**Level 2**

**Slide 203**

**RECORD ENTRY TYPES**

**ENTRY, MODIFY, SUPPLEMENTAL, LOCATE, CLEAR, CANCEL**

**Level II training reviews many of the files we looked at in level one but this time we are going to look at it from an entry standpoint. What do some of our screens look like? How do we know what to enter? Where can we find certain bits of information? Level 2 focuses on how records are placed into the files, not on what the returns look like.**

**These are the different entry types in the system and we are going to look and talk about each one.**

**Trainers: As you go through these slides you will see examples of different types of systems, OMNIXX (the new ACCESS switch), New World, Spillman..etc. Some will be familiar with the way they look, some will not.**

**Slide 204**
**RECORD ENTRY**

**Here is an example of an entry screen. Most types of screens will have the required fields highlighted, bolded or a different color, or pronounced in some way. There are many fields that are only optional.**

**Some fields are only required when one field is filled in. For example if you enter an OLN (which is not required) the system will now require the state and year of expiration because they are all tied together. These fields are called conditional.**

**Slide 205**

**MODIFY BASE RECORD**

**ADD**

FILLS IN INFORMATION IN A BLANK FIELD

**DELETE**

REMOVES INFORMATION FROM A FIELD

**CHANGE**

CORRECTS INFORMATION IN A FIELD

**We spoke about what a base record is, in Level 1. You can modify the base record of your entry by adding information you now have that you didn’t have originally, by deleting information that should not have been entered originally or by correcting a field in a record that is incorrect.**

**Slide 206**

**SUPPLEMENTAL ENTRY**

A SUPPLEMENTAL ENTRY CANNOT BE MODIFIED, THE SUPPLEMENTAL MUST BE CANCELLED AND RE-ENTERED

**You can also add additional information about a subject by entering supplemental entries. You can add up to 99 AKAS’s, DOB’s, SSN’s etc.**

**If you enter supplemental information into a record and determine that the information is incorrect you cannot modify that supplemental entry. So, you would have to cancel out the supplemental (not the entire entry, just the supplemental portion) and then re-enter it.**

**Slide 207**

**CLEAR OR CANCEL?**

**CLEAR ~ SUBJECT IS IN CUSTODY OR THE PROPERTY HAS BEEN RECOVERED**

**A clear is used when the record was good and is now located. So a warrant subject that is now in custody or a stolen vehicle that has been recovered.**

**CANCEL ~ THE RECORD IS INVALID OR HAS BEEN QUASHED BY THE COURT**

**A cancel is done when it is determined that a warrant is quashed or expired and is no longer any good. Or if a vehicle was entered as stolen but it is found that it never really was stolen, for example, a victim from a mall reports their vehicle stolen and it gets entered and then after the mall closes you discover the car parked on the opposite side of the mall from where the driver thought they had left it. That would be cancelled.**

**Slide 208**

**LINKED BY ORI & OCA
OR LKI &LKA**

**In Level 1 we talked about how you can do a related search hit to see any cases that are entered with either the same ORI and OCA (within an agency) or by entering a case that is linked between two different agencies by filling in the LKI and LKA Field with the other agencies ORI (LKI Field) and OCA (LKA Field). This example shows you those fields and how the entry would work.**

**Perhaps you are entering a stolen vehicle and find out that your suspect has an Violent Person record out of another agency. You can now link the two entries together.**

**Slide 209**

**WANTED PERSON ENTRY**

**AMOUNT OF BAIL**

**If you have multiple warrants on one person, you can only enter one into the system.**

**Which one are you going to enter? What bail amount are you going to enter into the AOB (amount of bail) field? You should always enter the warrant with the furthest extradition. Normally that is the one with the most bail but not always.**

**For the bail amount, you would only enter the amount on the warrant that you are entering. Information about the additional warrants can be placed in the MIS field. You do not want to add the bail amounts together (this is something some agencies have done in the past and should not be doing any longer).**

**EXTRADITION LIMITATION (EXL) field**

**When you are entering a wanted person always make sure that your extradition limitations are entered. If there is limited extradition you need to list the limitation in the MIS field.**

**TYPES OF EXL CODES**

**Extradition is the surrender by one state to another of an individual charged with or convicted of an offense outside its own territory and within territorial jurisdiction of the other. Before entering a record of a wanted person into WACIC/NCIC, the entering agency must attempt to determine, if the extradition will be authorized if/when the individual is found.**

**There are six extradition field codes you will find in the EXL Field. On Felonies the codes are 1-6 on Misdemeanors they are A-F. Although the codes are different the extradition limitations are the same.**

FULL EXTRADITION

**Must be used when an agency will go anywhere in the USA or US territories to extradite the wanted person.**

LIMITED EXTRADITION

**Must be used when an agency will extradite the wanted person from specific states. Additional data in the MIS field is required and must include approved NCIC state code abbreviations of each state the entering agency is willing to travel to extradite the wanted person.**

EXTRADITION – SURROUNDING STATES ONLY

**Must be used when an agency is only willing to extradite from surrounding states.**

**In Washington this would mean it would be extraditable from Oregon and Idaho (and Washington too of course)**

NO EXTRADITION

**Must be used when an agency is only willing to extradite within Washington State. Additional data in the MIS field must include extradition details to include specific county or city names an agency is willing to extradite from. If this code is used, extradition cannot occur outside of Washington State. Misdemeanor State warrants are listed as “D” No Extradition.**

PENDING EXTRADITION

**Must be used by the entering agency when extradition is taking place. Additional data in the MIS Field is required and must include details of the extradition. A phone number for the agency that is performing the extradition may be included.**

**Example: Portland Police Department is confirming a Seattle Police Department’s warrant. The Seattle Police Department has requested that Portland Police Department not locate the warrant as Seattle Police Department will modify the record. A wanted person record containing this type of extradition should not have a locate placed against it and must be cleared by the entering agency once the subject has been extradited.**

PENDING EXTRADITION DETERMINATION

**Must be used when forecast of extradition cannot be made at the time of entry. When extradition has been determined the EXL field must be modified immediately. The entering agency will receive a reminder notification every 15 days until the EXL field has been modified to include specific extradition information or the record is cleared.**

**Slide 210**

**WANTED PERSON DETAINER**

**WHEN A SUBJECT IS IN CUSTODY ON LOCAL CHARGES AT ONE AGENCY AND HAS A CONFIRMED WARRANT OUT OF ANOTHER AGENCY**

**A LOCATE IS PLACED ON THE OUTSTANDING WARRANT BY THE AGENCY THAT HAS THE SUBJECT IN CUSTODY**

**A DETAINER IS THEN PLACED ON THE LOCATED WARRANT BY THE AGENCY HOLDING THE OUTSTANDING WARRANT**

THIS MUST BE COMPLETED WITHIN 5 DAYS OF THE LOCATE

**The detainer file was created with large agencies like King County in mind. Many times a subject will be arrested and taken to jail on local charges but they have outstanding extraditable warrants out of other agencies. Many times after they serve their time they are released from the jail without the other agencies having the opportunity to come and take them into custody on their warrants. So what a detainer does is flag a located record and notifies the agency that holds a warrant on the subject that he will soon be released from jail.**

**Example: A person is brought into the Pierce County Jail on local charges and it is found that they also have a Puyallup Warrant. The jail calls and confirms the warrant with Puyallup and asks if they want the person when they have completed their time at the Pierce County Jail. Puyallup confirms the warrant and says yes, they want the individual. The Pierce County Jail will then locate the warrant and Puyallup will place a detainer on the located record. 5 days before the subject is released from jail, Puyallup will get a notification that the subject will be released. This gives them the opportunity to pick the subject up on their own warrant. Some agencies use the detainer file, some do not**

**Slide 211**

**DETAINER EXAMPLE**

**This is what a detainer looks like when you get a hit. As you can see it shows it as a located warrant but having a detainer. What would you do if you contacted someone, ran them, and this came up? You would want to call the originating agency to see if the warrant is still good. You would need to confirm it, just like you would a regular warrant hit. It could be that the subject was released and never served his time for the warrant or it could mean that the originating agency forgot to clear it out when they picked him/her up**

**Slide 212**

**PROTECTION ORDER**

**RECORD TYPE**

**When entering an order always make sure you enter the correct RTP (record type), this would be a RO, NCO, AHO etc. How can you be sure what type of order you are entering? What if it says No Contact/Anti Harassment Order? How do you know which one it is? One way would be to check the RCW on the order itself. All orders are issued by RCW and looking that RCW up should clarify what type of order you are looking at.**

**SERVICE**

**When you enter a record into the system, your agency is the only agency that can modify, supplement, clear or cancel that record or any part of it, with one exception, the Service Field in a Protection Order. The Service Field can be modified by any agency. Why would that be? Because sometimes one county enters the order into the system but it is actually served in another counties jurisdiction.**

**TYPE OF SERVICE**

**There is now a Type of Service (TOS) field. The option for this field is:**

Personally Served, Served by Publication and Served by Mail.

**PCO CODES**

**Remember that PCO codes are determined by the Judge. You need to enter whatever codes are indicated on the order. It is always recommended to put the PCO/07 in the base record so it is easier to find then it would be in the supplemental information.**

**BRADY**

**Brady is the federal restrictor and is determined by the entering agency reading the order and determining if it has met the four criteria, which we will talk about on the next slide.**

**Slide 213**

**BRADY RESTRICTION WHAT IS IT?**

**Brady is the federal firearms restriction. It is not determined by the judge like the state firearms restriction but by the four criteria set forth by the FBI. The entering agency must determine if all four criteria have been met in order to enter the Brady restrictor.**

**ALL FOUR CONDITIONS LISTED BELOW**

**MUST BE MET TO DETERMINE THE BRADY FLAG:**

* 1. RESPONDENT MUST HAVE BEEN SERVED AND HAD AN OPPORTUNITY TO ATTEND A COURT HEARING

**They may not have showed up for their hearing but they had the opportunity to do so.**

* 1. SUBJECT MUST BE AN INTIMATE PARTNER

**They must be spouses or ex-spouses, had co-habited at one time, or have a child in common. This can sometimes be hard to determine by the entering agency if the order is not marked correctly.**

* 1. ORDER MUST RESTRAIN FUTURE CONDUCT

**The order must say things like, cannot contact, cannot call, must not email. Words preventing them from future conduct.**

* 1. SUBJECT MUST BE LISTED AS A CREDIBLE THREAT OR PHYSICAL FORCE

**This means the order must restrict things like, assaulting, attacking, and molesting (anything physical).**

NOTE: BRADY AFFECTS NO CONTACT, PROTECTION, RESTRAINING AND VULNERABLE ADULT ORDERS

**Brady does not affect Sexual Assault Orders because a sexual assault is not a “wanted” intimate relationship. It also does not affect Anti-Harassment or Stalking Protection orders because harassment and stalking is not physical.
The wording in the RCW’s for these two types of orders does not meet the criteria for BRADY. All the other orders can be affected by BRADY.**

**Slide 214**

**MISSING PERSON**

**THE OFFICER REPORT DETERMINES THE TYPE OF MISSING PERSON**

**There are several types of Missing Persons (Juvenile, Physical Disability, Endangered, Involuntary (abducted), Catastrophe and other). The officer’s report will determine what type of missing person you are entering.**

**USE THE CODE “EMO” TO ENTER JUVENILE PERSONS BETWEEN THE AGES OF 18 TO 21**

**People between the ages of 18-21 who do not fit into any other category should be considered juveniles but placed in as “Other”. The system will not accept them as juveniles since they are above 18 but because of Adam Walsh Child Protection Safety Act and Suzannes Law they fall into the juvenile criteria for entry (no signed report needed) and must be entered within 2 hours.**

**REMEMBER THE CODES “AA” FOR AMBER ALERT AND “CA” FOR CHILD ABDUCTION**

**When entering a missing child remember to enter the circumstances, when they exist, (CA for Child Abduction and AA for Amber Alert). When you enter these alerts a notification is sent to NCMEC (National Center for Missing and Exploited Children) and CASKU (Child Abduction and Serial Killer Unit).**

**Always remember with missing person to enter jewelry, clothing, back packs etc. into the correct field. The MIS field is all free text and NOT searchable. So if a child was to go missing with a yellow backpack and someone found the backpack and used it as their search criteria, it would not pick up on the hit because the backpack was placed in the MIS Field.**

**Once again always refer to manuals for assistance.**

**Slide 215**

**UNIDENTIFIED PERSON**

**REMAINS IN THE SYSTEM UNTIL IDENTIFIED**

**If a match is made on a body part, the part will be removed for the Unidentified Persons File, although it would probably remain in the missing persons file until all parts were found.**

**IS THERE DNA AVAILABLE? WHERE?**

**If there is DNA you can indicate that in the entry. Once you indicate that there is DNA you are then required to enter the location of the DNA. This is so any possible matches can be researched.**

**A STATUS MUST BE LISTED FOR ALL BODY PART SEGMENTS (BPS)**

**If you have just one body part that is found, you must list the status of all other parts also.**

**Slide 216**

**VIOLENT PERSON
UNDERUTILIZED
Even if you are sitting here today and know of an incident where the suspect was not placed in this file, please go back and research it. If it fits the criteria, get them entered.
With all that has happened over the past couple of years, we really need to utilize this file and make sure not just our agencies know about these threats, but every agency in the country has the information.
FOUR CRITERIA**

1. ASSAULT ON LAW ENFORCEMENT
2. VIOLENT CRIME HOMICIDE/ATTEMPTED HOMICIDE
3. VIOLENT CRIME WITH A WEAPON
4. THREAT TO LAW ENFORCEMENT

**This criteria is so much broader now that many other individuals should be placed in here including people who have been convicted of resisting and fleeing.**

**MISCELLANEOUS (MIS) FIELD
Make sure the type of threat that occurred is listed in the MIS field. This way when an agency receives an Officer Safety hit, they will know more about the person they are contacting. For instance, did they use a weapon, did they threaten to use a gun or knife. Spell it out!
RETENTION
Once a person is entered into this file, they will remain in the file until the entering agency removes them.**

**Slide 217**

**IDENTITY THEFT**

**WHY IS THE CONSENT WAIVER IMPORTANT?**

**The victim must sign a consent waiver giving you permission to enter all their information into the system. If your agency does not have a consent waiver, you can find one on the ACCESS webpage. This will prevent a person from coming to your office a month after filing their report and asking you why all their information is in a government run database.**

**WHERE DOES THE PASSWORD COME FROM?**

**When the victim picks a password to use, you may want to point out that if they use a child’s or pets name which is easy for them to remember, it might also be easy for a family member to remember. (If they are the ones that are committing the fraud many times it is a sibling that is the suspect).**

**Also remember that information like the SID and WAC of a suspect can be entered in if known.**

**Slide 218**

**FELONY FIREARMS OFFENDER REGISTRY (FFOR)**

**MUST REGISTER WITH COUNTY WITHIN 48 HOURS OF RELEASE**

**If an individual is court ordered to register for the Felony Firearms Offender Registry, they must do so within 48 hours of release with the County.**

**RETAINED FOUR YEARS**

**The records in this file are retrained for four years.**

**FILE NEEDS TO BE CREATED IN WACIC**

SUBMIT WSP FORM

**Until the WACIC File is created, agencies must submit current registrants by using the form located on the ACCESS webpage.**

**FINGERPRINTS/PHOTOGRAPH OPTIONAL**

BLUE CIVIL APPLICANT CARD

**If an agency chooses to submit fingerprints and photographs in addition to the form, submit fingerprints by using a blue civil applicant fingerprint card.**

**Until the file is created the form, fingerprints and photographs must be mailed to:**

**MAIL TO**

ATTENTION ACCESS SECTION

CRIMINAL RECORDS DIVISION

WASHINGTON STATE PATROL

PO BOX 42619

OLYMPIA WA 98504-2619

**Slide 219**

**CAUTION AND MEDICAL CONDITIONS (CMC) FIELD**

**How would you determine if a caution or medical condition exists?**

**It could be on officer reports. Maybe you have a regional system and can look up previous events and can see that the last couple of times you contacted this person they had a heart problem. Use your resources. Do not go by the victim statement alone. Most of the time the victim is upset or angry and they may say things that are not necessarily true.**

**THE CAUTION INDICATOR “C” CAN BE ENTERED AS THE FOURTH CHARACTER OF ANY MESSAGE KEY (MKE) TO INDICATE A CAUTION**

**To enter a caution you would enter a “C” as the fourth character in the MKE field. This would enable the word \*\*\* Caution\*\*\* on the top of your hit. Example: to enter a Misdemeanor Warrant the MKE would be EWW. To enter a caution you would enter EWWC.**

**THE CMC FIELD MUST BE USED WHEN A CAUTION IS USED IN THE MESSAGE KEY**

**You would then fill in the CMC field with one of the 17 warnings that are listed in the NCIC Code manual.**

**Slide 220**

**LAW ENFORCEMENT OFFICERS FLYING ARMED (LEOFA)**

**TO FLY ARMED A LEO MUST:**

**BE A LAW ENFORCEMENT OFFICER EMPLOYED BY A GOVERNMENT AGENCY, SWORN AND COMMISSIONED**

**BE AUTHORIZED BY THEIR EMPLOYER TO HAVE THE WEAPON IN CONNECTION WITH ASSIGNED DUTIES**

**COMPLETE THE TRAINING PROGRAM “LAW ENFORCEMENT OFFICERS FLYING ARMED”**

**MUST HAVE AN OPERATIONAL NEED AND BE ON DUTY FROM CHECK-IN TO DEPLANNING**

**There are only specific reasons why a person is permitted to fly armed. There are still agencies out there flying armed for inappropriate reasons like training etc. Please be certain that your agency understands and follows the below criteria.**

CONDUCTING A HAZARDOUS SURVEILLANCE OPERATION

TRANSPORTING AN EXTRADITABLE SUBJECT

TRANSPORTING STATES EVIDENCE

EMPLOYED AS A FEDERAL LEO

**CONTACT THE OFFICE OF THE LAW ENFORCEMENT/FEDERAL AIR MARSHAL SERVICE LAISON DIVISION, FOR TIME SENSITIVE REQUESTS**

CALL 1-703-487-3100 OR EMAIL LEOFA@DHS.GOV

**Slide 221**

**LEOFA CONT**

**MESSAGE MUST BE SUBMITTED PRIOR TO TRAVEL**

**A RETURN MESSAGE WILL BE RECEIVED FROM NLETS**

**An NLETS message must be submitted prior to travel for all legs of the trip. Once the NLETS message is received, a return NLETS message will be sent to the employing agency with a unique identifier for verification at the airport on the date of travel.**

**This is an example of the return message from NLETS to include the Unique Identifier.**

**Slide 222**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*VIDEO \*\*\*\*\*\*\*\*\*\* (MUST CLICK ON VIDEO TO START)**

**Slide 223**

**ADDITIONAL ENTRY FILES AND INFORMATION**

**VEHICLE**

FELONY VEHICLES MUST HAVE THE TYPE OF FELONY IN THE MIS FIELD

**It’s important to fill in the MIS Field with as much about the crime and vehicle as possible. What type of weapons? Are there any additional descriptors? Anything that will help in the search and apprehension.**

**ARTICLE**

OAN

**Any type of article can be placed in the system as long as you have a serial number or an OAN to identify the item. Articles that are under $750 will only be entered into WACIC, anything over that amount will also go into NCIC.**

**GUN**

ALL CODES CAN BE FOUND IN THE MANUALS

RELY ON THE EXPERTS

**The NCIC Code manual for guns is very extensive. It is very important to assure that the proper gun and identifiers is placed in the system. If you are entering a gun and don’t feel you have all the information you need about a firearm (is it an automatic, semiautomatic, etc.), it may be a good idea to contact someone within your agency, like maybe an evidence person to assist you.**

**PART**

VEHICLE/BOAT/CONSTRUCTION/FARM

**Remember parts are anything taken from a vehicle or boat that cannot move themselves. Seats from a car, or a car hood or bumper, side car from a motorcycle, or a motor from a boat.**

**How about air bags? It’s expensive to replace an airbag, unless you can find someone with a stolen airbag and the knowledge to install it.**

**Slide 224**

**ADDITIONAL ENTRY FILES AND INFORMATION CONT**

IMAGE

ENTER BY WAC OR NIC – NOT BOTH

**Images are entered by using the base records WAC or NIC number. That is how it gets associated with the base entry. If you enter the image by both the WAC and NIC number it will place two identical images in the file.**

NUMBER OF IMAGES?

**You can enter up to 10 identifying images, like tattoos. You can also add an additional mug shot or signature. So a person’s entry can have up to 12 images associated with it. A vehicle, article or part can only have one image associated with the base record.**

**BOAT FILE**

NCIC ONLY

**Remember that a boat can only be entered into NCIC and if a boat motor is stolen that can be entered into the parts file also.**

**SECURITIES**

TYPES

**What types of securities can’t be entered into this file?**

 **Checks, Credit Cards and Coins**

**NSOR**

TRIBAL ENTRIES

**Entries into NSOR are made when agencies send the information to WSP SOR unit to be entered.**

**Due to the need for the entry of Tribal Sex Offenders and the fact that they cannot be entered by the state, a mask has been created so that Tribal Agencies can enter their sex offenders into the registry. The system will only accept entries made by tribal ORI’s. Also the Tribes are now able to create tribal warrants under the Person of Interest file.**

**Trainers, if you have tribal students who want more information on this, please have them contact ACCESS.**

**Slide 225**

**RECOMMENDATIONS AND REQUIREMENTS**

**RECOMMENDED**

PACKING THE RECORD

CRIMINAL HISTORY CHECKS

LOCAL FILES

DOL/DOC/WACIC/NCIC

COURT PROGRAMS (JIS)

PACKING BY SID

**Who here packs their records? For those of you who do not know what this is, it is a method where an entering agency checks every available database it has available to them in order to get the most current and up to date descriptor information on a subject and then puts all that information into the entry. You can check DOL, FORS, Criminal history. We do not require that you do this because it does take manpower hours but it is highly recommended for officer safety and public safety.**

**You also have the capability of packing by SID. This means that you can put a SID number in your entry and the system will take the identifying information from the person’s criminal history and pack the record for you. When packing by SID you must assure you are using the correct SID number. Also remember that a person’s criminal history may be several years old. If there last charge was 5 years ago, they could have accumulated more tattoos and even more names. When you pack, you want to make sure that you always use current information also.**

**REQUIRED**

2ND PARTY CHECKS

BE SURE TO DOCUMENT

**Any entry that is made into the system must be double checked by someone other than the person who entered it. This is called a 2nd party check. This check must be documented. The person doing the check must initial and date the entry to indicate that it was checked. Auditors can tell when 2nd party checks are not done by the amount of error they find in an agency’s records.**

TIMELY ENTRY

REFER TO MANUALS

**All entries must be made in a timely manner.**

**We have already talked about the 2 hour entry on missing juveniles and entering missing persons as soon as possible. What about warrants and protection orders? Warrants and protection orders must be entered within 72 hours. Sometimes agencies don’t even receive the paperwork from the court for more than 72 hours, so what can you do? You should date stamp or date and initial warrants and protection orders when you receive them and the auditors will count from that date and not the date the document was issued. Your agency name should be on the date stamp.**

**Slide 226**

**VALIDATIONS**

**AGENCIES RECEIVE A SAMPLING OF THEIR HOT FILE RECORDS EACH MONTH**

**TACS OR DESIGNEES VERIFY INFORMATION WITH REPORTING PARTIES, WITNESSES AND COMPLAINANTS**

**WARRANT AND PROTECTION ORDERS ARE VERIFIED THROUGH THE COURT, PROSECUTOR OR JIS**

**ANY ERROR SHOULD BE IMMEDIATELY CORRECTED**

**A LEGAL DOCUMENT/VALIDATION FORM IS SIGNED AND RETURNED TO ACCESS**

**THE TAC OR DESIGNEE SHOULD THEN DELETE THE COMPLETED VALIDATIONS**

**Who does validation? How do you do them? How do you validate Warrants and Protection orders?**

**Each agency receives a sampling of the hot files every month. The TAC goes out to the Fortress website and gets the list of their validations. Agencies normally will send letters to reporting parties or victims to verify that the information on the entry is still correct and the item is still stolen or person still missing. Sometimes agencies call instead of writing.**

**Warrants and Protection orders are sent back to the court for validation or the entering agency can check in JIS (Judicial Information System) to confirm that the record is still valid and should remain in the system.**

**Validations are documented by listing who was contacted, how the contact was made, what the outcome was, if changes were made, and who did the validations and when.**

**The TAC signs a legal document and sends it back to ACCESS stating that their validations for the month have been completed.**

**Then the agency goes back out to the fortress website and deletes their completed validation list.**

**Slide 227**

**TRIENNIAL ACCESS AUDITS**

**THE WSP CONDUCTS AN AUDIT OF EVERY CRIMINAL JUSTICE AGENCY THAT HAS A TERMINAL**

**This is an onsite audit. The TAC receives notification about 2 months before the audit. The letter they receive outlines the process and what types of records will be checked.**

**WSP AND MULTIPLE AGENCIES THROUGHOUT THE STATE ARE AUDITED BY THE FBI**

EVERY 3 YEARS

RESULTS REFLECT ON THE STATE AS A WHOLE

**The audits are a learning experience for both the agency being audited and ACCESS. The auditors clarify areas where more training is needed. They bring agency issues to the forefront and show us areas where we need to improve.**

**AUDITS VERIFY COMPLIANCE WITH GUIDELINES SET BY THE FBI**

**THE GOAL IS COMPLIANCE**

**Agencies are given a time frame in which they need to come into compliance. ACCESS assists in whatever way they can to assure that each agency is given the tools and information to fix the compliance issues**

**Slide 228**

**AUDITORS REVIEW**

**1% OF PERSONS RECORDS**

WANTED, MISSING AND PROTECTION ORDER

ACCURACY AND COMPLETENESS

TIMELY ENTRY AND REMOVAL

DOCUMENTED 2ND PARTY CHECKS

DOCUMENTED VALIDATIONS

**The auditors physically check the entries to assure that they are accurate and complete. They check the documentation for 2nd party checks and they check 3 months of validations.**

**1 MONTH OF CRIMINAL HISTORY INQUIRIES**

**Auditors look at criminal history logs to assure that agencies are filling in the Attention Field properly and using the correct purpose codes. Criminal History is where the auditors find most of the compliance issues at an agency.**

**SYSTEM SECURITY**

**Are the terminals secure from any non criminal justice personnel?**

**PERSONNEL SECURITY**

FINGERPRINTING AND RE-BACKGROUNDING

**We must all be fingerprinted within 30 days of being employed at our agency and have a SID number assigned. The TAC must also re-background (running criminal history) on all ACCESS users every 5 years.**

TRAINING/CERTIFICATION

**There are different type of training that we are all required to attend. Auditors will check certification lists, logs, etc. to assure that everyone has taken the appropriate training. Trainers, Go over the different types of training that is required to be completed (listed below)**

ACCESS,

**Users can use ACCESS for 6 months prior to attending an ACCESS class. This gives the user a little bit of hands on before they actually go through the training. We must re-certify every 2 years. Re-certification can be done on line. If our certification expires or we fail the recertification test, we will be required to come back to an ACCESS class. We are prohibited from using the ACCESS system if our certification expires or if we fail our recertification test.**

TAC

**TAC’s are required to also attend TAC training every 3 years within an audit cycle. This is an 8 hour class and covers the entire audit process from A-Z**

SECURITY AWARENESS

**Employees who have unexcorted ACCESS to CJI and are not ACCESS certified must view the online Basic Security Awareness and sign the signature log. This includes IT personnel.** UPPERMANAGEMENT AND ADMINISTRATORS OVERVIEW TRAINING

**Supervisors and administrators who manage ACCESS users but are not certified themselves are required to view the Upper Management and Administrators Overview Training, sign a signature log and that log needs to be available during the audit process.**

**WRITTEN PROCEDURES**

**Auditors also check written procedures. If an agency does not have written procedures, there are some templates on the ACCESS website for your use. Remember that these are only templates and must be tweaked to indicate the agencies actual procedure**

**Trainers, please go over the different types of written procedures that are looked at during the audit.**

CRIMINAL HISTORY

**Criminal History Procedures should explain exactly what the agency uses criminal history for, the process for making those inquires (like purpose codes, reasons etc.) and what the consequences for misuse will be. This could range from a verbal warning all the way to criminal charges and termination.**

DISPOSAL OF MEDIA

**How does your agency dispose of printed information, electronic information (like cd’s and thumb drives), laptops, computers, copy machines (all the things that could house or have printed CJI information on them.**

MEDIA PROTECTION

**How does your agency protect your computers, laptops, printed information? Are your secured areas really secured? Does anyone have keys or unescorted access afterhours. Are your case files in locked cabinets? If you have an MDC do you secure it when you are not in your vehicle.**

MISUSE

**You must have a procedure in place for what takes place when an accusation of misuse or a misuse situation has been identified. What is misuse and what will occur if you misuse the system. The sanctions could range from a written reprimand to termination.**

PHYSICAL PROTECTION

**Are your terminals and CJI records in a secure building or office? Who has keys? Maybe a Mayor or City Council member can get in after hours. If someone can get in your office unescorted they must be fingerprinted.**

VALIDATIONS

**This procedure should list the steps your agency takes to validate different kinds of records. It should talk about going to the Fortress website, using your ID and password, pulling off your validation for the month, and then the process you use to validate those records. Do you send letters, or emails? How do you contact the reporting parties? Do you contact the courts or do you check JIS to validate Warrants and Protection Orders. And how do you document those validations.**

**Slide 229**

**TRIENNIAL TECHNICAL SECURITY AUDIT**

**A TECHNICAL SECURITY AUDIT IS ALSO CONDUCTED EVERY THREE YEARS**

**The security audit is done by correspondence and a phone call contact to cover the questionnaire. It is done during the same cycle as the ACCESS audit but is a separate audit. Normally the technical audit will be sent to the technical point of contact at an agency, unless ACCESS does not have that information. If you are a TAC and you receive this audit but know nothing about the Technical procedures at your agency, let ACCESS know who your IT person is and they will conduct the audit through that person.**

**AUDIT TOPICS**

VERIFICATION OF IT TRAINING AND BACKGROUNDING

PHYSICAL AND INFORMATIONAL SECURITY

PASSWORD/AUTHENTICATION

WIRELESS/INTERNET ACCESS

NETWORK SECURITY

ENCRYPTION

WRITTEN PROCEDURES

**All the topics above are covered during the technical audit. The information requested will need to be sent back to the ACCESS ISO (Information Security Officer). Once again, just like the ACCESS audit, compliance is the goal.**

**SLIDES 230 – 234 TEST QUESTIONS 21-25**

**Slide 235**

**LEVEL 2**

**TEST QUESTIONS REVIEW**

**SLIDES 236 – 240 LEVEL 2 TEST QUESTIONS REVIEW**

**Slide 241**

**LEVEL 2 CERTIFICATION COMPLETE**