Physically Secure Location Checklist for TAP Biometrics Workstation

Agencies must ensure the following provisions are met in order to meet the requirements of a physically secure location as defined by the CJIS Security Policy, Section 5.9.1:

"A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof."

- ☐ The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls
- ☐ The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.
- ☐ The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.
- ☐ The agency shall control physical access to information system distribution and transmission lines within the physically secure location.
- ☐ The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.
- ☐ The agency shall monitor physical access to the information system to detect and respond to physical security incidents.
- ☐ The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.
- ☐ The agency shall authorize and control information system-related items entering and exiting the physically secure location.

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

- ☐ Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
- ☐ Lock the area, room, or storage container when unattended.
- ☐ Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
- ☐ Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e., data "at rest") of CJI.