



Outsourcing Agreements

Required by the National Crime Prevention and Privacy Compact Council

- When a contractor performs a non-criminal justice administrative function.
- Outsourcing includes Casino or Tribal IT personnel

Outsourcing Agreement Process

- Prepare draft contract with contractor / vendor
- Send letter and draft contract to FBI Compact Officer (& a copy to the NIGC ISO)
- Once approved, execute contract and audit contractor within 90 days



First Steps to Achieve Compliance


Section 7 - First Steps to Achieve Compliance

7.1 How to achieve compliance


The NIGC has created the following guideline to assist TGRAs in ensuring compliance with the FBI CJIS Security Policy and NIGC MOU requirements.

1. Review Memorandum of Understanding with NIGC (10 days)
 - a. Ensure most recent version is in use (current version 2017);
 - b. Ensure current TGRA head or authorized official has executed agreement; and
 - c. Ensure all staff subject to agreement and using CHRICHRI has reviewed its contents.
2. Update authorized personnel list (<http://bit.ly/AUserList>) (10 days)
 - a. Designate Local Agency Security Officer (LASO);
 - b. List all personnel with access to FBI CHRI received from NIGC; and
 - c. Send authorized personnel list to NIGC Information Security Officer (ISO) at iso@nigc.gov...
 - d. Maintain up-to-date authorized personnel list on site and on record with NIGC ISO.
3. Complete and document initial CJIS Security Awareness Training within next 6 months via (30 -60 days):




 **First Steps to Achieve Compliance**

- Review MOU
- Update & Submit Authorized Personnel List
- Complete Security Awareness Training

 **First Steps to Achieve Compliance**

4. Begin reviewing resource information (<https://www.nigc.gov/compliance/CJIS-Training-Materials>) (30-60 days):
 - a. National Information Systems (NIS) Resource Guide;
 - b. Criminal Justice Information Services (CJIS) Security Policy
 - c. NIGC Fingerprint site (<https://www.nigc.gov/finance/fingerprint-process>); and
 - d. TGRA internal policies.
5. Complete CJIS IT Questionnaire (<http://bit.ly/CJISITQuestions>) (10 days):
 - a. Determine readiness/compliance level; and
 - b. Begin improving network hardware, software and policy to achieve compliance (6-12 months).
6. Develop/refine written internal TGRA policies to meet CJIS requirements including (6-12) months:
 - a. Use of fingerprint based CHRI;
 - b. Applicants Rights Notice/FBI Privacy Act Notice/Opportunity to Correct/Copy of CHRI;
 - c. Security Awareness Training;
 - d. Incident Response Policy;
 - e. Auditing and Accountability;
 - f. Access Control;
 - g. Identification and Authentication;
 - h. Configuration Management;
 - i. Media Protection;
 - j. Physical Protection;

 **First Steps to Achieve Compliance**

- Review resource information
- Complete CJIS IT Questionnaire
- Develop / Refine TGRA policies
