Initial Steps to CJIS Compliance

(Estimated Days to Complete Task)

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 CHRI 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):
    a. PowerPoint presentation;
    b. Video presentation; or
    c. Online.
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;
    k. System and Communication Protection and Information Integrity;
    l. Formal Audits;
    m. Personnel Security; and
    n. Mobile Devices;
7. Complete and document internal training on TGRA policies (following timeline of Step 6, 30-60 days).
8. Authorized personnel sign training/penalty acknowledgement statements for TGRA policies (following Step 7).
9. Outsourcing Agreements for non-channelers (6-9 months):
    a. Identify all IT service providers with access to electronic media containing FBI CHRI;
    b. Identify other service providers with access to physical copies of CHRI (shredding services, storage facilities);
    c. Submit request letter to FBI Compact Officer for outsourcing contract approval;
    d. Execute contract;
    e. Complete 90-day audit of contractor; and
    f. Provide certification to FBI Compact Officer that contractor meets CJIS Security Policy.
10. Prepare for first annual NIGC audit using site visit checklist (http://bit.ly/CJISSVCKList) (on-going).
11. Continue internal auditing/monitoring to maintain compliance with FBI requirements (on-going).
12. Complete biennial training for users and annually for outsourced non-channelers (on-going).

FBI CJIS Auditor will select three to four tribes Summer/Fall of 2021 for testing against full compliance with NIS and CJIS Security Policy standards as they apply to non-criminal justice agencies and the NIGC MOU.

Additional resource material available at https://www.nigc.gov/compliance/CJIS-Training-Materials and https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center. Updated February 24, 2020