



Office of the Inspector General
U.S. Department of Justice



**Audit of Compliance with
Standards Governing Combined
DNA Index System Activities at
the Denver Police Department
Crime Laboratory
Denver, Colorado**

Audit Division GR-60-17-013

September 2017

REDACTED – FOR PUBLIC RELEASE

AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE DENVER POLICE DEPARTMENT CRIME LABORATORY DENVER, COLORADO

EXECUTIVE SUMMARY*

The Department of Justice Office of the Inspector General (OIG), Audit Division, has completed an audit of compliance with standards governing Combined DNA Index System (CODIS) activities at the Denver Police Department Crime Laboratory (Laboratory) in Denver, Colorado.

The Federal Bureau of Investigation's (FBI) CODIS program combines forensic science and computer technology to provide an investigative tool to federal, state, and local crime laboratories in the United States, as well as those from select international law enforcement agencies. The CODIS program allows these crime laboratories to compare and match DNA profiles electronically to assist law enforcement in solving crimes and identifying missing or unidentified persons.² The FBI's CODIS Unit manages CODIS, as well as develops, supports, and provides the program to crime laboratories to foster the exchange and comparison of forensic DNA evidence.

The FBI implemented CODIS as a distributed database with hierarchical levels that enables federal, state, and local crime laboratories to compare DNA profiles electronically. The hierarchy consists of three distinct levels that flow upward from the local level to the state level and then, if allowable, the national level. The National DNA Index System (NDIS), the highest level in the hierarchy, contains DNA profiles uploaded by law enforcement agencies across the United States and is managed by the FBI. NDIS enables the laboratories participating in the CODIS program to electronically compare DNA profiles on a national level. The State DNA Index System (SDIS) is used at the state level to serve as a state's DNA database and contains DNA profiles from local laboratories and state offenders. The Local DNA Index System (LDIS) is used by local laboratories.

Our audit generally covered the period from February 2012 through March 2017. The objectives of our audit were to determine if: (1) the Laboratory was in compliance with select NDIS Operational Procedures; (2) the Laboratory was in compliance with certain Quality Assurance Standards (QAS) issued by the FBI;

* Redactions were made to the full version of this report for privacy reasons. The redactions are contained only in Appendix 3, the grantee's response, and are of an individual's names.

² DNA, or deoxyribonucleic acid, is the hereditary material found in almost all organisms that contains encoded information necessary for building and maintaining an organism. More than 99 percent of human DNA is the same for all people. The differences found in the remaining less than 1 percent allow scientists to develop a unique set of DNA identification characteristics (a DNA profile) for an individual by analyzing a specimen containing DNA.

and (3) the Laboratory's forensic DNA profiles in CODIS databases were complete, accurate, and allowable for inclusion in NDIS.

We found that the Laboratory did not encrypt backup CODIS data and did not timely notify the FBI on the change in employment status for 10 users of CODIS, categorized as "IT Users." We did not identify any other areas of non-compliance by the Laboratory with the remaining NDIS Operational Procedures we reviewed.

We further found that the Laboratory was in compliance with the QAS we reviewed, as the Laboratory underwent QAS reviews within the designated parameters and timeframes, had policies in place to ensure Laboratory access was limited to authorized personnel, and had adequate procedures to ensure the integrity of physical and sampled evidence. We also reviewed 100 of the Laboratory's 3,646 forensic DNA profiles that were uploaded to NDIS between February 2012 and February 2017, and determined that all the profiles that we reviewed were complete, accurate, and allowable for inclusion in NDIS.

We make two recommendations to address the Laboratory's compliance with standards governing CODIS activities, which are discussed in detail in the body of the report. Our audit objectives, scope, and methodology are detailed in Appendix 1 of the report and the audit criteria are detailed in Appendix 2. We discussed the results of our audit with Laboratory officials and have included their comments in the report as applicable.

**AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING
COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE
DENVER POLICE DEPARTMENT CRIME LABORATORY
DENVER, COLORADO**

TABLE OF CONTENTS

OIG Audit Objectives	1
Legal Foundation for CODIS	1
Allowable DNA Profiles.....	2
Allowable Disclosure of DNA Profiles	2
CODIS Architecture	2
National DNA Index System	3
State and Local DNA Index Systems.....	5
Laboratory Information.....	5
Compliance with Select NDIS Operational Procedures	6
Encryption of the Local CODIS Database Backup.....	6
Discrepancies in Active CODIS and IT Users as listed at the FBI and the Laboratory.....	7
Compliance with Certain Quality Assurance Standards	7
Suitability of Forensic DNA Profiles in CODIS Databases.....	8
Conclusion	9
Recommendations.....	9
APPENDIX 1: OBJECTIVES, SCOPE, AND METHODOLOGY	10
APPENDIX 2: AUDIT CRITERIA.....	12
APPENDIX 3: DENVER POLICE DEPARTMENT CRIME LABORATORY RESPONSE TO THE DRAFT AUDIT REPORT.....	15
APPENDIX 4: FEDERAL BUREAU OF INVESTIGATION RESPONSE TO THE DRAFT AUDIT REPORT.....	17
APPENDIX 5: ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE AUDIT REPORT.....	18

AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE DENVER POLICE DEPARTMENT CRIME LABORATORY DENVER, COLORADO

The Department of Justice Office of the Inspector General (OIG), Audit Division, has completed an audit of compliance with standards governing Combined DNA Index System (CODIS) activities at the Denver Police Department Crime Laboratory (Laboratory) in Denver, Colorado.

The Federal Bureau of Investigation's (FBI) CODIS provides an investigative tool using forensic science and computer technology to federal, state, and local crime laboratories in the United States and, on a case-by-case basis, select international law enforcement agencies. The CODIS program allows these laboratories to compare and match DNA profiles electronically, thereby assisting law enforcement in solving crimes and identifying missing or unidentified persons.¹ The FBI's CODIS Unit manages CODIS and is responsible for its use in fostering the exchange and comparison of forensic DNA evidence.

OIG Audit Objectives

Our audit generally covered the period from February 2012 through March 2017. The objectives of our audit were to determine if: (1) the Laboratory was in compliance with select National DNA Index System (NDIS) Operational Procedures; (2) the Laboratory was in compliance with certain Quality Assurance Standards (QAS) issued by the FBI; and (3) the Laboratory's forensic DNA profiles in CODIS databases were complete, accurate, and allowable for inclusion in NDIS. Appendix 1 contains a detailed description of our audit objectives, scope, and methodology; and Appendix 2 contains the criteria used to conduct the audit.

Legal Foundation for CODIS

The FBI's CODIS program began as a pilot project in 1990. The DNA Identification Act of 1994 (Act) authorized the FBI to establish a national index of DNA profiles for law enforcement purposes. The Act, along with subsequent amendments, has been codified in a federal statute (Statute) providing the legal authority to establish and maintain NDIS.²

¹ DNA, or deoxyribonucleic acid is the hereditary material found in almost all organisms that contains encoded information necessary for building and maintaining an organism. More than 99 percent of human DNA is the same for all people. The differences found in the remaining less than 1 percent allow scientists to develop a unique set of DNA identification characteristics (a DNA profile) for an individual by analyzing a specimen containing DNA.

² 42 U.S.C.A. § 14132 (2006).

Allowable DNA Profiles

The Statute authorizes NDIS to contain the DNA identification records of persons convicted of crimes, persons who have been charged in an indictment or information with a crime, and other persons whose DNA samples are collected under applicable legal authorities. Samples voluntarily submitted solely for elimination purposes are not authorized for inclusion in NDIS. The Statute also authorizes NDIS to include analysis of DNA samples recovered from crime scenes or from unidentified human remains, as well as those voluntarily contributed from relatives of missing persons.

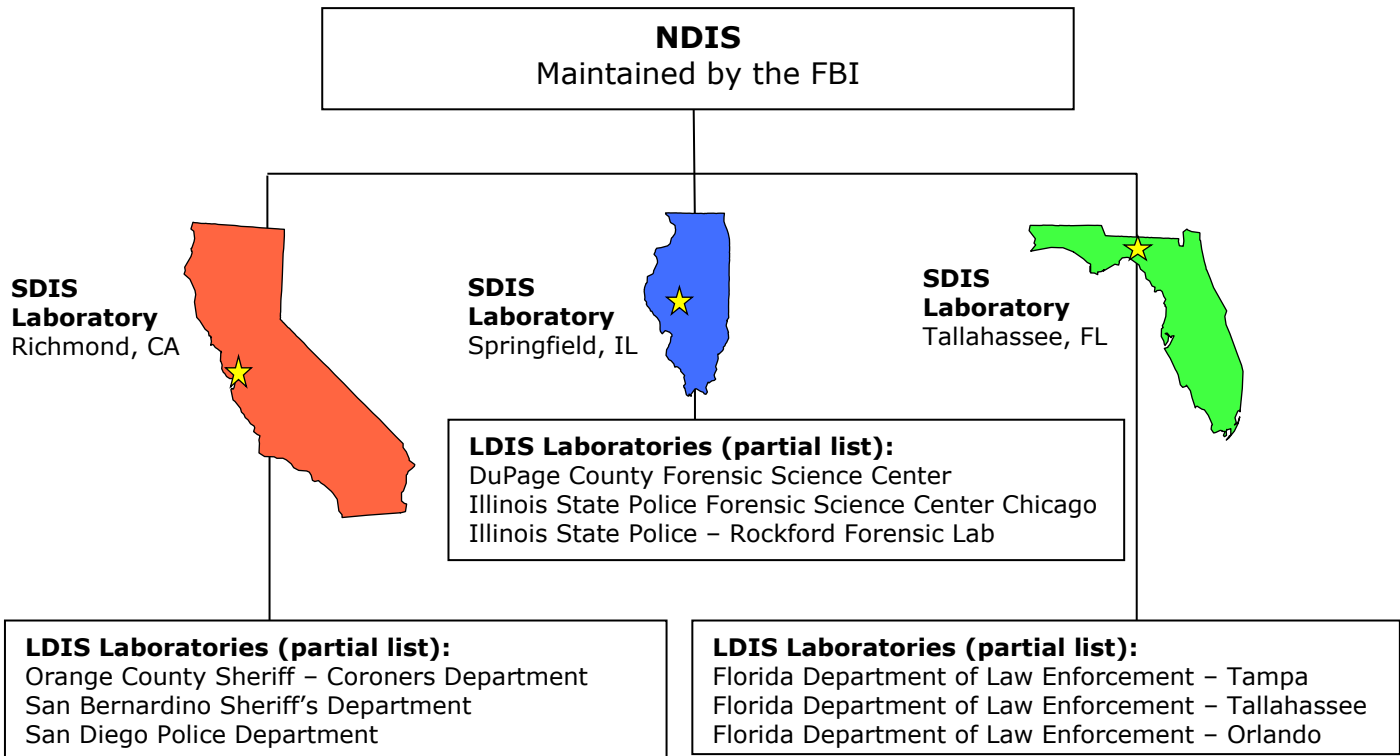
Allowable Disclosure of DNA Profiles

The Statute requires that NDIS only include DNA information that is based on analyses performed by or on behalf of a criminal justice agency – or the U.S. Department of Defense – in accordance with QAS issued by the FBI. The DNA information in the index is authorized to be disclosed only: (1) to criminal justice agencies for law enforcement identification purposes; (2) in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules; (3) for criminal defense purposes, to a defendant who shall have access to samples and analyses performed in connection with the case in which the defendant is charged; or (4) if personally identifiable information (PII) is removed for a population statistics database, for identification research and protocol development purposes, or for quality control purposes.

CODIS Architecture

The FBI implemented CODIS as a distributed database with hierarchical levels that enables federal, state, and local crime laboratories to compare DNA profiles electronically. CODIS consists of a hierarchy of three distinct levels: (1) NDIS, managed by the FBI as the nation's DNA database containing DNA profiles uploaded by participating states; (2) the State DNA Index System (SDIS), which serves as a state's DNA database containing DNA profiles from local laboratories within the state and state offenders; and (3) the Local DNA Index System (LDIS), used by local laboratories. DNA profiles originate at the local level and then flow upward to the state and, if allowable, national level. For example, the local laboratory in the Florida Department of Law Enforcement Orlando, Florida, sends its profiles to the state laboratory in Tallahassee, Florida, which then uploads the profiles to NDIS. Each state participating in CODIS has one designated SDIS laboratory. The SDIS laboratory maintains its own database and is responsible for overseeing NDIS issues for all CODIS-participating laboratories within the state. The graphic below illustrates how the system hierarchy works.

Example of System Hierarchy within CODIS



National DNA Index System

NDIS, the highest level in the CODIS hierarchy, enables laboratories participating in the CODIS program to electronically compare DNA profiles on a national level. NDIS does not contain names or other PII about the profiles. Therefore, matches are resolved through a system of laboratory-to-laboratory contacts. NDIS contains the following searchable indices:

- Convicted Offender Index contains profiles generated from persons convicted of qualifying offenses.³
- Arrestee Index is comprised of profiles developed from persons who have been arrested, indicted, or charged in an information with a crime.
- Legal Index consists of profiles that are produced from DNA samples collected from persons under other applicable legal authorities.
- Detainee Index contains profiles from non-U.S. persons detained under the authority of the U.S. and required by law to provide a DNA sample.
- Multi-allelic Offender Index consists of profiles from offenders (arrestees, convicted offenders, detainees, or legal index specimens) having three or more alleles at two or more loci.

³ The phrase “qualifying offenses” refers to state or federal crimes that require a person to provide a DNA sample in accordance with applicable laws.

- Forensic Index contains DNA records originating from and associated with an evidence sample from a single source (or a fully deduced profile originating from a mixture) that was found at a crime scene.
- Forensic Mixture Index profiles originate from forensic samples that contain DNA contributed from more than one source attributable to a putative perpetrator(s).
- Forensic Partial Index consists of DNA profiles from forensic samples that do not contain the results for all 13 Original CODIS Core Loci and/or that may indicate a possibility of allelic dropout.
- Missing Person Index contains known DNA records of missing persons and deduced missing persons.
- Unidentified Human (Remains) Index holds profiles from unidentified living individuals and the remains of unidentified deceased individuals.⁴
- Relatives of Missing Person Index is comprised of DNA profiles generated from the biological relatives of individuals reported missing.
- Pedigree Tree Index consists of DNA records of biological relatives and spouses of missing persons that are associated with a pedigree tree.

Given the multiple indices, the main functions of CODIS are to: (1) generate investigative leads that may help in solving crimes and (2) identify missing and unidentified persons.

The Forensic Index generates investigative leads in CODIS that may help solve crimes. Investigative leads may be generated through matches between the Forensic Index and other indices in the system, including the Convicted Offender, Arrestee, and Legal Indices. These matches may provide investigators with the identity of suspected perpetrators. CODIS also links crime scenes through matches between Forensic Index profiles, potentially identifying serial offenders.

In addition to generating investigative leads, CODIS furthers the objectives of the FBI's National Missing Person DNA Database program through its ability to identify missing and unidentified individuals. For instance, those persons may be identified through matches between the profiles in the Missing Person Index and the Unidentified Human (Remains) Index. In addition, the profiles within the Missing Person and Unidentified Human (Remains) Indices may be searched against the Forensic, Convicted Offender, Arrestee, Detainee, and Legal Indices to provide investigators with leads in solving missing and unidentified person cases.

⁴ An example of an Unidentified Human (Remains) Index profile from a living person is a profile from a child or other individual, who cannot or refuses to identify themselves.

State and Local DNA Index Systems

The FBI provides CODIS software free of charge to any state or local law enforcement laboratory performing DNA analysis. Laboratories are able to use the CODIS software to upload profiles to NDIS. However, before a laboratory is allowed to participate at the national level and upload DNA profiles to NDIS, a Memorandum of Understanding (MOU) must be signed between the FBI and the laboratory. The MOU defines the responsibilities of each party, includes a sublicense for the use of CODIS software, and delineates the standards laboratories must meet in order to utilize NDIS.

States are authorized to upload DNA profiles to NDIS based on local, state, and federal laws, as well as NDIS regulations. However, states or localities may maintain NDIS-restricted profiles in SDIS or LDIS. For instance, a local law may allow for the collection and maintenance of a victim profile at LDIS but NDIS regulations do not authorize the upload of that profile to the national level.

The utility of CODIS relies upon the completeness, accuracy, and quality of profiles that laboratories upload to the system. Incomplete CODIS profiles are those for which the required number of core loci were not tested or do not contain all of the conclusive DNA information that resulted from a DNA analysis and may not be searched at NDIS.⁵ The probability of a false match among DNA profiles is reduced as the completeness of a profile increases. Inaccurate profiles, which contain incorrect DNA information, may generate false positive leads, false negative comparisons, or lead to the identification of an incorrect sample. Further, laws and regulations exclude certain types of profiles from being uploaded to CODIS to prevent violations to an individual's privacy and foster the public's confidence in CODIS. Therefore, it is the responsibility of the Laboratory to ensure that it is adhering to the NDIS Operational Procedures and the profiles uploaded to CODIS are complete, accurate, and allowable for inclusion in NDIS.

Laboratory Information

The Laboratory, specifically the Forensic Biology/DNA Unit, participates in the CODIS program as an LDIS laboratory and maintains a forensic database. The Laboratory began processing DNA evidence for criminal cases in 1993 to compare profiles at the local and state level, and began performing Short Tandem Repeat analysis in 1999. In 2003, the Laboratory's DNA Unit first achieved QAS compliance and expanded its searching capabilities to the national level of the FBI's CODIS database.

The Laboratory achieved International Organization for Standardization (ISO) accreditation in 2005, which is an internationally recognized quality management

⁵ A "locus" is a specific location of a gene on a chromosome. The plural form of locus is loci. As of January 1 2017, the FBI expanded the minimum number of CODIS Core Loci by 7, to a total of 20 core loci.

system. It is currently accredited under ISO 17025:2005 and performs an internal ISO audit annually. The Laboratory's most recent ISO 17025:2005 review took place in April 2015, and the Laboratory is eligible for renewal the summer of 2017.⁶

In March 2017, the CODIS Administrator at the Laboratory stated that the Laboratory does not currently outsource the analysis or technical review of forensic DNA samples to another laboratory, and has not done so in the last 2 years. He also stated that the Laboratory has not employed any contract employees in the last 2 years.

Compliance with Select NDIS Operational Procedures

The NDIS Operational Procedures Manual, which include the NDIS Laboratories Participation Requirements, establish the responsibilities and obligations of laboratories that participate in the CODIS program at the national level. The NDIS Operational Procedures provide detailed instructions for laboratories to follow when performing certain procedures pertinent to NDIS. The NDIS operational procedures we reviewed are listed in Appendix 2 of this report.

We found that the Laboratory did not encrypt the backups of local CODIS data and did not timely notify the FBI on the change in employment status for 10 IT Users, as explained in more detail in the following sections.

Encryption of the Local CODIS Database Backup

NDIS Security Requirements state that the NDIS participating laboratory shall be responsible for conducting backups of CODIS data, and that all backup files shall be encrypted. Additionally, the Denver Technology Services' policies and procedures states that confidential information should be saved in an encrypted form or to encrypted media. The CODIS Administrator stated that the Laboratory backs up CODIS data every night to an external device and rotates backups on a weekly and monthly basis. However, the CODIS Administrator confirmed that the external devices and the data within all backups are not encrypted. Therefore, the Laboratory's DNA Unit does not adhere to the NDIS Security Requirements regarding encryption and does not meet local encryption standards for confidential information. We recommend that the FBI ensure that the Laboratory encrypts all backups of CODIS data. The CODIS Administrator stated that the Laboratory is working to remediate the encryption of the CODIS backup with their technology services.

⁶ Subsequent to the issuance of the final report, the Laboratory provided the OIG with additional information that resulted in non-material report revisions pertaining to the chronology of the Laboratory's participation in CODIS.

Discrepancies in Active CODIS and IT Users as listed at the FBI and the Laboratory

The NDIS Operational Procedures Manual states that if a CODIS or IT user leaves employment at a participating laboratory or if a change in job status makes it inappropriate to continue access, the CODIS Administrator at the participating lab must request the removal of the user within 30 days and forward this request to the FBI CODIS Unit. We compared the FBI's list of active CODIS and IT users to the Laboratory's. We identified more active users within the FBI's list than were actually active at the Laboratory. Specifically, we identified 1 CODIS User and 12 IT Users listed by the FBI as active users at the Laboratory that had no access to CODIS at the Laboratory.

For the one CODIS User, the FBI official stated that this CODIS User was misfiled and currently works at an SDIS lab. As a result of our audit, the FBI updated the record for this CODIS User. For the 12 IT Users, the FBI official stated that she was able to locate emails from the Laboratory indicating that two IT Users no longer needed access to CODIS. As a result of our audit, the FBI updated the records for these two IT Users as *Prior Users*. However, the FBI official could not locate any communication from the Laboratory regarding the remaining 10 IT Users, and she stated that in order to appropriately update her records, she would need the Laboratory to notify her by email that these individuals are no longer providing IT support. Since July 2012, 8 of the 10 IT Users have not needed access to CODIS. Of the remaining two IT Users, one did not need access since November 2016, and the other currently works at the Laboratory in Technology Services, but does not need access to CODIS. However, the Laboratory did not request removal of these users or notify the FBI. Therefore, we recommend that the FBI ensure the Laboratory provides an accurate listing of IT Users to the FBI.

Although we identified the two deficiencies above, we found that the Laboratory complied with the other NDIS operational procedures we reviewed including: (1) the physical security of the CODIS servers and workstations, (2) CODIS Users completing mandatory annual training, and (3) the CODIS Administrator confirming the NDIS matches within the required 30 business days for a judgmental sample of 10 NDIS matches.

Compliance with Certain Quality Assurance Standards

During our audit, we considered the Forensic QAS issued by the FBI.⁷ These standards describe the quality assurance requirements that the Laboratory must follow to ensure the quality and integrity of the data it produces. We also assessed

⁷ Forensic Quality Assurance Standards refer to the Quality Assurance Standards for Forensic DNA Testing Laboratories, effective September 1, 2011.

the two most recent QAS reviews that the laboratory underwent.⁸ The QAS we reviewed are listed in Appendix 2 of this report.

We found that the Laboratory complied with the Forensic QAS tested. Specifically, we found the Laboratory: (1) underwent QAS reviews, (2) had policies in place to help ensure Laboratory access was limited to authorized personnel, (3) had adequate procedures to ensure the integrity of evidence and extracted DNA samples, and (4) had adequate physical controls to isolate DNA amplification from other processes.

Suitability of Forensic DNA Profiles in CODIS Databases

We reviewed a sample of the Laboratory's Forensic DNA profiles to determine whether each profile was complete, accurate, and allowable for inclusion in NDIS. To test the completeness and accuracy of each profile, we established standards that require a DNA profile include each value returned at each locus for which the lab obtained conclusive results, and that the values at each locus match those identified during analysis. Our standards are described in more detail in Appendix 2 of this report.

The FBI's NDIS Operational Procedures Manual establishes the DNA data acceptance standards by which laboratories must abide. The FBI also developed guidance for the laboratories for determining what is allowable in the forensic index at NDIS. Laboratories are prohibited from uploading forensic profiles to NDIS that clearly match the DNA profile of the victim or another known person that is not a suspect. A profile at NDIS that matches a suspect may be allowable if the contributor is unknown at the time of collection, however, NDIS guidelines prohibit profiles that match a suspect if that profile could reasonably have been expected to be on an item at the crime scene or part of the crime scene independent of the crime. For instance, a profile from an item seized from the suspect's person, such as a shirt, or that was in the possession of the suspect when collected is generally not a forensic unknown and would not be allowable for upload to NDIS. The NDIS procedures we reviewed are listed in Appendix 2 of this report.

We selected a judgmental sample of 100 profiles out of the 3,646 forensic profiles the Laboratory had uploaded to NDIS as of February 23, 2017.⁹ We found that all profiles reviewed were complete, accurate, and allowable for inclusion in NDIS.

⁸ The QAS require that laboratories undergo annual audits. Every other year, the QAS requires that the audit be performed by an audit team of qualified auditor(s) from an external agency. These audits are not required by the QAS to be performed in accordance with the *Government Auditing Standards* (GAS) and are not performed by the Department of Justice Office of the Inspector General. Therefore, we will refer to the QAS audits as reviews (either an internal laboratory review or an external laboratory review, as applicable) to avoid confusion with our audits that are conducted in accordance with GAS.

⁹ We requested from the FBI the universe of forensic profiles uploaded by the Laboratory to NDIS from February 24, 2012, to February 23, 2017.

Conclusion

As a result of our audit testing, we conclude that the Laboratory did not adhere to all the NDIS Participation Requirements that we reviewed. Specifically, we found that the Laboratory did not encrypt the backups of local CODIS data and did not timely notify the FBI on the change in employment status for 10 IT Users. However, we determined that the Laboratory did comply with other select NDIS Operational Procedures that we reviewed, including providing adequate physical security of the CODIS server and work stations, successfully completing the annual training, and confirming NDIS matches in a timely manner for a judgmental sample of NDIS matches. Additionally, we did not identify any significant issues regarding the Laboratory's compliance with the certain Forensic QAS that we tested, as the Laboratory underwent QAS reviews within the designated parameters and timeframes, had policies in place to ensure Laboratory access was limited to authorized personnel, and had adequate procedures to ensure the integrity of physical and sampled evidence. Finally, we found that all the forensic profiles that we tested were complete, accurate, and allowable in NDIS. We provide two recommendations to address the deficiencies identified.

Recommendations

We recommend that the FBI:

1. Work with the Laboratory to ensure that it encrypts all backups of CODIS data.
2. Ensure the Laboratory provides an accurate listing of IT Users to the FBI.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit generally covered the period from February 2012 through March 2017. The objectives of the audit were to determine if the: (1) Laboratory was in compliance with select National DNA Index System (NDIS) Operational Procedures; (2) Laboratory was in compliance with certain Quality Assurance Standards (QAS) issued by the FBI; and (3) Laboratory's forensic DNA profiles in CODIS databases were complete, accurate, and allowable for inclusion in NDIS. To accomplish the objectives of the audit, we:

- Examined internal and external Laboratory QAS review reports and supporting documentation for corrective action taken, if any, to determine whether: (a) the Laboratory complied with the QAS, (b) repeat findings were identified, and (c) recommendations were adequately resolved.

In accordance with the QAS, a laboratory shall establish, follow, and maintain a documented quality system with procedures that address, at a minimum, a laboratory's quality assurance program, organization and management, personnel, facilities, evidence and sample control, validation, analytical procedures, calibration and maintenance of equipment, proficiency testing, corrective action, review, documentation and reports, safety, audits, and outsourcing. The QAS require that internal and external reviews be performed by personnel who have successfully completed the FBI's training course for conducting such reviews. We obtained evidence concerning: (1) the qualifications of the internal and external reviewers, and (2) the independence of the external reviewers.

- Interviewed Laboratory officials to identify management controls, Laboratory operational policies and procedures, Laboratory certifications or accreditations, and analytical information related to DNA profiles.
- Toured the Laboratory to observe facility security measures as well as the procedures and controls related to the receipt, processing, analyzing, and storage of forensic evidence DNA samples.
- Reviewed the Laboratory's written policies and procedures related to conducting internal reviews, resolving review findings, and resolving matches among DNA profiles in NDIS.

- Reviewed supporting documentation for 10 of 94 NDIS matches in the last 2 years to determine whether they were resolved in a timely manner. The Laboratory provided the universe of NDIS matches as of March 13, 2017. The sample was judgmentally selected to include both case-to-case and case-to-offender matches. This non-statistical sample does not allow projection of the test results to all matches.
- Reviewed the case files for selected forensic DNA profiles to determine if the profiles were developed in accordance with the Forensic QAS and were complete, accurate, and allowable for inclusion in NDIS.

We obtained an electronic file identifying the specimen identification numbers of 3,646 searchable forensic profiles the Laboratory had uploaded to NDIS between February 24, 2012, and February 23, 2017. We limited our review to a judgmental sample of 100 profiles.

Using the judgmentally-determined sample size, we employed a stratified sample design to randomly select a representative sample of profiles in our universe. However, since the sample size was judgmentally determined, the results obtained from testing this limited sample of profiles may not be projected to the universe of profiles from which the sample was selected.

The objectives of our audit concerned the Laboratory's compliance with required standards and the related internal controls. Accordingly, we did not attach a separate statement on compliance with laws and regulations or a statement on internal controls to this report. See Appendix 2 for detailed information on our audit criteria.

AUDIT CRITERIA

In conducting our audit, we considered the NDIS Operational Procedures, QAS, and guidance issued by the FBI regarding forensic profile allowability in NDIS. However, we did not test for compliance with elements that were not applicable to the Laboratory. In addition, we established standards to test the completeness and accuracy of DNA profiles as well as the timely notification of DNA profile matches to law enforcement.

NDIS Operational Procedures

The NDIS Operational Procedures, which include the NDIS Participation Requirements, establish the responsibilities of the FBI and the NDIS participating laboratories. We focused our audit on the following specific sections of the NDIS Procedures:

- NDIS Laboratories
- Quality Assurance Standards Audit Review
- NDIS Confirmation and Hit Dispositioning
- NDIS DNA Records
- DNA Data Acceptance Standards
- NDIS Searches
- NDIS Security Requirements

Quality Assurance Standards

The FBI issued two sets of QAS: (1) QAS for Forensic DNA Testing Laboratories, effective September 1, 2011 (Forensic QAS); and (2) QAS for DNA Databasing Laboratories, effective September 1, 2011 (Offender QAS). The Forensic QAS and the Offender QAS describe the quality assurance requirements that the Laboratory should follow to ensure the quality and integrity of the data it produces.

For our audit, we reviewed the Laboratory's most recent annual external review and performed audit work to verify that the Laboratory was in compliance with the QAS listed below because they have a substantial effect on the integrity of the DNA profiles uploaded to NDIS.

- Facilities (Forensic QAS and Offender QAS 6.1): The laboratory shall have a facility that is designed to ensure the integrity of the analyses and the evidence.
- Evidence Control (Forensic QAS 7.1 and 7.2): The laboratory shall have and follow a documented evidence control system to ensure the integrity of physical evidence. Where possible, the laboratory shall retain or return a portion of the evidence sample or extract.

- Analytical Procedures (Forensic QAS): The laboratory shall monitor the analytical procedures using [appropriate] controls and standards.
- Review (Forensic QAS 12.1): The laboratory shall conduct administrative and technical reviews of all case files and reports to ensure conclusions and supporting data are reasonable and within the constraints of scientific knowledge.
- [Reviews] (Forensic QAS): The laboratory shall be audited annually in accordance with [the QAS]. The annual audits shall occur every calendar year and shall be at least 6 months and no more than 18 months apart.

At least once every 2 years, an external audit shall be conducted by an audit team comprised of qualified auditors from a second agency(ies) and having at least one team member who is or has been previously qualified in the laboratory's current DNA technologies and platform.

- Outsourcing (Forensic QAS): A vendor laboratory performing forensic and database DNA analysis shall comply with these Standards and the accreditation requirements of federal law.
- Forensic QAS 17.4: An NDIS participating laboratory shall have and follow a procedure to verify the integrity of the DNA data received through the performance of the technical review of DNA data from a vendor laboratory.

Office of the Inspector General Standards

We established standards to test the completeness and accuracy of DNA profiles as well as the timely notification of law enforcement when DNA profile matches occur in NDIS. Our standards are listed below.

- Completeness of DNA Profiles: A profile must include each value returned at each locus for which the lab obtained conclusive results. Our rationale for this standard is that the probability of a false match among DNA profiles is reduced as the number of loci included in a profile increases. A false match would require the unnecessary use of laboratory resources to refute the match.
- Accuracy of DNA Profiles: The values at each locus of a profile must match those identified during analysis. Our rationale for this standard is that inaccurate profiles may: (1) preclude DNA profiles from being matched and, therefore, the potential to link convicted offenders to a crime or to link previously unrelated crimes to each other may be lost; or (2) result in a false match that would require the unnecessary use of laboratory resources to refute the match.
- Timely Notification of Law Enforcement When DNA Profile Matches Occur in NDIS: Laboratories should notify law enforcement personnel of NDIS matches within 2 weeks of the match confirmation date, unless there are extenuating circumstances. Our rationale for this standard is that untimely notification of law enforcement personnel may result in the suspected

perpetrator committing additional, and possibly more egregious, crimes if the individual is not deceased or already incarcerated for the commission of other crimes.

**DENVER POLICE DEPARTMENT CRIME LABORATORY
RESPONSE TO THE DRAFT AUDIT REPORT**



**CITY AND COUNTY OF DENVER
DEPARTMENT OF SAFETY
FIRE • POLICE • SHERIFF
9-1-1 • COMMUNITY CORRECTIONS
CRIME PREVENTION & CONTROL • SAFE CITY**

Forensics and Evidence
Division
Denver Police Department
1371 Cherokee Street
Denver, CO 80204
Phone: (720) 337-2010
Fax: (720) 337-2012

August 25, 2017

David Sheeren
Regional Audit Manager
Denver Regional Audit Office
Office of the Inspector General
U.S. Department of Justice
1120 Lincoln Street, Suite 1500
Denver, Colorado 80203

Dear Mr. Sheeren:

We write to respond to the findings presented in your draft report received August 3, 2017. This report summarized the findings of your office during their audit of the CODIS program at the Denver Police Department Crime Laboratory in March of 2017. The report outlines two findings on page 6. Below are our responses and plan for remediation for these two issues.

Finding #1

The Laboratory does not encrypt the backups of local CODIS data.

The Laboratory currently performs a backup of all local CODIS data to a flash drive weekly. The Laboratory secures the flash drive in a locked box prior to transporting it offsite for secure storage in a locked safe. There is no evidence that the integrity of the flash drive with the backup data has ever been compromised. A benefit of encryption during backup is that the data is password protected in order to unlock it. In response to this finding, the Laboratory is implementing a backup software program that will encrypt the local CODIS data during the weekly backup. This procedural change has been initiated and will be in place by the end of September of 2017. CODIS data that is shared between laboratories is always encrypted and on a separate, secure network; this is a completely separate process from the local backup procedures.

Finding #2

The Laboratory did not timely notify the FBI on the change in status for 10 IT Users.

Users that are cleared for access to the CODIS terminals for technology support are categorized as IT Users. There were ten (10) IT users at the Laboratory that previously required CODIS access, but no longer required access at the time of the audit. They had not been removed from the FBI's access list for the Laboratory and appeared as active IT users. None of these 10 IT users have had access to the Crime Laboratory facility, nor have they had CODIS login accounts on the CODIS server since 2012. This finding has already been remediated. The Local CODIS Administrator coordinated with the CODIS Unit at the FBI to remove these 10 individuals from the access list for the Laboratory in August of 2017. There are five (5) current IT users (all different than the 10 above) and their need for access will be monitored. A notification will be made by the Local CODIS Administrator to the CODIS Unit at the FBI when and if these individual(s) no longer require access.

These procedural changes will be included in the next version of the Laboratory's CODIS standard operating procedure. Please contact us if additional information is needed.

Sincerely,

Handwritten signature of Gregory LaBerge in blue ink, dated 25-Aug-2017.

Gregory LaBerge
Laboratory Director

Handwritten signature of Bonnie Mountain in blue ink.

Bonnie Mountain
Deputy Director, Quality Assurance Manager

Handwritten signature of Susan G. Berdine in blue ink.

Susan G. Berdine
Deputy Director

Handwritten signature of Eric J. Duvall in blue ink.

Eric J. Duvall
Local Casework CODIS Administrator

cc: Dr. Douglas Hares, NDIS Custodian, Federal Bureau of Investigation
[REDACTED] Paralegal, Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
RESPONSE TO THE DRAFT AUDIT REPORT



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D.C. 20535-0001

September 5, 2017

David M. Sheeren, Regional Audit Manager
Denver Regional Audit Office
Office of the Inspector General
1120 Lincoln, Suite 1500
Denver, CO 80203

Dear Mr. Sheeren:

Your memorandum to Acting Director McCabe forwarding the draft audit report for the Denver Police Department Crime Laboratory, Denver, Colorado ("Laboratory"), has been referred to me for response.

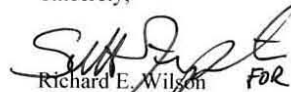
Your draft audit report contained two recommendations relating to the Laboratory's compliance with the FBI's Memorandum of Understanding and *Quality Assurance Standards for Forensic DNA Testing Laboratories*.

With respect to recommendation one relating to the encryption of all backups of CODIS data, the FBI requires that all CODIS backup files are encrypted. Therefore, the FBI agrees with the recommendation to the Laboratory. The Laboratory is implementing a software program to encrypt its weekly backups of CODIS data and updating its standard operating procedures to include this requirement. A completion date of one month is projected for this recommendation. The FBI CODIS Unit is in contact with the Laboratory and continues to work with its staff to ensure that the Laboratory quickly moves forward on this task.

With respect to recommendation two relating to the timely notification of the change in status of IT Users, the FBI requires that a request be submitted within 30 days to remove any CODIS users that no longer need access. Therefore, the FBI agrees with the recommendation to the Laboratory. The Laboratory has already requested the removal of all of its IT users that no longer require CODIS access and is in the process of updating its standard operating procedures to include this requirement. The FBI CODIS Unit is in contact with the Laboratory and continues to work with its staff to ensure that the Laboratory completes this task.

Thank you for sharing the draft audit report with us. If you have any questions, please feel free to contact me at (703) 632-8315.

Sincerely,


Richard E. Wilson
CODIS Unit Chief
Laboratory Division

**OFFICE OF THE INSPECTOR GENERAL
ANALYSIS AND SUMMARY OF ACTIONS
NECESSARY TO CLOSE THE AUDIT REPORT**

The Department of Justice Office of the Inspector General (OIG) provided a draft of this audit report to the Denver Police Department Crime Laboratory (Laboratory) and the Federal Bureau of Investigation (FBI) officials. We incorporated the Laboratory's response in Appendix 3, and the FBI's response in Appendix 4 of this final report. In response to our draft audit report, the FBI stated that it agreed with our recommendations and, as a result, the status of the audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

Recommendations for the FBI:

1. Work with the Laboratory to ensure that it encrypts all backups of CODIS data.

Resolved. In its response to the draft audit report, the FBI stated that it requires that all CODIS backup files are encrypted, and the FBI agreed with the recommendation. It also stated that the FBI CODIS Unit is in contact with the Laboratory to ensure that the Laboratory implements a software program to encrypt the weekly backups of CODIS data and updates its standard operating procedures to include this requirement.

The Laboratory did not agree or disagree with the audit finding. In its response, the Laboratory stated its procedure on the creation and rotation of backup information and the physical security of the flash drive. Further, the Laboratory stated that it will implement a backup software program that will encrypt the local CODIS data during the weekly backup and that this procedural change will be in place by the end of September 2017. Additionally, Laboratory officials stated that they will include this procedural change in the next version of the Laboratory's standard operating procedure.

This recommendation can be closed when we receive confirmation from the FBI that the Laboratory's CODIS data backups are encrypted and documentation that the Laboratory's standard operating procedures have been updated to include this requirement.

2. Ensure the Laboratory provides an accurate listing of IT Users to the FBI.

Resolved. The FBI agreed with the recommendation. In its response to the draft audit report, the FBI stated that it requires a request be submitted within 30 days to remove any CODIS users that no longer need access. Additionally, the FBI stated that the Laboratory has already requested the

removal of its IT users that no longer require CODIS access and is in the process of updating its standard operating procedures to include this requirement. The FBI CODIS Unit is in contact with the Laboratory to ensure it completes this task.

The Laboratory did not agree or disagree with the audit finding. In response, Laboratory officials stated that the Local CODIS Administrator coordinated with the FBI CODIS Unit to remove the 10 IT Users from the access list in August 2017. They also stated that there are currently five IT Users at the lab, and their need for access will be monitored. Once their need for access is no longer required, the Local CODIS Administrator will notify the CODIS Unit at the FBI. Additionally, Laboratory officials stated that they will include this procedural change in the next version of the Laboratory's CODIS standard operating procedure.

This recommendation can be closed when we receive documentation that the Laboratory requested removal of the 10 IT Users that no longer required access to CODIS and that the Laboratory's standard operating procedures have been updated to include this requirement.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.



Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig

REDACTED – FOR PUBLIC RELEASE

REDACTED – FOR PUBLIC RELEASE