

## **TIME Agency Coordinator (TAC) Responsibilities**

It shall be the responsibility of each local agency to designate a TAC. The TAC will act as the primary liaison between their agency and the Crime Information Bureau (CIB), regularly communicating with CIB, participating in sponsored meetings, and providing feedback and recommendations for system improvement. The TAC is normally TIME System certified. The TAC will ensure that all physical, personnel, computer and communications safeguards, and security are functioning properly and are in compliance with the Departme Of Justice (DOJ), Crime Information Bureau (CIB), National Crime Information Center (NCIC), and International Justice and Public Safety Information Sharing Network, (Nlets) rules and regulations to include:

- 1) Ensure within six months of employment or assignment that all personnel accessing TIME/NCIC have completed the required TIME System training. This includes eTIME, MDT/MDC, Basic & Advanced certifications and Security Awareness Training for IT staff that configure and maintain systems and networks with access to the TIME System and those with unescorted access to the secure location.
- 2) Ensure that each new employee reviews the TIME System New Operator Handout and demonstrates TIME System terminal operation.
- 3) Ensure thorough background screening by the employing agency of personnel is required. State and national criminal history checks by fingerprint identification must be conducted within 30 days upon initial employment or assignment for all personnel who have authorized access to the TIME System and those who have direct responsibility to configure and maintain computer systems and networks with direct access to the TIME System and those with unescorted access to the secure location. The minimum check must include submission of completed applicant fingerprint cards to the FBI CJIS Division and the CIB through the state identification bureau. CIB and NCIC Wanted Person Files must also be checked. Sworn personnel who have been fingerprinted and certified by the Law Enforcement Standards Board already meet this requirement. Background re-investigations are recommended every 5 years as good business practice.
- 4) Ensure that TIME System Advanced Project results are reviewed with the employee when returned to the department.
- 5) Ensure all certified operators and those needing security awareness training have successfully passed the TIME System biennial written/computer based re-certification examination.
- 6) Ensure that all certified operators are provided biennial Inservice training.
- 7) Ensure agency complies with all applicable CJIS Security Policies.
- 8) Ensure their computer site and/or terminal areas have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment, display or to any criminal justice data.

- 9) Ensure all visitors to computer centers and/or terminal areas are accompanied by staff personnel at all times. Visitor access records must be maintained and reviewed for accuracy and completeness.
- 10) Ensure that all individuals who store, process and/or transmit information on the TIME System are uniquely identified. The unique identification can be in the form of a name, badge number, serial number or other unique alphanumeric identifier.
- 11) Ensure all computer terminals are updated with the most current version of TIME System software.
- 12) Ensure that the Portal 100 Authorization Form is properly completed, updated and forwarded to the Crime Information Bureau for personnel who will use the Portal 100 Software.
- 13) Provide instructional material for the functional use of the local equipment and formats to be used for TIME System applications.
- 14) Ensure TIME System Newsletters and related correspondences are disseminated and available to the appropriate personnel. This includes briefing administrative staff whenever appropriate.
- 15) Maintain records of all TIME System training, testing and proficiency affirmation.
- 16) Ensure that the Crime Information Bureau is notified in a timely manner when an individual's TIME System access should be deactivated. (Including, but not limited, to duty changes that no longer require TIME System access and those who are no longer employed by your agency.)
- 17) Ensure signed user agreements are on file with non-terminal users that the agency provides with TIME service/information.
- 18) Ensure Management Control Agreements are signed when appropriate.
- 19) Ensure all monthly validations are completed on time & exception report records are handled per instructions.
- 20) Ensure the department has written policies and procedures in place as required by standards set by CIB and CJIS including, but not limited to disciplinary action for misuse of the TIME System and criminal justice information. Ensure policies and procedures are updated when necessary.
- 21) The TAC should understand the record system and communications capabilities of their agency.
- 22) Ensure that the CIB is advised of any change in the status of the TAC due to reassignment, promotions, etc.
- 23) The TAC is responsible for assisting the CIB and NCIC personnel throughout the agency during audits or other official visits.
- 24) Ensure compliance with the criminal history record inquiry requirements of CIB/NCIC, to include creation of a secondary dissemination log, identifying the requesting individual, proper use of purpose codes and justification for each inquiry.