Noncriminal Justice Information Technology Security Audit Outline

This outline provides baseline actions necessary to determine compliance with requirements for limited access only to criminal justice information (CJI) for noncriminal justice purposes. The checklist can be used by states and federal agencies when preparing to conduct audits of their local agencies/subcomponents, or to advise audit participants on what to expect during an audit. The checklist is categorized by policy areas assessed during Information Technology Security audits conducted by the Federal Bureau of Investigation's (FBI) Criminal Justice Services (CJIS) Division, CJIS Audit Unit. This checklist serves as a guide to those agencies whose only access to CJI is either hard copy or digital copy not stored electronically within a database or hard copy not housed by another entity.

1. **Local Agency Security Officer (LASO)**
   Every agency shall have an individual who ensures the following components are met.
   Each LASO shall:
   1. Identify who is using the approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
   2. Ensure that personnel security screening procedures are being followed and as a note, for noncriminal justice users the appropriate statute must be in place for this policy to be applicable.
   3. Ensure the approved and appropriate security measures are in place and working as expected.
   4. Support policy compliance and ensure the appropriate personnel are promptly informed of security incidents.

2. **Standards of discipline**
   Every agency will have a policy that outlines a formal sanctions process for personnel failing to comply with established information security policies and procedures.

3. **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. Below are the minimum list of security topics that must be covered by each employee dependent on their level of access to CJI.
   Level One Security Awareness Training: includes all personnel who have unescorted access to a physically secure location.
   At a minimum, the following topics shall be addressed as baseline security awareness training:
   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.

Level Two Security Awareness Training: includes all authorized personnel with access to CJI.

In addition to the Level One Security Awareness Training requirements, the following topics, at a minimum, shall be addressed as baseline security awareness training:

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.

4. Physical Protection

Every agency will have a physical protection policy that outlines how CJI, specifically hard copy media is physically protected through access control measures.

1. The policy will cover the physical security controls used to help safeguard CJI.
2. The agency will develop a list of authorized personnel.
3. All visitors will be escorted at all times.
4. The agency will authenticate visitors prior to being escorted.

5. Media Protection

Every agency will have a media protection policy that outlines how CJI, specifically physical hard copy media is physically protected through access control measures.

1. The agency shall securely store physical hard copy media.
2. The agency shall restrict access to physical hard copy media to only authorized individuals.

6. Media Disposal

Every agency will have a media disposal policy that outlines how CJI, specifically hard copy media is physically destroyed at the end of life.

1. Physical media shall be securely disposed of when no longer required, using formal procedures.
2. Physical media shall be destroyed by shredding or incineration.
3. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

7. Security Incident Response

Every agency will have a media disposal policy that outlines how a security incident will be identified and reported to the FBI CJIS Division.