



ILLINOIS STATE POLICE
Office of the Director

Bruce Rauner
Governor

April 3, 2018

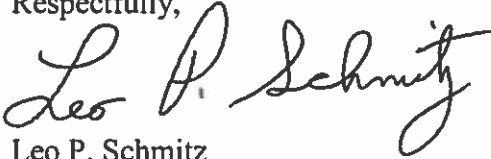
Leo P. Schmitz
Director

The Honorable Bruce Rauner
Governor of Illinois
207 State House
Springfield, Illinois 62706

Dear Governor Rauner:

In accordance with the Illinois Uniform Conviction Information Act, 20 ILCS 2635/21, the Illinois State Police shall conduct regular representative audits of the criminal history record system and report the findings of the audit to the Governor and General Assembly.

The Illinois State Police utilizes the Federal Bureau of Investigation's triennial audit of our criminal history system to meet this requirement. Attached are the executive summaries of the most recent audits conducted as well as the final audit compliance letter. The complete audit reports are available upon request.

Respectfully,

Leo P. Schmitz
Director

Enclosure

cc: Senator William E. Brady
Senator John Cullerton
Representative Jim Durkin
Representative Michael Madigan



National Crime Prevention and Privacy Compact

Compact Council Office
1000 Custer Hollow Road
Clarksburg, WV 26306-0145

July 5, 2017

Lieutenant John Rattigan
Bureau Chief
Bureau of Identification
Illinois State Police
260 North Chicago Street
Joliet, IL 60432-4075

Dear Lieutenant Rattigan:

The National Crime Prevention and Privacy Compact Council's (Council's) Sanctions Committee, in accordance with Title 28, Code of Federal Regulations, Part 907, reviews applicable results of National Identity Services (NIS) audits and Information Technology Security audits conducted by the Federal Bureau of Investigation's (FBI's) Criminal Justice Information Services Division. The Sanctions Committee also reviews the results of Interstate Identification Index usage assessed during National Crime Information Center audits. The process includes a review of responses provided by audit participants to ensure corrective actions adequately address compliance issues.

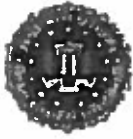
In May 2017, the Sanctions Committee reviewed your response resulting from the Council's request for additional information in correspondence dated January 13, 2017. Based on recommendations made by the Sanctions Committee, the Council is **satisfied** with the updated corrective actions taken to address the compliance issues identified during the NIS audit. The Council does not require an additional response and considers the NIS **audit formally closed**.

The Council encourages your continued endeavors to comply with policy requirements. Should you have any questions, please contact Ms. Chasity S. Anderson, FBI Compact Officer, at 304-625-2803 or <csanderson@fbi.gov>.

Sincerely yours,

A handwritten signature in cursive script that reads "Dawn A. Peck".

Ms. Dawn A. Peck
Council Chairman



U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

National Identity Services Audit Report

Illinois

March 2015

Executive Summary

Overview

The FBI's Criminal Justice Information Services (CJIS) Division has established audit programs for the purpose of evaluating compliance with policy requirements associated with access to CJIS systems and information. The National Identity Services (NIS) Audit assesses compliance with Interstate Identification Index (III) and National Fingerprint File (NFF) participation standards; federal laws and regulations associated with the use, dissemination, and security of national criminal history record information (CHRI); and National Crime Prevention and Privacy Compact (Compact) rules and procedures. The NIS Audit is conducted with state criminal history record repositories, federal agencies, and other entities that are authorized direct access to Next Generation Identification (NGI) and III, and includes reviews of local agencies which receive CHRI for non-criminal justice purposes.

Audit Results

The CJIS Division conducted the eighth cycle NIS Audit of Illinois State Police (ISP) during March 2015. The following recommendations are based on policy violations and require a response describing corrective actions:

1. **Use of CHRI.** Ensure CHRI obtained through fingerprint-based submissions is only used for authorized purposes. *(This was a recommendation during the previous audit cycle.)*
2. **Dissemination.** Ensure CHRI is not disseminated outside the receiving departments, related agencies, or other authorized entities. *(This was a recommendation during the previous two audit cycles.)*
3. **Applicant Notification and Record Challenge.** Ensure requirements are met for applicant notification and record challenge. *(This was a recommendation during the previous two audit cycles.)*

The following recommendations should be considered based on areas of concern associated with additional policies and best business practices:

- **Outsourcing of Non-Criminal Justice Administrative Functions.** Ensure local agencies approved to outsource noncriminal justice administrative functions involving access to CHRI meet all provisions of the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers.

NIS Audit Findings Summary Chart

Policy	Finding
Fingerprint Identification Matters	
Management Control	In Compliance
Fingerprint Identification	In Compliance
Sole Source Submission	In Compliance
Supporting Fingerprints	In Compliance
Continued Submission	In Compliance
Record Content and III Maintenance	
Record Content	In Compliance
Record Expungement	In Compliance
Record Synchronization	In Compliance
Record Maintenance	In Compliance
Record Response	
Record Response	In Compliance
Literal Translation	In Compliance
Out-of-State and Federal Records	In Compliance
Non-Criminal Justice Use of CHRI and User Fee	
Use of CHRI	Out of Compliance
Reason Fingerprinted Field and Purpose Code Usage	In Compliance
Dissemination of CHRI	Out of Compliance
Applicant Notification and Record Challenge	Out of Compliance
Security of CHRI	In Compliance
III Access for Non-Criminal Justice Applicant Purposes (Purpose Code I)	In Compliance
III Access for Exigent Circumstances (Purpose Code X)	In Compliance
Outsourcing of Non-Criminal Justice Administrative Functions	Area of Concern
State Non-Criminal Justice Agency Audits	In Compliance
User Fee	In Compliance



U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Non-Criminal Justice (NCJA)
Information Technology Security (ITS)
Audit Report

Illinois

March 2015

Executive Summary

Overview

The FBI CJIS Division is authorized to conduct security audits of the CJIS Systems Agency (CSA) and State Identification Bureau (SIB) networks and systems, once every three (3) years at a minimum, to assess agency compliance with the *CJIS Security Policy*. The essential premise of the *CJIS Security Policy* is to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI) which includes national criminal history record information (CHRI), a subset of CJI, whether at rest or in transit. The *CJIS Security Policy* provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information. Policies and procedures governing the security of CJI are examined during the audits. Although compliance with all CJIS security policies was not assessed, adherence to all CJIS security policies and procedures is required for FBI CJIS systems access.

Audit Recommendations

Based on the ITS Audit conducted during March 2015, the FBI's CJIS Division makes the following recommendation(s) to the CSA/SIB as listed below.

- 1. Ensure local agencies implement the Security and Management Control Outsourcing Standard prior to executing a contract or agreement that permits a contractor to access national CHRI.**
- 2. Ensure the CSA provides security awareness training to all agency terminal operators, IT personnel, noncriminal justice agency personnel, and private contractor personnel who manage and/or have access to CJI within six months of assignment and/or at least once every two years.**
- 3. Ensure the local agencies display an approved system use notification message on all information systems accessing CJI.**

Since most non-criminal justice agencies have not previously been subject to an ITS audit by the FBI CJIS Division CAU prior to October 1, 2014, the first cycle ITS audit will be considered a zero-cycle audit. These policy requirements, although assessed, will not be forwarded through the APB Compliance Evaluation Subcommittee or the National Crime Prevention and Privacy Compact Council's Sanctions Committee during the current zero-cycle audit. The intent is for agencies to start working toward compliance immediately. The audit can be used as a tool for financial planning and justification to meet these security requirements. Adherence to all policies and procedures is required for access to and use of CJI.

The following terms are used in compliance summary charts throughout the report.

IN	Agency is <i>IN</i> compliance with policy/procedure.
OUT	Agency is <i>OUT</i> of compliance with policy/procedure. Corrective Action is needed.
N/A (Not Applicable)	Policy/procedure is not applicable to the agency and therefore not assessed. Policies which are not assessed as part of the audit are displayed as shaded areas within each summary chart.

ITS Audit Policy Compliance Summary

The following chart provides a listing of policies assessed during the audit and indicates overall compliance by the Illinois State Police.

Policy	Finding
System Administration	
CJIS Systems Officer/Repository Manager	IN
Information Security Officer	IN
Local Agency Security Officer (LASO)	IN
Administration of Non-Criminal Justice Functions	
Contracted Non-Criminal Justice Services	OUT
Information Protection	
IT Security Program	IN
Standards of Discipline	IN
Personnel Security	IN
Security Awareness Training	OUT
Physical Security	IN
Security Audits	IN
Media Protection	IN
Media Transport	IN
Media Disposal	IN

Policy	Finding
Network Infrastructure	
Network Configuration	IN
Personally Owned Information Systems	
Publicly Accessible Computers	IN
System Use Notification	OUT
Identification/UserID	IN
Authentication	IN
Session Lock	IN
Event Logging	IN
Remote Maintenance	
Advanced Authentication	
Encryption	IN
Dial-up Access	
Mobile Devices	
Personal Firewalls	
Cellular Access	
Bluetooth Access	
Wireless (802.11x) Access	
Boundary Protection	IN
Intrusion Detection Tools & Techniques	IN
Malicious Code Protection	IN
Spam and Spyware Protection	IN
Security Alerts and Advisories	IN



Patch Management	IN
Voice over Internet Protocol (VoIP)	
Partitioning and Virtualization	
Cloud Computing	
Security Incident Response	IN