

Management Control Agreements

A Management Control Agreement (MCA) should be put in place when you have a Criminal Justice Agency (CJA) receiving services from a Non-Criminal Justice Agency (NCJA) that is a government entity, such as a county or city IT department. This applies to entities who have access to unencrypted Criminal Justice Information (CJI) including physical or logical access to devices that store, process or transmit unencrypted CJI. As with any legal documents both parties should consult legal counsel before implementing.

The purpose of this document is to establish and enforce Security Control of the access and use of the CJI, Law Enforcement Automated Data System (LEADS) and associated Ohio Department of Public Safety (ODPS), FBI and other systems in a location where access to and/or use of that system is accomplished by a CJA with the assistance of a NCJA. This document places Security Control of that access under the authority of the CJA.

Therefore, the following are needed when dealing with a governmental NCJA:

- MCA: is an agreement with respect to the administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (e.g. - LEADS) for the interstate exchange of criminal history/CJI, the CJA shall have the authority, via managed control, to set and enforce:
 - 1) Priorities.
 - 2) Standards for the selection, supervision, and termination of personnel.
 - 3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
 - 4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
 - 5) Compliance with all rules and regulations of the CJA Policies and CJIS Security Policy in the operation of all information received.
- Background Check: To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days.
- Security Awareness Training: Basic security awareness training shall be required within six months of initial assignment and biennially thereafter.

Responsibility for management control of the criminal justice function shall remain solely with the criminal justice agency.

The following are requirements for a CJA receiving services from a NCJA that is a non-government entity, such as a contractor or vendor. This applies to individuals who have access to unencrypted CJJ including physical or logical access to devices that store, process or transmit unencrypted CJJ.

- **Background Check:** To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days.
- **Security Training:** Basic security awareness training shall be required within six months of initial assignment and biennially thereafter.
- **FBI CJIS Security Addendum:** This document is a “uniform” addendum to an agreement between a government entity and a private contractor or vendor. The certification page is an acknowledgement, by the contractor/vendor (NCJA) and its individual employees that they have read and understand the requirements contained within FBI CJIS Security Policy. The addendum states that private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the Criminal Justice Information Services (CJIS) Security Addendum (SA) Certification page, and abide by all aspects of the CJIS Security Addendum.

PLEASE NOTE: The FBI CJIS SA is a “uniform” addendum approved by the Attorney General of the United States and needs to be part of any contract a CJA may have with a vendor where they may have access to CJIS data.

It is important that the SA be included in its entirety and not modified in any way. If the SA is not included as part of the contract or is modified, it’s not considered “uniform” and therefore, not compliant with the requirements of the CJIS Security Policy.

Some vendors (or their lawyers) will try and send back the SA with all sorts of red-lines, additions and/or modifications. Modifications to the CJIS SA can only be enacted by the Director of the FBI, acting for the U.S. Attorney General.

Here are the CJIS SA facts:

- The FBI CJIS SA shall be executed pursuant to an agreement (contract) between a government entity and a contractor/vendor when that contractor/vendor needs access to CJJ to perform their contracted duties. The government entity can be either a criminal justice (e.g. police

department) or non-criminal justice (e.g. county IT department running criminal justice systems for a police department per an MCA) agency.

- Each private contractor/vendor employee who works pursuant to the contract/engagement shall acknowledge, by signing the CJIS SA Certification page, and abide by all aspects of the CJIS Security Addendum.

- Private contractors/vendors who perform criminal justice functions and have access to CJI shall meet the same training and certification criteria required of governmental agencies performing a similar function and are subject to audit to the same extent as are local agencies.

- Modifications to the CJIS SA shall be enacted only by the Director of the FBI, acting for the U.S. Attorney General. Remember, accept no changes, additions or deletions from the contractor/vendor (of course, you can't make any either).

The only exception to any of the above requirements is if NCJA personal are escorted and directly supervised 100% of the time when accessing a physically secure location.