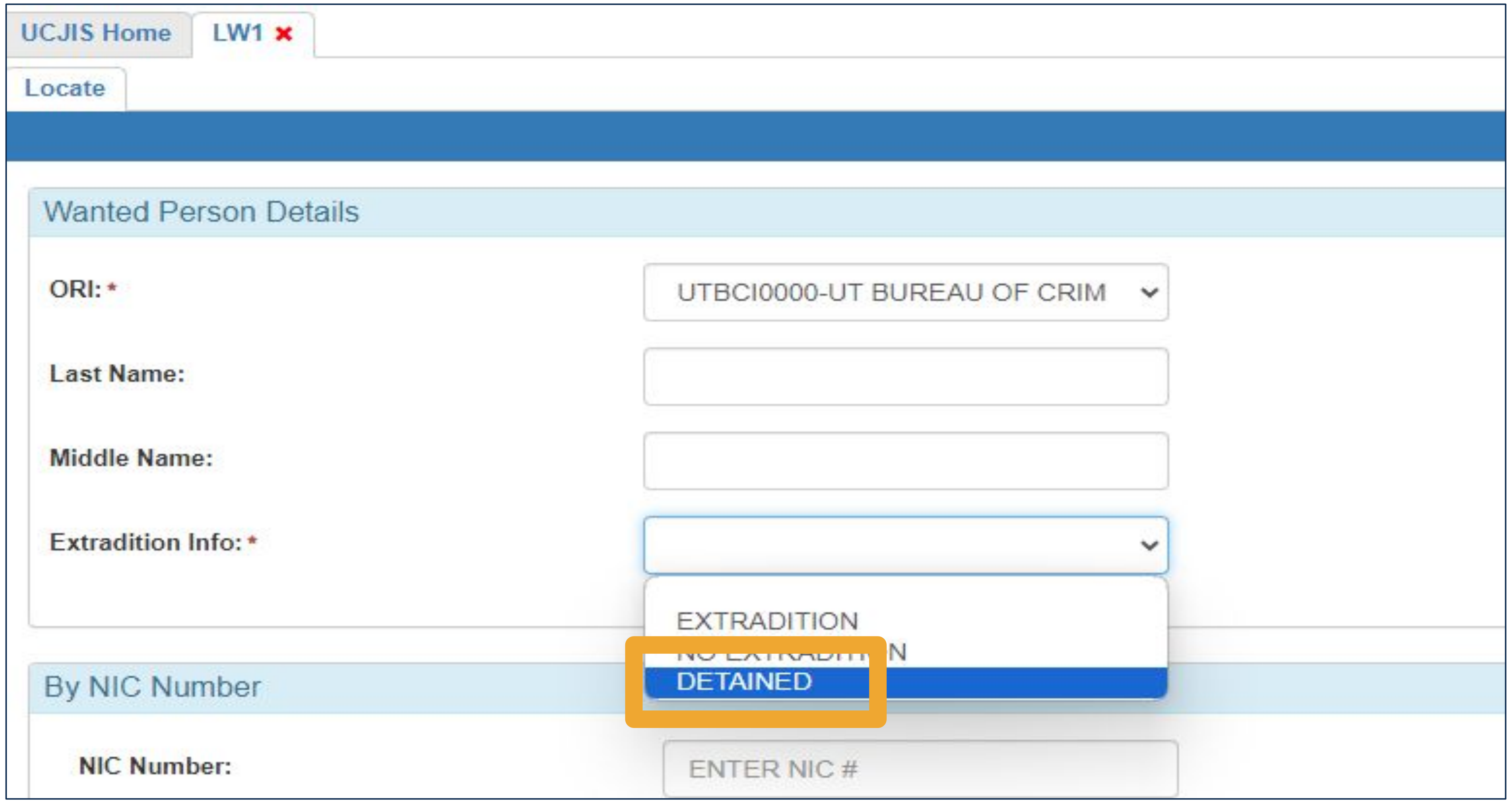
- Please remember to select the correct Extradition information when entering a warrant
- The holding agency should put a locate on an individual if it is within the specified extradition on the warrant



FEL. FULL EXTRADITION
FEL. LIMITED EXTRADITION (MIS FIELD REQ)
FEL. EXTRADITION-SURROUNDING STATES ONLY
FEL. NO EXTRADITION
FEL. PENDING EXTRADITION ARRANGEMENTS (SEE MIS FIELD)
FEL. PENDING EXTRADITION DETERMINATION
MISD. FULL EXTRADITION
MISD. LIMITED EXTRADITION (MIS FIELD REQ)
MISD. EXTRADITION-SURROUNDING STATES ONLY
MISD. NO EXTRADITION
MISD. PENDING EXTRADITION ARRANGEMENTS (SEE MIS FIELD)
MISD. PENDING EXTRADITION DETERMINATION

DETAINERS

- If a locating agency is detaining and holding an individual on local charges before extradition will occur, the locating agency should select ‘Detained’ for the extradition on the locate. If they do not, the entering agency will be notified to remove the record from NCIC



Wanted Person Details

ORI: * UTBCI0000-UT BUREAU OF CRIM

Last Name:

Middle Name:

Extradition Info: *

EXTRADITION
NO EXTRADITION
DETAINED

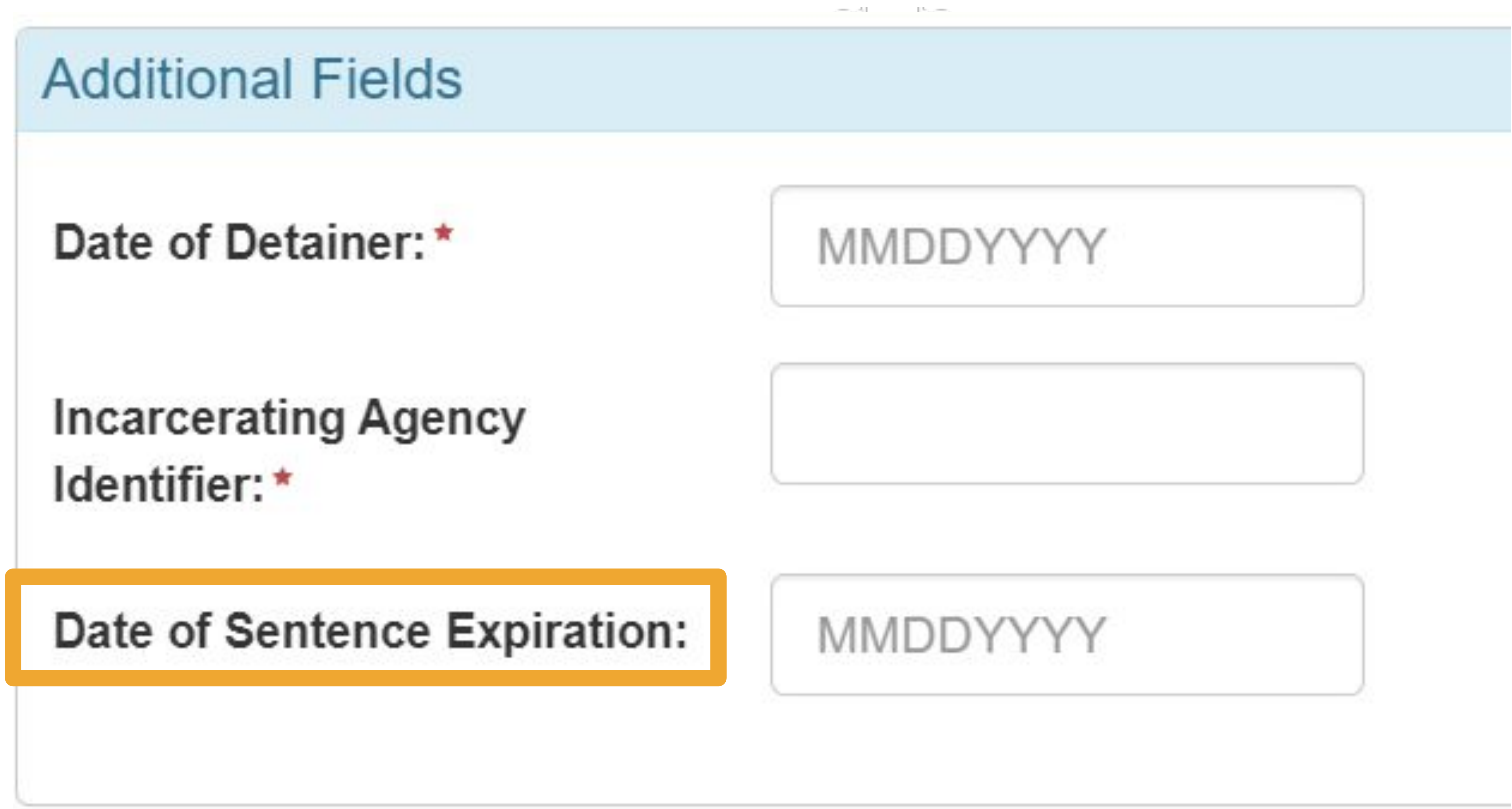
By NIC Number

NIC Number: ENTER NIC #

DETAINERS

- If “detained” is not selected, the entering agency must modify their detainer with the ‘Sentence Expiration’ information. This will allow the entering agency to keep their NCIC listed
- The entering agency will get a $. notification 5 days before the sentence expiration date as a reminder that the individual is being released and extradition should be coordinated with the holding agency
- This extra work can be avoided if the locating agency places the locate correctly, selecting “detained” in the locate transaction

DETAINERS



Additional Fields

Date of Detainer: * MMDDYYYY

Incarcerating Agency Identifier: *

Date of Sentence Expiration: MMDDYYYY

TRAFFIC STOPS

- During traffic stops, if the registered owner (RO) is not the driver of the vehicle, law enforcement should not run the RO in UCH/III
  - For example, if Driver A is driving Driver B's vehicle and is pulled over, Driver B cannot be run. The only exception would be upon crash or impound to get contact information
  - Only Driver License (not UCH/III)

Security Awareness

Overview of Privacy & Security Awareness Training

```
                height="450" viewBox="0 0 800 450" xmlns=[illegible]
  <defs>
    <linearGradient x1="100%" y1="0%" x2=[illegible] y2=[illegible] id=[illegible]
      <stop stop-color="#06101F" offset=[illegible]/>
      <stop stop-color="#1D304B" offset=[illegible]/>
    </linearGradient>
  </defs>
  <rect width="800" height="450" rx="8" fill=[illegible]
</svg>
<div class="media-control">
  <svg width="96" height="96" viewBox="0 0 96 96" xmlns=[illegible]
    <defs>
      <linearGradient x1="87.565%" y1=[illegible]
        <stop stop-color="#FFF" stop-opacity=[illegible]
        <stop stop-color="#FFF" offset=[illegible]/>
      </linearGradient>
      <filter x="-500%" y="-500%" width=[illegible]
        <feOffset dy="16" in="SourceAlpha" [illegible]
        <feGaussianBlur stdDeviation=[illegible]
        <feColorMatrix values=[illegible]
      </filter>
              fill-rule="evenodd">
                cx="48" cy=[illegible]
```

- Purpose:
  - To educate employees about their roles and responsibilities in protecting sensitive information.
  - To inform about applicable privacy laws and security policies.
- Importance:
  - Ensures compliance with CJIS (Criminal Justice Information Services) requirements.
  - Protects the organization from data breaches and legal violations.

User Security Responsibilities

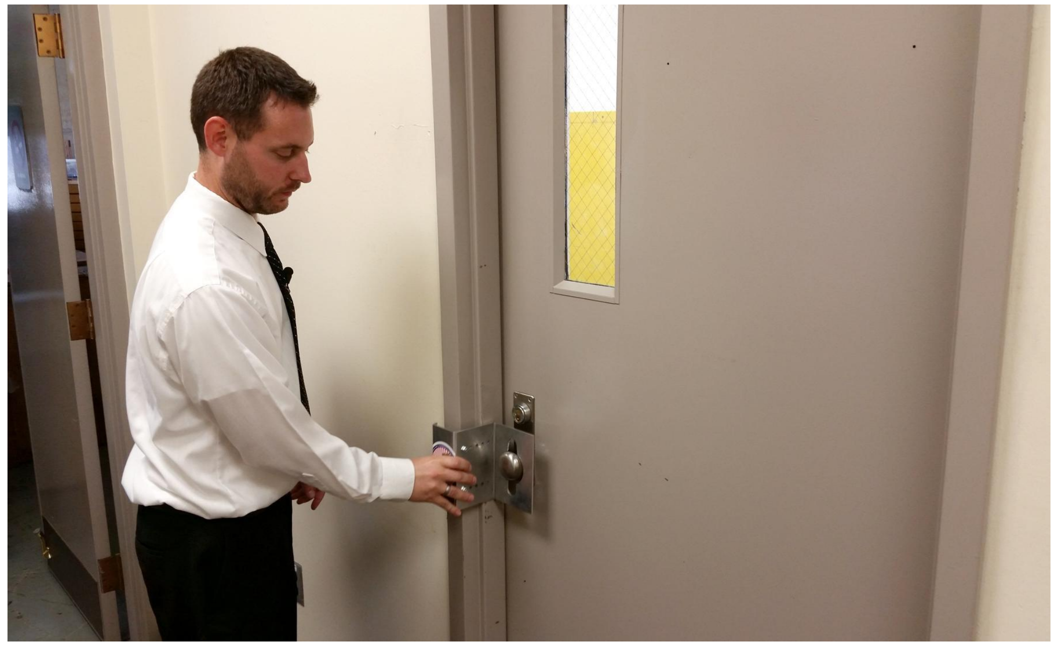
- User Roles:
  - General Users:
    - Limited access to sensitive data.
    - Responsible for safeguarding their login credentials.
  - Privileged Users:
    - Access to sensitive and confidential information.
    - Required to follow stricter security protocols and reporting any anomalies.
  - Organizational Personnel:
    - Responsible for overall security measures.
    - Required to ensure their teams understand and follow security policies.

TOP SECRET
CONFIDENTIAL
TOP SECRET

Logins and Password Management

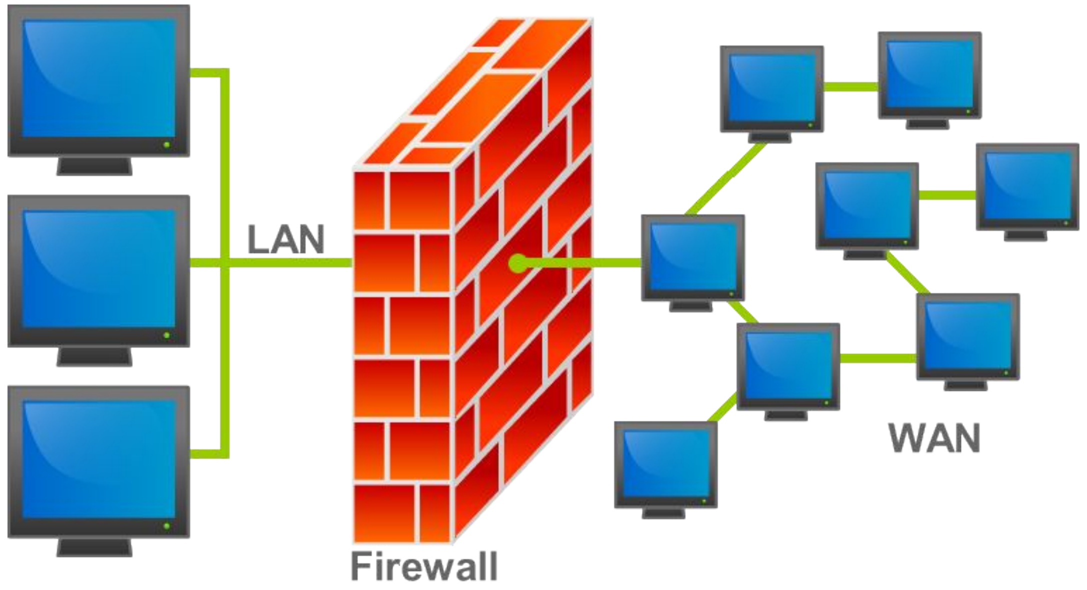
- Login Policies:
    a. Every employee must maintain a unique login to ensure accountability.
    b. Sharing credentials is strictly prohibited.
- Password Standards:
    a. Passwords should be at least eight characters long, containing a mix of upper and lowercase letters, numbers, and special characters.
    b. Passwords must be changed every 90 days to enhance security and prevent unauthorized access.
    c. Consider implementing multi-factor authentication (MFA) for additional security.

Workplace Security Protocols



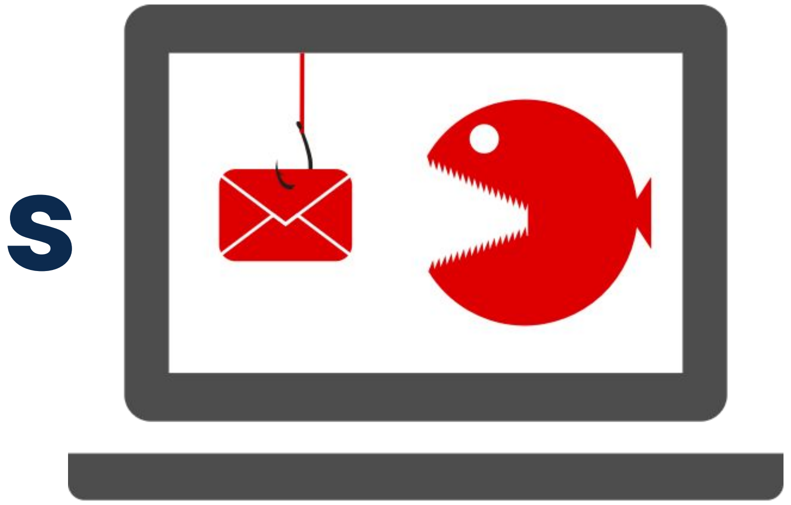
- Security Measures:
  - Computers should be placed in secure areas where unauthorized persons cannot view screens.
  - Ensure physical security through locked doors and secured entry points.
- Visitor Access Control:
  - All visitors must sign in and be issued badges.
  - Visitors must be escorted by authorized personnel throughout their stay.

Information Security Policies



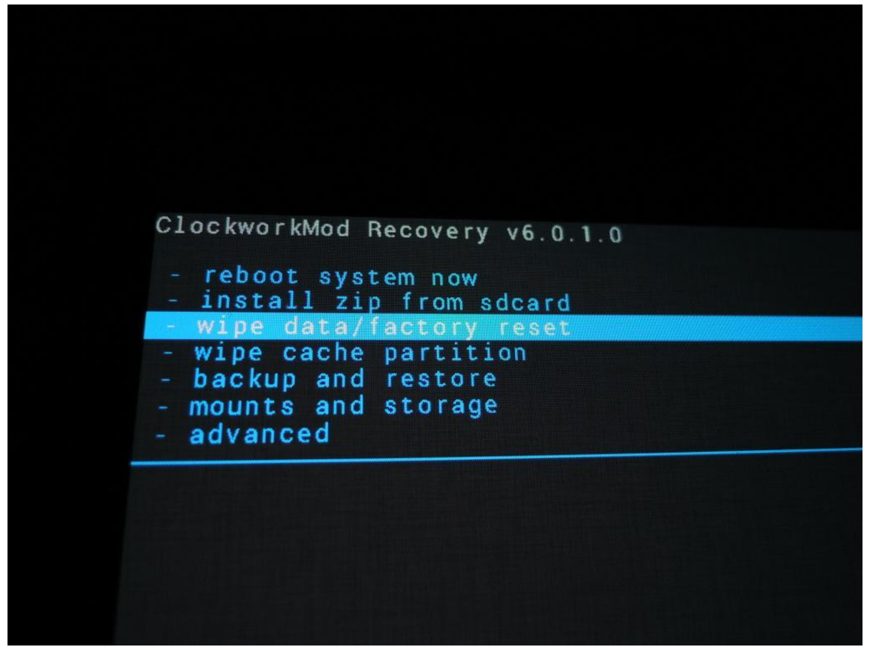
- Legal Compliance:
  - UCJIS files and related data must comply with all applicable federal and state laws regarding data protection.
- Technical Controls:
  - Firewalls and spam filters must be in place to guard against external threats.
  - Operating systems and applications should be updated regularly to patch vulnerabilities.
- Wireless Security:
  - Implement WPA2 encryption for wireless networks to protect data in transit.
  - Regularly review and update network configurations.

Social Engineering & Insider Threats



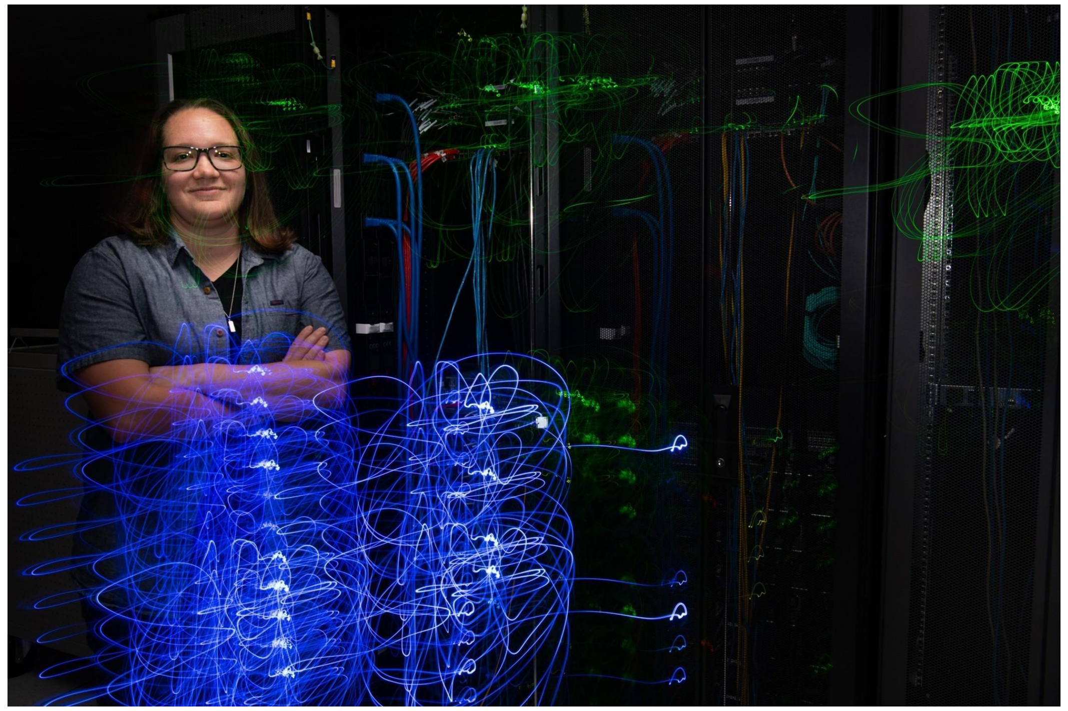
- Understanding Tactics:
  - Phishing: Emails attempting to trick users into providing sensitive information.
  - Shoulder Surfing: Observing someone entering sensitive information, such as passwords.
  - Baiting: Offering something enticing to manipulate individuals into revealing information.
- Prevention:
  - Regular training on recognizing social engineering tactics.
  - Encourage a culture of reporting suspicious activities.

Data Handling & Dissemination



- Information Guidelines:
  - All communication regarding sensitive data should include a clear record (who accessed it, what was shared, when, and why).
  - Only share sensitive data with authorized personnel who have a legitimate need to know.
- Data Destruction:
  - Securely dispose of printed documents by cross-cut shredding.
  - Ensure electronic data is wiped or destroyed following established protocols to prevent recovery.

Incident Response and Threat Management



- Incident Procedures:
  - Establish a clear process for reporting, tracking, and documenting security incidents.
  - Conduct regular exercises to ensure preparedness among employees.
- Preparedness:
  - Train staff to recognize signs of digital threats, such as unusual activity on systems.
  - Develop a disaster recovery plan that includes data backup strategies.
- Mobile Devices Require Multi Factor Authentication
  - You must have an MFA set up for mobile devices

Consequences of Security Misuse

- Penalties:
  a. Failure to comply with privacy and security policies may result in civil lawsuits against the organization and personal repercussions for involved employees.
- Compliance Importance:
  a. Consistent adherence to policies protects not just the organization but also the careers and reputations of employees.
  b. Non-compliance can lead to serious legal ramifications and loss of public trust.

Kahoot Time!