TRAIN THE TRAINER

HELPFUL TIPS & TRICKS FROM ONE TAC TO ANOTHER

Introduction

ALLI LACHOWSKY
CRIME ANALYST
SOUTH SALT LAKE POLICE DEPARTMENT
18¼ YEARS

NOT AN EXPERT – ENTHUSIASTICALLY INVESTED IN MAINTAINING SANITY

TAC & Alt TAC Coordination

- SHARE THE RESPONSIBILITY!
- INCLUDE EACH OTHER IN ALL TAC RELATED COMMUNICATIONS
- KEEP DOCUMENTATION IN A SHARED LOCATION
- KEEP TRAINING MATERIALS IN A SHARED LOCATION
- USE GOOGLE DRIVE (OR SIMILAR) TO SHARE ELECTRONIC DOCUMENTS (NO SENSITIVE/CJI INFORMATION)
- USE ANY COMPLIANCE ISSUES FOUND DURING INTERNAL AUDITS AS TRAINING OPPORTUNITIES

Starting the Process – New Users & Non Users

- ASK TO BE LOOPED IN ON THE HIRING PROCESS, SO YOU KNOW WHEN SOMEONE NEW WILL BE STARTING
- ASK TO BE LOOPED IN ON VOLUNTEER OR INTERN PROCESSES
- START SCHEDULING TRAINING AND FINGERPRINTING AS SOON AS A START DATE HAS BEEN SET
- IF THEY ARE COMING FROM ANOTHER LAW ENFORCEMENT AGENCY, ADD THEM IN UCJIS EARLY TO CAPTURE THEIR PRINTS ON FILE

Training New Users & Non Users – When to Train

- USE THE 6 MONTH DEADLINE AS A TESTING DEADLINE ONLY. TRAIN BEFORE FIRST DAY (IF POSSIBLE).
- IF YOU CAN'T DO TRAINING BEFORE, SCHEDULE FOR FIRST THING ON DAY ONE.
- SET USERS UP FOR SUCCESS BY GIVING THEM THE TOOLS EARLY.

Training New Users & Non Users – What to Train

- LEAN TOWARDS OVER TRAINING
- INCLUDE SECURITY AWARENESS TRAINING BASED ON CJIS SECURITY POLICY
- PRIVACY, DISSEMINATION AND SECURITY OF CJIS INFORMATION
- USE OF UCJIS TRANSACTIONS AND INFORMATION
- HOW/WHERE TO ACCESS MANUALS
- TEST RECORDS AVAILABLE FOR PRACTICE
- MISUSE AND CONSEQUENCES

CJIS SECURITY AWARENESS TRAINING

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

What Every User Must Know

STATE OF UTAH
BUREAU OF CRIMINAL IDENTIFICATION

5.6 What every User must know

Dissemination

- Never discuss information received from any UCJIS file with someone outside of the criminal justice industry
- Even if someone does not have a criminal history and that information is passed to someone outside of the criminal justice industry, that is dissemination and should not be done.

Privacy

- Never, never look up a person in any file in UCJIS for curiosity sake (family, neighbors, ex-family, soon-to-be-family, fellow employees, people you are mad at, people you want to irritate, etc.)
- Never discuss the information you see or print from UCJIS outside of your agency.
- If you misuse the information found in UCJIS, you could be charged with a Class B Misdemeanor.
- If you have visitors at your desk, cover up all information printed from UCJIS and lock your monitor.

Security

- Lock your keyboard (the window key and "L", or Ctrl Alt Del) when you leave your desk.
- Never share User ID information or tell anyone your user ID information and password.
- Retainable fingerprints are checked daily through the FBI Rap Back process for new arrests
- If you print anything out of UCJIS, destroy (shred or burn) the document when you are finished.

Manuals

- Manuals are located on the TAC website, click on MANUALS.
- Open up the manual you need, hit Ctrl F and a search window will appear, type in the word or phrase you are looking for.
- The Operation Manuals tell you how to enter information and what the field acronyms mean.
- The NCIC Code Manuals gives you the codes to enter into the specific fields.
- The NCIC TOUs (Tech. Operations Updates) have updated information on codes and fields for NCIC Entry. The TOUs are located on the TAC home page under MANUALS.

NCIC Entries

- Entries must be **accurate, timely, and complete.**
- "**Pack**" the entry with all available information - case files, every file in UCJIS you have access to.

Courts

- Entering Jail Release Agreement and Protective Order information timely and accurately is crucial.
- When the Judge makes a decision on a case, enter it into CORIS/UCJIS as soon as possible.
- If the Court does not expire JRA and POs timely, the court may be held liable.
- "**Pack**" a warrant with all available information – case files, every file in UCJIS you have access to.

Who to call first

- Your TAC/Alt TAC is the first person you call if you have a problem or need your password reset.
- If your TAC/Alt TAC is not available, call the BCI CIC Help desk: 801-965-4446
- You can also call your agency's BCI Field Services Rep. Click on "BCI Regions" on the TAC website home page to find the name and phone number of your Rep.

Miscellaneous

- Passwords expire 90 days from the last time it was set up. If you are on vacation when your password expires, change your password before you leave, type CPW in the transaction code field in UCJIS.

Training Existing Users – Sworn Officers

- DON'T WAIT FOR TWO YEARS – TRAIN CONTINUALLY
- BCI NEWSLETTER INFORMATION
- INFORMATION FROM TAC CONFERENCE
- IF TEST QUESTIONS ARE ANSWERED INCORRECTLY, FOLLOW UP WITH SPECIFIC TRAINING
- HAVE EVERYONE SIGN A TRAINING ROSTER FOR ALL TRAINING

Training Existing Users – Records Staff

- DON'T WAIT FOR TWO YEARS – TRAIN CONTINUALLY
- BCI NEWSLETTER INFORMATION
- RECURRING MORNING TRAINING WITH ROTATING TOPICS – USE BCI PRESENTATIONS
- AS QUESTIONS ARISE, USE AS TRAINING OPPORTUNITY
- IF TEST QUESTIONS ARE ANSWERED INCORRECTLY, FOLLOW UP WITH SPECIFIC TRAINING

Avenues for Training

- TRAINING VIDEOS OR PROGRAMS
- SHIFT BRIEFINGS
- TRAIN SERGEANTS IN STAFF MEETING TO TAKE BACK TO BRIEFINGS
- IN-SERVICE TRAINING
- EMAIL
- BULLETIN
- CREATE A SECURITY TRAINING OUTLINE AND SEND TO ALL USERS/NON USERS AFTER TRAINING

Training Records & Documentation

- SPREADSHEET SHOWING TRAINING DATE, WHICH SECURITY LEVEL (CJIS POLICY), WHO TRAINED
- TRAINING ROSTERS
- SAVE TRAINING MATERIALS SOMEWHERE ACCESSIBLE BY ALL DEPARTMENT EMPLOYEES (SHARED NETWORK DRIVE)

Testing New Users

- REGULARLY REVIEW TAC REPORT FOR UPCOMING TESTING DEADLINES
- DO A REFRESHER TRAINING RIGHT BEFORE TESTING
- USE INCORRECTLY ANSWERED TEST QUESTIONS TO PROVIDE FOLLOW UP TRAINING – SHOWS POTENTIAL DEFICIENCIES IN INITIAL TRAINING

Biennial User Testing

- TEST ALL USERS AT THE SAME TIME TO KEEP A CONSISTENT SCHEDULE
- CIRCLE BACK ON INCORRECTLY ANSWERED QUESTIONS TO MAKE SURE THE CORRECT ANSWER IS UNDERSTOOD (NOT JUST KNOWN)
- KEEP AN ONGOING LIST OF QUESTIONS BETWEEN TESTS

Sources for Test Questions

- BCI NEWSLETTERS
- PRIOR TAC TESTS
- BCI MANUALS
- AUDITS AND AUDIT FINDINGS
- MOST OFTEN MISSED QUESTIONS FROM PREVIOUS TESTS
- USE THE TESTING AGREEMENT AS A CHECKLIST TO MAKE SURE TEST COVERS ALL TOPICS

Methods of Testing

- HARD COPY TEST – DISTRIBUTE TO SERGEANTS FOR COMPLETION IN BRIEFINGS
- GOOGLE FORMS – COMPLETED ELECTRONICALLY AND AUTO CORRECTED
- COMMERCIAL TRAINING AND TESTING PLATFORM

Strategies for Improving Your Performance as a TAC

- NEW TAC WELCOME PACKET IN THE MANUAL – NOT JUST FOR NEW TACS!
- DO SELF-EVALUATIONS REGULARLY – WHERE DO I STRUGGLE?
- ESTABLISH A GOOD RELATIONSHIP WITH YOUR IT DEPARTMENT, AND COMMUNICATE OFTEN
- MEET WITH YOUR FELLOW TACS – IN YOUR OWN DEPARTMENT & BEYOND

QUESTIONS?

CONTACT INFO:

ALLI LACHOWSKY
ALACHOWSKY@SSLC.COM
801-412-3607