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

**OVERSIGHT ★ INTEGRITY ★ GUIDANCE**

# Audit of Compliance with Standards Governing Combined DNA Index System Activities at the San Diego County Sheriff's Department Regional Crime Laboratory, San Diego, California

Audit Division GR-90-18-004

August 2018

# Executive Summary

*Audit of Compliance with Standards Governing Combined DNA Index System Activities at the San Diego County Sheriff's Department Regional Crime Laboratory, San Diego, California*

## Objectives

The objectives of our audit were to determine if: (1) the San Diego County Sheriff's Department (SDSD) Regional Crime Laboratory (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 Federal Bureau of Investigation (FBI); and (3) the Laboratory's forensic DNA profiles in the Combined DNA Index System (CODIS) databases were complete, accurate, and allowable for inclusion in NDIS.

## Results in Brief

Our audit concluded that the Laboratory did not fully comply with NDIS Operational Procedures and certain QAS that we reviewed. We found that the Laboratory did not limit and control access to its laboratory as required by NDIS Security Requirements. Specifically, the Laboratory did not deactivate keycards, which allowed access to restricted areas of the laboratory of former employees and contractors after their work had been completed or their employment with the SDSD had ceased. We also found that the Laboratory's keycard distribution list was not current, as required by the FBI's QAS.

Further, we determined that the Laboratory did not provide adequate physical security over its DNA data and records. We also found that the Laboratory did not properly secure evidence at the end of the day, as required by the Laboratory's policies.

## Recommendations

Our report contains six recommendations to address the Laboratory's compliance with the standards governing CODIS activities. We requested from the Laboratory and FBI their responses to the recommendations, which can be found in Appendices 3 and 4, respectively. Our analysis of those responses is included in Appendix 5.

## Background

The FBI's CODIS program allows crime laboratories across the country to compare and match DNA profiles electronically to help solve crimes and identify missing persons. The FBI implemented CODIS as a distributed database consisting of three distinct hierarchical levels that flow upward from the local level to the state level and then, if allowable, the national level. NDIS, the highest level in the hierarchy, is managed by the FBI and contains DNA profiles uploaded by local, state, and federal crime laboratories. CODIS program participants must comply with FBI requirements to use the system, and this audit reviewed the Laboratory's compliance with those requirements. This audit generally covered the period from December 2012 through November 2017.

## Audit Results

***Forensic DNA Profiles*** – We reviewed a sample of 100 out of a total of 2,461 forensic profiles that the Laboratory had uploaded to NDIS as of November 2017. We found that 17 forensic profiles in our sample lacked adequate information in their respective case files to enable us to determine their CODIS eligibility. However, after our inquiries, the Laboratory was subsequently able to obtain enough additional information to support each of the 17 forensic DNA profile's CODIS eligibility. We determined that all of the forensic DNA profiles in our sample were complete, accurate, and allowable for inclusion in NDIS.

***NDIS Operational Procedures*** – The Laboratory did not adequately limit and control access to its laboratory facility as required by NDIS Security Requirements. We found that the Laboratory did not deactivate keycards for six former employees and contractors upon completion of their work at the Laboratory or separation from the SDSD. Instead, these keycards were active between 8 to 14 years after the keycards should have been collected and deactivated. Further, the Laboratory could not confirm that it retrieved the former employees' and contractors' keycards. We also found that an additional former employee turned in their keycard upon their separation, but that keycard was not deactivated for 111 days, which allowed another authorized employee to use the former employee's card

to gain access to the Laboratory's restricted areas. We also found that the Laboratory did not provide adequate physical security for its DNA data and records.

***Quality Assurance Standards*** – We found that the Laboratory had not complied with the QAS related to controlled access to the Laboratory. Specifically, we found that the Laboratory's distribution list of keycards was inaccurate. Further, we noted that some evidence was left unsecured in the Laboratory. By not securing evidence in storage cabinets, whenever possible, the Laboratory increases its risk of contamination and loss.

# AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE SAN DIEGO COUNTY SHERIFF'S DEPARTMENT REGIONAL CRIME LABORATORY, SAN DIEGO, CALIFORNIA

## TABLE OF CONTENTS


INTRODUCTION ..... 1

OIG Audit Objectives ..... 1

Legal Foundation for CODIS ..... 2

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

AUDIT RESULTS ..... 6

Compliance with Select NDIS Operational Procedures ..... 6

Inadequate Physical Security to the Laboratory ..... 6

DNA Records and Data ..... 9

Compliance with Certain Quality Assurance Standards ..... 11

Internal and External QAS Reviews ..... 11

Safeguarding Evidence ..... 12

Suitability of Forensic DNA Profiles in CODIS Databases ..... 14

Lack of Documentation in its Case Files ..... 14

CONCLUSION AND RECOMMENDATIONS ..... 16

APPENDIX 1: OBJECTIVES, SCOPE, AND METHODOLOGY ..... 18

APPENDIX 2: AUDIT CRITERIA ..... 20

APPENDIX 3: LABORATORY'S RESPONSE TO THE DRAFT AUDIT REPORT ..... 22

APPENDIX 4: FBI'S RESPONSE TO THE DRAFT AUDIT REPORT ..... 26

APPENDIX 5: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT ..... 28

# AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE SAN DIEGO COUNTY SHERIFF'S DEPARTMENT REGIONAL CRIME LABORATORY, SAN DIEGO, CALIFORNIA

## INTRODUCTION

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 San Diego County Sheriff's Department (SDSD) Regional Crime Laboratory (Laboratory) in San Diego, California.

The Federal Bureau of Investigation's (FBI) CODIS is an investigative tool utilizing forensic science and computer technology that is available 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 December 2012 to November 2017. The objectives of our audit were to determine if: (1) the SDSD 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 into 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. We discussed the results of our audit with Laboratory and FBI officials and have included their comments in the report, as applicable. In addition, we received written responses from the Laboratory and FBI, which can be found in Appendices 3 and 4, respectively. Our analysis of those responses and the summary of action necessary to close the report are found in Appendix 5.

[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.

## 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]

*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

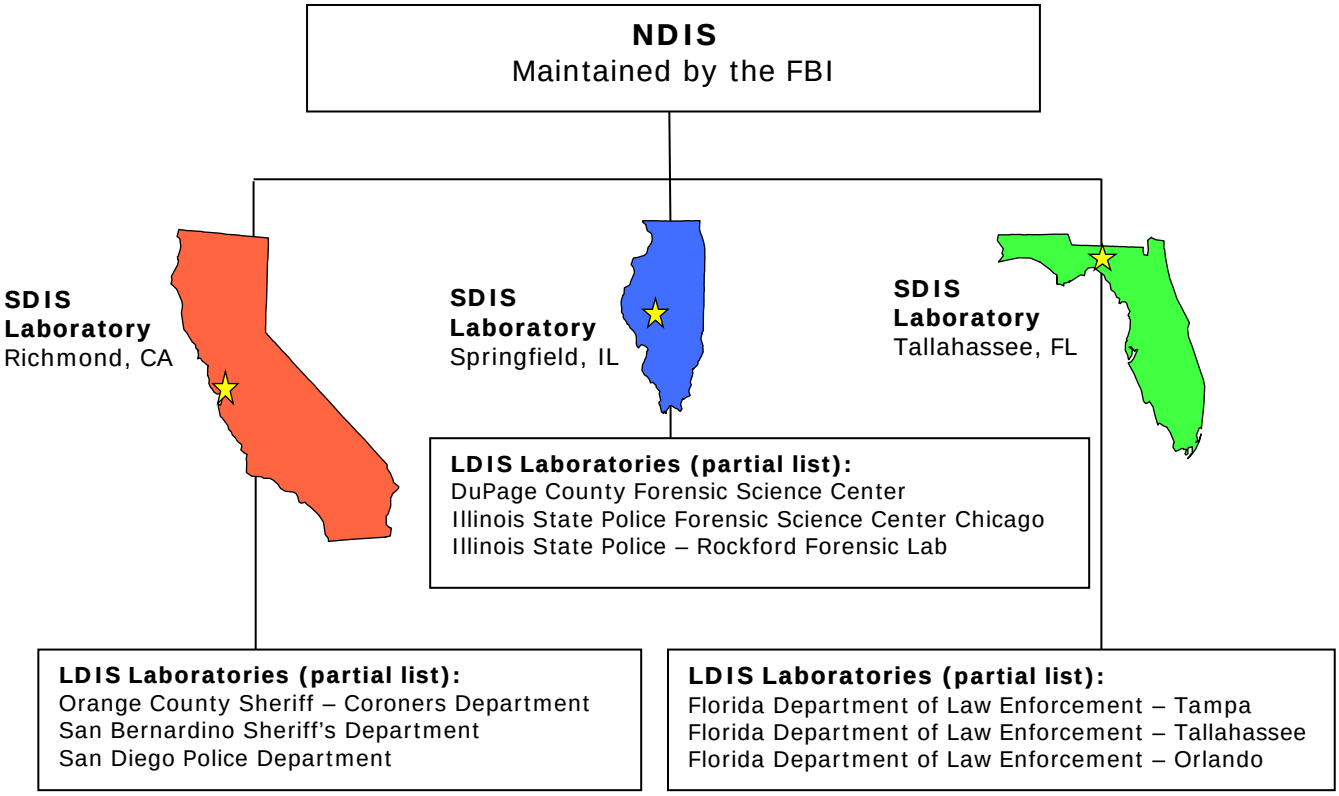
The FBI implemented CODIS as a distributed database with hierarchical levels that enables federal, state, and local crime laboratories to compare DNA profiles electronically. CODIS consists of a hierarchy of three distinct levels: (1) NDIS, managed by the FBI as the nation's DNA database containing DNA 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

[2] 42 U.S.C.A. § 14132 (2006).

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.

**Figure 1**

**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.

[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.

- 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.
- 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 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, missing or unidentified 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 result from a DNA analysis and may not be searched in 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 SDSD Laboratory provides services to 34 law enforcement and criminal justice agencies, including the SDSD with its 21 stations, as well as federal, state, and local law enforcement agencies. In total, the Laboratory serves a population size of approximately 3 million people within San Diego County. The Laboratory participates in the CODIS program as an LDIS Laboratory and began analyzing DNA using short tandem repeat (STR) in 2000, and began processing evidence in criminal cases and uploading forensic profiles into NDIS in 2003. In April 2014 the Laboratory was accredited for 5 years by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). Thus, the Laboratory's accreditation will be up for renewal in April 2019.[6]

---

[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.

[6] The NDIS Operational Procedures Manual, effective January 2017 notes that ASCLD/LAB and Forensic Quality Services, both separately approved as accrediting agencies, are now part of ANSI-ASQ National Accreditation Board (ANAB).

# AUDIT RESULTS

## Compliance with Select NDIS Operational Procedures

The NDIS Operational Procedures Manual, which includes the NDIS Laboratories Participation Requirements, establishes 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 fully comply with the NDIS Security Requirements that require controlled access to its laboratory facility and related assets. Specifically, as of February 2018, we found that the Laboratory did not deactivate the keycards for six of the Laboratory's former employees and contractors upon completion of their work at the Laboratory or separation from the SDSD. We also found one keycard had been returned timely but had not been deactivated in a timely manner. As a result, the keycard was used by another authorized employee to gain access to areas of the Laboratory. We also found that the Laboratory did not have adequate internal controls in place to protect against unauthorized personnel gaining access to DNA data and records. The results of our audit are described in more detail below.

*Inadequate Physical Security to the Laboratory*

The FBI is responsible for the physical security of NDIS, while NDIS participating laboratories are required to adequately secure CODIS servers and clients. The main public entrance to the Laboratory building was accessible to the public during regular business hours, but required a keycard for entry after-hours and on the weekends. All other entrances to the building were locked and secured, and required a keycard to obtain access. We requested a tour of the Laboratory, during which we observed security cameras mounted around the outside of the building, and the CODIS Administrator stated that the building had an alarm system that was activated after-hours and on the weekends. The building's main public entrance led to a waiting room where visitors could check in, receive a visitor's badge, and wait for Laboratory officials to escort them into the building.

The CODIS Administrator stated that within the building, personnel were required to swipe their keycards to gain access to restricted areas. We observed, from the main public entrance, that all Laboratory personnel could access the main hallway of the building, which led to areas such as forensic biology, firearms, and latent prints. To further enter these restricted areas, additional keycard access was required. During our visit and tour we asked the CODIS Administrator how many

staff members had physical access to the main hallway and we were provided with an access list of 214 active keycards that had such access.[7]

Former Employees and Contractors with Active Keycards

The NDIS Security Requirements state that the NDIS participating laboratory is responsible for providing adequate physical security for the CODIS servers and clients against any unauthorized personnel gaining access to the computer equipment or to any of the stored data. In addition, NDIS Security Requirements state that all exterior entrance and exit points require security controls and that the distribution of all keys and combinations shall be documented and limited to the personnel designated by laboratory management. Further, according to the Laboratory's Quality Manual, employees are required to return proximity keycards to the Laboratory when their employment at the Laboratory ends.[8]

We judgmentally selected a sample of 16 keycards that belonged to a combination of employees and contractors from the Laboratory's keycard access list to determine if the list was accurate and up-to-date.[9] We found that the Laboratory's list was neither accurate, nor up-to-date, because the Laboratory had failed to properly collect and deactivate keycards for six of these individuals when they ceased employment with the SDSD or upon completion of their work at the Laboratory. The Laboratory could not confirm that it had retrieved the keycards from the former employees and contractors. Therefore, it was possible that the former employees and contractors may not have turned in their keycards upon their departure from the Laboratory.

As shown in Table 1, 6 of the 16 selected keycards were active and provided access to the forensic biology section of the Laboratory as of February 2018. The six keycards had been active for at least 8 years after the associated individuals no longer required keycard access to the Laboratory; the most egregious example was a keycard that remained active approximately 14 years after the contractor no longer required access to the Laboratory. When we inquired about these active keycards, the Security Supervisor deactivated the cards and provided evidence that the keycards were not used to access areas of the Laboratory after the employees and contractors no longer required access to the Laboratory.

[7] The Laboratory's access list of 214 active keycards included 190 proximity keycards assigned to employees and contractors, and 24 keycards that were designated as spare or to be available in case of an emergency.

[8] Proximity keycards are issued to authorized personnel only. The cards, which are programmable, operate electronic card readers. Successful activation of a card reader releases a lock on the adjoining door, allowing the cardholder to open the door.

[9] The San Diego County Sheriff's Department employs both full-time permanent employees and persons or companies that perform work on a contract basis.

**Table 1**

**Former SDSD Employees and Contractors with Active Keycards**
**As of February 2018**

| Former SDSD Employee and Contractor Count | Date Keycard was Last Used[b] | Date the Keycard was Deactivated | Length of Time to Deactivate Keycards |
|---|---|---|---|
| 1 | 06/14/04 | 02/06/18 | 14 years |
| 2 | 11/21/05 | 02/06/18 | 12 years |
| 3 | 11/02/06 | 02/06/18 | 11 years |
| 4 | 02/07/07 | 02/06/18 | 11 years |
| 5 | 04/06/09 | 02/06/18 | 9 years |
| 6 | 08/31/09 | 02/06/18 | 8 years |

Source: SDSD Laboratory

We asked the Laboratory's Security Supervisor if the individuals' keycards were collected to be deactivated upon completion of their work at the Laboratory or when their employment with the SDSD had ceased. The Security Supervisor stated that his predecessor most likely failed to collect the keycards, which would explain why the six individuals' keycards were still active. We believe that if there were periodic reviews of the Laboratory's keycard access list, someone would have noticed that there were former employees and contractors included on the list.

In addition to the six employees mentioned above, we determined that one of the remaining 10 keycards was returned by a former employee in a timely manner upon departing from the Laboratory, but was not immediately deactivated and was used by another employee to access areas of the Laboratory. We asked the Security Supervisor why the former employee's keycard had not been deactivated and the Security Supervisor stated that the keycard was returned to a Senior Office Assistant, who did not immediately provide the keycard for deactivation. Rather, the Senior Office Assistant used the keycard to access areas of the Laboratory when she left her own keycard at home. Upon our inquiry, the keycard was deactivated, 111 days after the employee's departure from the SDSD. The remaining nine employees in our sample either worked at the Laboratory at the time of our audit with keycard access that was appropriate in order to perform their job responsibilities, or were former employees whose keycards had been deactivated.

By failing to maintain an up-to-date list of individuals who had been provided keycards, the Laboratory was not retrieving and deactivating keycards of former personnel as required by both the Laboratory and NDIS requirements. This created a heightened risk of improper access to privacy information and evidence by unauthorized individuals, as well as compromising the chain of custody of the evidence. In addition, the security of the Laboratory was put at risk. Therefore, we recommend that the FBI work with the Laboratory to ensure that it implements the required physical access controls to properly track and maintain its distribution of

keycards to ensure that all former employees' and contractors' keycards have been retrieved and deactivated in a timely manner. We also recommend that the FBI ensure that the Laboratory review its keycard distribution list to confirm that all individuals have appropriate access and that all former employees' and contractors' keycards have been deactivated.

*DNA Records and Data*

According to NDIS Security Requirements and the Operational Procedures Manual, the NDIS participating laboratory shall ensure that it has adequate physical security measures in place to protect against unauthorized personnel gaining access to DNA samples or any DNA data. Also, the NDIS participating laboratory shall not provide access to or disclosure of DNA records that have been uploaded to CODIS to an agency that is not a criminal justice agency or authorized to access such DNA records under the Federal DNA Act. During our site visit, while taking a tour of the Laboratory facility, we observed that at least one, if not more, of the Laboratory's CODIS specimen reports was left in an unsecured mailbox in the main hallway of the Laboratory that was accessible to all of the Laboratory's employees and visitors, many of whom may not have a need to access such a report. When we asked why the specimen report was left there, the CODIS Administrator stated that the Laboratory's CODIS users have a practice of leaving specimen reports that they are working on in the mailbox in the main hallway where the CODIS Administrator could pick them up later and review them prior to uploading the forensic profiles into CODIS. The CODIS Administrator went on to say that access to the Laboratory was limited to only authorized personnel. Although access to the Laboratory is limited to authorized personnel, not all authorized personnel have a need to access specimen reports, especially if certain personnel are not connected to the DNA analysis of forensic profiles. The specimen reports contain personally identifiable information and according to NDIS requirements, access to DNA data, such as specimen reports, should be secured and accessible only to those Laboratory employees needing such access. Further, based on the other security risks we identified, including active keycards being held by former employees and contractors, the Laboratory was at an increased risk of unauthorized access to and potential mishandling of personally identifiable information and evidence. During our exit conference with the Laboratory, a Laboratory official stated that the Laboratory generally allows all authorized Laboratory employees to have access to all reports and there was no concern on the part of the Laboratory with leaving specimen reports in the main hallway. During our exit conference with the FBI, an FBI official stated that access to specimen reports should be restricted to personnel that are involved in analyzing the DNA data or have a need to know about the information contained in the specimen reports. Therefore, we recommend that the FBI work with the Laboratory to align its policies, procedures, and practices with NDIS requirements regarding physical security measures over DNA records and data.

We found that the Laboratory complied with the other NDIS operational procedures we reviewed, as described below.

- According to the NDIS Security Requirements, participating laboratories are required to provide adequate physical security for the CODIS server and clients against any unauthorized personnel gaining access to the computer equipment or to any of the stored data. Placing a CODIS server or a client in a common data center may be permitted as long as the data center is located within the criminal justice agency and the server or client is physically secure. During a walk-through tour of the Laboratory, we observed that the CODIS server and clients were physically safeguarded from unauthorized personnel gaining access to the computer equipment or to any of the store data.
- The NDIS participating laboratory is required to ensure that each CODIS user has a CODIS user account, including an individual username and password to log-in to the client containing the CODIS software.[10] In addition, the NDIS participating laboratory is required to ensure that all CODIS servers and clients' screens are set to lock after 10 minutes of inactivity and require a CODIS user's password to unlock the screen. We judgmentally selected 3 of the Laboratory's 16 CODIS users and asked if they had their own CODIS user account. We verified that all three CODIS users had their own unique CODIS username and password and that the Laboratory's clients locked after 10 minutes of inactivity.
- CODIS users are required to be notified of and provided access to revised NDIS Operational Procedures and other documentation necessary to properly participate in NDIS. We judgmentally selected 3 of the Laboratory's 16 CODIS users and asked if they were aware of the NDIS procedures and knew how to access them. All three CODIS users stated that they were aware of the NDIS procedures and could access the procedures on the FBI's Criminal Justice Information System-Shared Enterprise Network.
- For each CODIS user, the FBI requires that a participating laboratory submit fingerprint cards, background information, CODIS user information, and other appropriate documentation to the FBI. We verified that all necessary documents were provided to the FBI for each of its 16 CODIS users, 4 CODIS SEN users, and 3 information technology CODIS users.
- CODIS users are required to annually complete the FBI's Annual Review of DNA Data Accepted at NDIS training. The FBI provided us a list of Laboratory personnel who had completed this mandatory annual training. We judgmentally selected five CODIS users and determined that each had

[10] A CODIS user is a government employee who: (1) has login access to the CODIS system and is authorized to read, add, modify, or delete DNA records in CODIS; or (2) is a qualified DNA analyst responsible for producing the DNA profiles stored in NDIS. There are three additional categories of CODIS users that are required to be cleared at NDIS, although they are not authorized to add, modify, or delete DNA records in CODIS: (1) CODIS Contract user; (2) CODIS Information Technology (IT) user; and (3) CODIS Shared Enterprise Network (SEN) user. A CODIS user, CODIS IT user and CODIS SEN user must undergo an FBI security check and maintain a security clearance.

successfully completed the FBI's Annual Review of DNA Data Accepted at NDIS training for 2015, 2016, and 2017.

- The NDIS's Confirmation and Hit Dispositioning Operational Procedures provides guidance for participating laboratories to follow when confirming matches that are identified in the CODIS system. We reviewed a sample of nine NDIS matches and determined that:
    - The Laboratory sent confirmation requests in a timely manner for all nine matches;
    - Confirmation generally took place within 30 days after the originating laboratory's request was sent out; and
    - The Laboratory notified investigators of match confirmation within 10 days for all nine matches.

## Compliance with Certain Quality Assurance Standards

During our audit, we considered the Forensic QAS issued by the FBI.[11] These standards describe the quality assurance requirements that the Laboratory must follow to ensure that the data it produces meets the required level of quality and integrity. We also assessed the two most recent QAS reviews that the Laboratory underwent.[12] The QAS that we utilized in our audit are listed in Appendix 2 of this report.

We found that security at the Laboratory did not fully meet the QAS standards that outline controlled access to the Laboratory. Specifically, we found that the Laboratory's distribution list of keycards was inaccurate and not up-to-date as required by the FBI. We also found that the Laboratory had not properly secured evidence at the end of a work day as required by the Laboratory. The results of our audit are described in more detail below.

*Internal and External QAS Reviews*

NDIS participating laboratories are required to undergo annual internal reviews and biennial external reviews using the FBI's QAS review document. QAS Standard 6 of the FBI's QAS review guidance document asks if access to the laboratory was controlled and limited in a manner that prevents access by unauthorized personnel, and whether the distribution of all keys and combinations are documented and limited to personnel designated by laboratory management. We found that on both the Laboratory's 2016 external review and 2017 internal

[11] Forensic QAS refers to the Quality Assurance Standards for Forensic DNA Testing Laboratories, effective September 1, 2011.

[12] The QAS requires that laboratories undergo annual audits. Every other year, the QAS requires that the audit be performed by an audit team of qualified auditors from an external agency. These audits are not required by the QAS to be performed in accordance with the *Government Auditing Standards* and are not performed by the Department of Justice Office of the Inspector General. Therefore, in this report, we 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 the *Government Auditing Standards*.

review that the reviewers marked "yes" and did not note any deficiencies. In the review document's discussion section, it states that to successfully satisfy Standard 6, the laboratory must demonstrate compliance with all of the subcategories, which includes limiting access to internal controlled areas to only authorized personnel, and ensuring that the distribution system of all keys and combinations are current, accurate, clearly documented, and available for review. Based on our review, the Laboratory's keycard distribution list was outdated and inaccurate as we found former employees and contractors had active keycards far past the completion of their work or their separation date with the SDSD. In fact, the Laboratory was unable to confirm that it retrieved keycards from six individuals and those keycards remained active between 8 to 14 years after the individuals no longer required access to the Laboratory. In a separate incident, a Laboratory employee retrieved a keycard from a former employee, but the Laboratory did not deactivate the keycard until months later when we began our audit and inquired into the Laboratory's keycard access system. In reviewing these matters, we noted that the Laboratory does not have any policy or procedures in place requiring periodic review of the accuracy of its keycard distribution list. We believe that the Laboratory should establish such policy or procedures to ensure that it maintains an up-to-date and accurate keycard distribution list, paying special attention to the Laboratory's adherence to QAS Standard 6.

We recommend that the FBI work with the Laboratory to ensure that it strengthens its annual QAS compliance reviews to include verifying that the Laboratory's keycard distribution list is current and accurate.

*Safeguarding Evidence*

According to FBI's QAS for Forensic Testing Laboratories, the Laboratory is required to have and follow documented procedures designed to minimize loss, contamination, and deleterious change of evidence and work product in progress. Also, the Laboratory is required to have secure, controlled access areas for evidence storage and work product in progress. We found that the Laboratory used an electronic system called Liberty Sentinel to track and document the chain of custody over evidence maintained by the Laboratory. Law enforcement officers drop off evidence at the Laboratory's Property and Evidence Unit, where it is checked in, given a unique bar code identification number in Liberty Sentinel, and secured in the unit. Each time a DNA analyst requests evidence from the Property and Evidence Unit, the DNA analyst is required to sign an evidence check-out release form and Property and Evidence personnel scan the bar code on the evidence's identification tag to update the location of the evidence in Liberty Sentinel, documenting the chain of custody.

According to the Laboratory's Quality Manual, each DNA analyst is responsible for ensuring the integrity of the evidence that they check out and for storing any evidence in their assigned storage cabinets or refrigerators at the end of each day. Bulky or larger evidence items that do not fit into storage cabinets may be stored overnight in a locked examination or storage room. During our facility walkthrough, we noted a package containing evidence on a DNA analyst's workspace, however the DNA analyst was not in the Laboratory. The evidence had

been placed in a bag and the top of the bag had been folded over. When we asked the CODIS Administrator about the whereabouts of the analyst, he stated that the analyst was not working at the Laboratory that day. However, when we asked the CODIS Administrator about the evidence package, he stated that the employee might return to the Laboratory later that day. The CODIS Administrator stated that the DNA analyst who left evidence unsecured at their workspace did not have a personal storage cabinet. The Laboratory should ensure that its DNA analysts have the means by which to adhere to Laboratory policy for securing evidence in storage cabinets at the end of each day, to minimize the risk of contamination and loss. Therefore, we recommend that the FBI ensure that the Laboratory adheres to its policy that evidence be stored in assigned storage cabinets or refrigerators at the end of each day.

We found that the Laboratory complied with the other QAS we tested, as described below.

- The QAS requires laboratories to undergo an annual review, including an external review every 2 years. Between calendar years 2016 and 2017, the Laboratory had an external QAS review performed in November 2016 and an internal QAS review performed in August 2017, in accordance with the FBI's requirement.
- We reviewed the Laboratory's most recent QAS review reports. Both the external and internal reviews were conducted using the FBI's QAS Review Document. In addition, the FBI confirmed that at least one of the QAS reviewers for both reviews had successfully completed the FBI's QAS review training course.
    - The external QAS review conducted in November 2016 noted no findings for the Laboratory.
    - The internal QAS review conducted in August 2017 noted no findings for the Laboratory.
- The QAS requires that an external quality assurance review be forwarded to the FBI within 30 days of the participating laboratory's receipt of the report. Based on our review of the Laboratory's November 2016 external QAS review, the report was submitted to the FBI's NDIS Custodian within 30 days. We also determined that each of the QAS reviewers who conducted the external QAS review had completed the auditor's self-certification worksheet and indicated that there were no impairments to their independence.
- The QAS requires amplified DNA to be generated, processed, and stored in a room separate from evidence examination, DNA extraction, and polymerase chain reaction (PCR) setup areas. We observed that the Laboratory had separate areas for DNA examination and extraction, PCR setup, and DNA amplification. The Laboratory was physically separated into pre-PCR and post-PCR areas, and during our site visits we observed that the doors between the rooms remained closed and evidence flowed one-way to avoid amplified DNA from being introduced into pre-PCR areas of the Laboratory.

We also observed designated laboratory coats (distinguished by color) were used in the pre- and post-amplification rooms to prevent contamination.

## 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. 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 2,461 forensic DNA profiles the Laboratory had uploaded to NDIS as of November 2017. We found that all profiles reviewed were complete, accurate, and allowable for inclusion in NDIS. However, we were only able to conclude that all profiles were allowable for inclusion in NDIS after obtaining additional information that was not maintained in the case files for 17 of the 100 profiles we reviewed.

### *Lack of Documentation in its Case Files*

According to the FBI's NDIS Operational Procedures Manual, only CODIS eligible profiles may be uploaded to NDIS. To determine whether a forensic DNA profile is eligible for NDIS, a DNA analyst must have enough information to determine that a crime was committed, the type of crime that occurred, and that the evidence being analyzed was attributable to a putative perpetrator. DNA analysts we interviewed stated that supervising criminalists perform a cursory review of each case file (including a review for CODIS eligibility) prior to assigning casework to each DNA analyst at the Laboratory. Once the DNA analyst has been assigned a case, the analyst can utilize the SDSD's regional law enforcement records management system, called NETRMS, to review law enforcement's investigative notes on the case to assist in determining CODIS eligibility. DNA analysts also ask the CODIS Administrator if they have questions about determining CODIS eligibility for a forensic DNA profile.

We found that the case files for 17 of the 100 sampled forensic DNA profiles lacked sufficient information for us to determine whether a profile was eligible for CODIS. Although DNA analysts at the Laboratory stated that they had reviewed information in NETRMS when determining CODIS eligibility, evidence of those reviews were not maintained in the Laboratory's case files. The CODIS Administrator was able to obtain the investigative notes from NETRMS for 15 of the profiles. During our exit conference with the Laboratory, a Laboratory official stated that the information stored in NETRMS is an extension of the Laboratory's case files and that information in NETRMS is not printed out and placed into the Laboratory's hardcopy case files. During our exit conference with the FBI, an FBI official stated that the case file must contain evidence of the review for CODIS eligibility, such as the date NETRMS was accessed to determine CODIS eligibility or a print out of the information reviewed in NETRMS to determine CODIS eligibility being added to the case file. Additionally, an FBI official stated that if a Laboratory is not in control of who can alter or delete information in the electronic database being used for determining CODIS eligibility, then that information should be maintained outside of the database, such as in a case file. For the remaining two profiles, the CODIS Administrator reached out to law enforcement personnel and obtained additional information regarding each profile. Based on the information obtained, we were able to determine that each of the 17 forensic DNA profiles were eligible for upload into NDIS. However, without sufficient documentation within each case file, the Laboratory could not ensure that another qualified individual could arrive at the same conclusion for determining CODIS eligibility when reviewing the case file, as required by the FBI. Therefore, we recommend that the FBI work with the Laboratory to ensure that all case files contain sufficient information in order to determine CODIS eligibility.

## CONCLUSION AND RECOMMENDATIONS

We identified a number of issues with the Laboratory's security and implementation of NDIS Procedures. Specifically, we found that the Laboratory failed to retrieve and deactivate keycards from six former employees and contractors after they no longer required access to the Laboratory. In addition, another former employee's keycard that was retrieved was not deactivated until months after the employee had left the employment of the Laboratory and after we began our audit and review of the Laboratory's keycard access system. This allowed another employee to use the former employee's keycard to gain access to areas of the Laboratory on at least one occasion. As a result, we found that the Laboratory's keycard distribution list was not current, as required by the FBI's NDIS Security Requirements. We also identified an instance where the Laboratory did not properly secure evidence at the end of the day, as required by the Laboratory's policies.

Moreover, based on our testing of 100 forensic DNA profiles that had been uploaded to NDIS, we determined that the Laboratory's case files for 17 forensic profiles lacked sufficient information to determine CODIS eligibility. However, after our inquiries, the Laboratory was subsequently able to obtain enough additional information to support each of the 17 forensic DNA profile's CODIS eligibility. We determined that all of the forensic DNA profiles in our sample were complete, accurate, and allowable for inclusion in NDIS.

We recommend that the FBI:

1. Work with the Laboratory to ensure that it implements the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employees' and contractors' keycards have been retrieved and deactivated in a timely manner.

2. Ensure that the Laboratory reviews its keycard distribution list to confirm that all individuals have appropriate access and that all former employees' and contractors' keycards have been deactivated.

3. Work with the Laboratory to align its policies, procedures, and practices with NDIS requirements regarding physical security measures over DNA records and data.

4. Work with the Laboratory to ensure that it strengthens its annual QAS compliance reviews to include verifying that the Laboratory's keycard distribution list is current and accurate.[13]

5. Ensure that the Laboratory adheres to its policy that evidence be stored in assigned storage cabinets or refrigerators at the end of each day.

[13] We revised this recommendation based on additional information we received from the FBI after our draft audit report was issued, as discussed in Appendix 5.

6. Work with the Laboratory to ensure that all case files contain sufficient information in order to determine CODIS eligibility.

## APPENDIX 1

# OBJECTIVES, SCOPE, AND METHODOLOGY

### Objectives

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.

### 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 December 2012 through November 2017. 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.

- Reviewed the Laboratory's written policies and procedures related to conducting internal reviews, resolving review findings, expunging DNA profiles from NDIS, and resolving matches among DNA profiles in NDIS.
- Reviewed supporting documentation for 9 of 89 NDIS matches to determine whether they were resolved in a timely manner. The Laboratory provided the universe of NDIS matches as of December 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 2,461 searchable forensic profiles the Laboratory had uploaded to NDIS between December 1, 2012, and November 30, 2017. We limited our review to a sample of 100 profiles. This sample size was determined judgmentally because preliminary audit work determined that risk was not unacceptably high.
- 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 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.

## APPENDIX 2

# 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 Procedure
- NDIS Confirmation and Hit Dispositioning Procedure
- 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 and Offender QAS 9.5): 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 ae reasonable and within the constraints of scientific knowledge.
- [Reviews] (Forensic QAS and Offender QAS 15.1 and 15.2): 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.
- 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.

## APPENDIX 3

## LABORATORY'S RESPONSE TO THE DRAFT AUDIT REPORT

**San Diego County Sheriff's Department**

Post Office Box 939062 • San Diego, California 92193-9062

***William D. Gore, Sheriff***

July 18, 2018

David J. Gaschke, Regional Audit Manager
U.S. Department of Justice
Office of the Inspector General
San Francisco Regional Audit Office
90 7th Street, Suite 3-100
San Francisco, CA 94103

Dear Mr. Gaschke,

I received the draft report on the Audit of Compliance with Standards Governing Combined DNA Index System Activities for our San Diego County Sheriff's Regional Crime Laboratory. This is our official response to the draft report.

There were six areas where your team expressed concerns:

1."The Laboratory did not adequately limit and control access to its laboratory facility as required by NDIS Security Requirements. We found that the Laboratory did not deactivate keycards for six former employees and contractors upon completion of their work at the Laboratory or separation from the SDSD. Instead, these keycards were active between 8 to 14 years after the keycards should have been collected and deactivated. Further, the Laboratory could not confirm that it retrieved the former employees' and contractors keycards. We also found that an additional former employee turned in their keycard upon their separation, but that keycard was not deactivated for 111 days, which allowed another authorized employee to use the former employee's card to gain access to the Laboratory's restricted areas."

RESPONSE:

We agree. We will be moving out of the current laboratory building effective August 8, 2018. Any keycards to this building will be of no significance after that date. We will track keycards for the new laboratory building and we will establish a new policy for an annual review of access records and the keycard distribution list. By August 13, 2018 the new policy will be established and in place. We will share that policy with you when it is finalized.

*Keeping the Peace Since 1850*

2."We also found that the Laboratory did not provide adequate physical security for its DNA data and records."

RESPONSE:

We disagree with the statement that we do not provide adequate physical security for DNA data and records, as we occupy a secure facility that is not accessible to the public and our own employees are backgrounded and ethics-trained. DNA reports including CODIS information are transferred from one analyst to another for technical review or for administrative review through the use of mailboxes in the laboratory hallway outside the management offices.

If "adequate physical security" includes restricting access by crime laboratory employees outside the Forensic Biology Unit, we propose a solution: we will maintain the CODIS information worksheet as a digital file on a server accessible only the Forensic Biology Unit, rather than on a page or pages in the case file. The case packet review checklist will be in the case file, will not bear the actual CODIS data but will refer back to the appropriate electronic file where that CODIS data may be found. The case packet review checklist will be signed by the analyst, technical reviewer and CODIS reviewer and those signatures will signify that they have reviewed the electronic CODIS information worksheet. We will develop a policy to be added to the Forensic Biology Unit Manual along those lines and will forward a copy of that policy to you when it is finalized.

3."The Laboratory's distribution list of keycards was inaccurate."

RESPONSE:

We agree. With the move to the new laboratory building effective August 8, 2018, a new keycard list will be generated, and an annual review of access records and the keycard list will be implemented. We will occupy the new laboratory building and the policy for review of the keycard distribution list and access records will be in place by August 13, 2018.

4."We found eight DNA forensic profiles where the separate concordant review was performed by the same individual that conducted the initial review."

RESPONSE:

We disagree. The initial assessment is performed by the analyst who conducted the work and will be authoring the report. The analyst is responsible for determining the eligibility of a sample for CODIS, the appropriate DNA types for entry into CODIS, and the appropriate specimen category. All of this information is captured in our CODIS sample information worksheet which (currently) is initialed and dated by the analyst. The second assessment is by a technical reviewer. The technical reviewer reviews all of this information and then (currently) signs the worksheet to document their assessment. The author of the report (the analyst) and the technical reviewer are never the same person so this constitutes two independent assessments.

We perform an additional assessment which we designate a "CODIS review" when a profile is to be uploaded to CODIS. Our CODIS review is an additional step we take to ensure that we further maintain and control the quality of the samples we put into CODIS.

Going forward, the CODIS sample information worksheet will be maintained electronically, and the reviews of this worksheet will be documented by signatures on the case packet review checklist.

---

5."We noted that some evidence was left unsecured in the Laboratory. By not securing evidence in storage cabinets, whenever possible, the Laboratory increases its risk of contamination and loss."

RESPONSE:

We agree that whenever possible (based on the size of the item), the analyst should make use of a short term evidence locker if that analyst is going to be gone for the day. All Forensic Biology staff members have access to a short term evidence locker.

The laboratory's Quality Manual states:

"If stored during processing and analysis, an evidence package should be kept closed, but does not need to be sealed. For example, a paper bag may be folded over to protect the evidence. If an examiner needs to leave for a short period of time, such as for lunch, the evidence does not need to be repackaged if it is in a secure area, but needs to be protected from possible contamination and loss of evidence. Analysts may have access to temporary overnight storage lockers for evidence that is being examined. Analysts

are responsible for storing their evidence in a way that reduces the risk of evidence loss, cross-transfer contamination, or other deleterious change. An individual laboratory section may develop storage policies appropriate for that section's particular evidence storage needs."

The policy in the Forensic Biology Unit Manual currently states:

"All attempts shall be made to maintain the integrity of the evidence while in analysts' possession. Analysts are responsible for selecting and maintaining appropriate storage conditions for evidence in their custody." We will change this Forensic Biology Unit Manual policy to specify that evidence left unattended between shifts must be secured in a short term evidence locker, if size permits. We will share that policy with you when it is finalized.

---

6. "We found that 17 forensic profiles in our sample lacked adequate information in their respective case files to enable us to determine their CODIS eligibility." (Additional information was provided by the Laboratory to support CODIS eligibility for these profiles.)

RESPONSE:

We agree. Effective July 18, 2018, we will ensure that notes in the case file by the analyst, supervisor or CODIS Administrator clearly support the CODIS eligibility of a profile.

We are pleased that the audit found that all 100 profiles they chose to review were in fact CODIS eligible.

Sincerely,

Michael J. Grubb
Crime Laboratory Director

cc: Jesse Carver, CODIS Administrator
Paula Pagano, FBI CODIS Unit

## APPENDIX 4

# FBI'S RESPONSE TO THE DRAFT AUDIT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

July 26, 2018

David J. Gaschke, Regional Audit Manager
San Francisco Regional Audit Office
Office of the Inspector General
90 7th Street, Suite 3-100
San Francisco, CA 94103

Dear Mr. Gaschke:

Your memorandum to Director Wray forwarding the draft audit report for the San Diego County Sheriff's Department Regional Crime Laboratory, San Diego, California ("Laboratory"), has been referred to me for response.

Your draft audit report contained six 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 implementation of a tracking and maintenance system for keycards, the FBI requires that access to the Laboratory shall be controlled and limited in a manner to prevent access by unauthorized personnel. Therefore, the FBI concurs with the recommendation to the Laboratory. The Laboratory is moving to a new facility in a couple of weeks. At that time, all personnel will receive new keycards for access and all keycards for its current facility will be deactivated. Upon occupying the new facility, the Laboratory will implement a procedure to document, track, and review its distribution of keycards to ensure access to the facility is limited to the personnel designated by laboratory management. The FBI will continue to work with the Laboratory as it develops the procedure.

With respect to recommendation two relating to the review of the keycard distribution list and deactivation of any nonessential keycards, the FBI, as stated above, requires that access to the Laboratory shall be controlled and limited in a manner to prevent access by unauthorized personnel. Therefore, the FBI concurs with the recommendation to the Laboratory. The Laboratory completed its review of its keycard distribution list, has confirmed that all individuals have appropriate access, and all former employees' and contractors' keycards have been deactivated. The FBI CODIS Unit supports closure of this recommendation.

With respect to recommendation three relating to the physical security of DNA records and data, the FBI requires that the Laboratory follow procedures to ensure the privacy of DNA records and data. Therefore, the FBI concurs with the recommendation to the Laboratory. The Laboratory is in the process of implementing a procedure to digitalize portions of its DNA records/data and maintain it on a secure server with limited access so that information is no longer in its case files. The Laboratory will continue to use its current mailbox system, however, no reports or other private information will be visible by those that pass by. The FBI will continue to work with the Laboratory as it develops a mutually acceptable procedure.

With respect to recommendation four relating to the verification of accurate keycard distribution lists and concordant reviews of DNA profiles for CODIS eligibility prior to upload, the FBI requires that the Laboratory prevents access by unauthorized personnel and that appropriate concordant assessments for CODIS eligibility are conducted. Therefore, the FBI concurs with the recommendation to the Laboratory as to the accurate keycard distribution list issue but it does not agree with the conclusion that the Laboratory did not follow the Quality Assurance Standards regarding concordant assessments for the verification of CODIS eligibility and DNA record information. The FBI is working with the Laboratory relating to its keycard issues. However, the FBI has reviewed the Laboratory's process for verification of CODIS eligibility, DNA types and specimen category for its DNA profiles and has determined that the Laboratory is providing appropriately, two concordant assessments by a qualified analyst or technical reviewer.

With respect to recommendation five relating to evidence storage, the FBI requires that the Laboratory have secure, controlled access areas for evidence storage and work product in progress to minimize loss, contamination, and/or deleterious change. Therefore, the FBI concurs with the recommendation to the Laboratory. The FBI will work with the Laboratory to develop and implement an acceptable method to convey to its staff the importance of utilizing its short term evidence storage area when away for an extended period.

With respect to recommendation six relating to maintaining the appropriate documentation to support CODIS eligibility, the FBI requires that information that supports eligibility must be accessible. Therefore, the FBI concurs with the recommendation to the Laboratory. The Laboratory has implemented a process to ensure that CODIS eligibility is documented in its case files. The FBI will work with the Laboratory to verify that the new process has been implemented and the staff is fully aware of its responsibility.

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

## APPENDIX 5

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

The OIG provided a draft of this audit report to the San Diego County Sheriff's Department Regional Crime Laboratory (Laboratory) and the Federal Bureau of Investigation (FBI) for review and official comment. The Laboratory's response is included in Appendix 3 and the FBI's response is included as Appendix 4 of this final report. The FBI agreed with five recommendations contained in this report and disagreed, in part, with one recommendation. As a result, 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 implements the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employees' and contractors' keycards have been retrieved and deactivated in a timely manner.**

   Resolved. The FBI concurred with our recommendation and stated that the Laboratory is moving to a new facility in August 2018. The FBI stated that upon occupying the new facility, the Laboratory will implement a procedure to document, track, and review its distribution of keycards to ensure access to the facility is limited to personnel designated by laboratory management. The FBI stated that it will continue to work with the Laboratory as it develops the procedure.

   Although the Laboratory did not state whether it agreed or disagreed with our recommendation, the Laboratory did state in its response that it agreed that the Laboratory did not adequately limit and control access to its laboratory facility as required by NDIS Security Requirements. The Laboratory stated in its response that it is moving to a new facility on August 8, 2018, and any keycards to its current building will be of no significance after that date. The Laboratory also stated that it will track keycards for its new facility and that it will establish a new policy for an annual review of access records and its keycard distribution list. The Laboratory stated that the new policy will be established and in place by August 13, 2018.

   This recommendation can be closed when we receive evidence that the Laboratory has implemented the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employees' and contractors' keycards have been retrieved and deactivated in a timely manner.

**2. Ensure that the Laboratory reviews its keycard distribution list to confirm that all individuals have appropriate access and that all former employees' and contractors' keycards have been deactivated.**

Resolved. The FBI concurred with our recommendation and stated that the Laboratory has completed its review of its keycard distribution list, has confirmed that all individuals have appropriate access, and that all former employees' and contractors' keycards have been deactivated. The FBI stated that it supports closure of this recommendation, however it did not provide evidence that the laboratory has completed its review and former employee and contractor keycards have been deactivated.

Although the Laboratory did not state whether it agreed or disagreed with our recommendation, the Laboratory did state in its response that it agreed that the Laboratory's distribution list of keycards was inaccurate. The Laboratory stated in its response that the crime laboratory is moving to a new facility on August 8, 2018, and that a new keycard list will be generated and an annual review of access records and its keycard distribution list will be implemented. The Laboratory stated that the new policy will be in place by August 13, 2018.

This recommendation can be closed when we receive evidence that the Laboratory has reviewed its keycard distribution list to confirm that all individuals have appropriate access and that all former employees' and contractors' keycards have been deactivated.

**3. Work with the Laboratory to align its policies, procedures, and practices with NDIS requirements regarding physical security measures over DNA records and data.**

Resolved. The FBI concurred with our recommendation and stated that the Laboratory is in the process of implementing a procedure to digitalize portions of its DNA records and data, and maintain it on a secure server with limited access so that the information is no longer in its case files. The FBI stated that the Laboratory will continue to use its current mailbox system, however, no reports or other private information will be visible by those that pass by. The FBI stated that it will continue to work with the Laboratory to develop a mutually acceptable procedure.

Although the Laboratory did not state whether it agreed or disagreed with our recommendation, the Laboratory did state in its response that it disagreed with the report statement that, "We also found that the Laboratory did not provide adequate physical security for its DNA data and records." The Laboratory stated that its facility is secure and not accessible to the public and that its employees undergo background checks and receive ethics training. The Laboratory further stated that its DNA reports, including CODIS information, are transferred from one DNA analyst to another for technical review or administrative review through the use of mailboxes located in the main hallway of the Laboratory. As stated in our report, FBI NDIS

Procedures require that only authorized personnel, should have access to such information. Yet we observed that at least one, if not more, of the Laboratory's CODIS specimen reports was left in an unsecured mailbox in the main hallway of the Laboratory that was accessible to all of the Laboratory's employees and visitors, many of whom may not have had a need to access such a report.

The Laboratory stated that if adequate physical security includes restricting access to DNA reports by crime laboratory employees outside the forensic biology unit, then the Laboratory can maintain its CODIS information worksheet as a digital file on a server accessible only to the forensic biology unit, rather than on a page or pages in the case file. The Laboratory stated that the case packet review checklist maintained in the case file, will not include DNA data but will refer back to the appropriate electronic file where that DNA data may be found and the case packet review checklist will be signed by the analyst, the technical reviewer, and the CODIS reviewer. The Laboratory stated that those signatures will signify that the appropriate staff have reviewed the electronic CODIS information worksheet. The Laboratory stated that it will update its Forensic Biology Unit Manual to include this new procedure.

This recommendation can be closed when we receive evidence of the updates to its Forensic Biology Unit Manual to ensure that it is aligned with NDIS requirements regarding physical security measures over DNA records and data.

**4. Work with the Laboratory to ensure that it strengthens its annual QAS compliance reviews to include verifying that the Laboratory's keycard distribution list is current and accurate.**

Resolved. After our draft report was issued, the FBI provided additional information clarifying that the Laboratory's process for reviewing profiles for eligibility in CODIS was performed in accordance with requirements. As a result, we revised this recommendation in this final report. The FBI concurred with this recommendation and stated that it will work with the Laboratory to develop and implement an acceptable method to convey to its staff the importance of utilizing its short term evidence storage area when away for an extended period.

Although the Laboratory did not state whether it agreed or disagreed with our recommendation that it strengthen its annual QAS compliance reviews to include verifying that its keycard distribution list is current and accurate, the Laboratory did state that it agreed that its distribution list of keycards was inaccurate. The Laboratory stated in its response that it is moving to a new facility on August 8, 2018, and that a new keycard list will be generated. The Laboratory further stated that an annual review of access records and its keycard distribution list will be implemented and that it plans to have the new policy in place by August 13, 2018.

This recommendation can be closed when we receive evidence that the Laboratory has strengthened its annual QAS compliance reviews to include verifying that the Laboratory's keycard distribution list is current and accurate.

**5. Ensure that the Laboratory adheres to its policy that evidence be stored in assigned storage cabinets or refrigerators at the end of each day.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the Laboratory to develop and implement an acceptable method to convey to its staff the importance of utilizing its short term evidence storage area when away for an extended period of time.

Although the Laboratory did not state whether it agreed or disagreed with our recommendation, the Laboratory did state in its response that it agreed that its DNA analysts, whenever possible, should make use of a short term evidence locker if that DNA analysts is going to be gone for the day. The Laboratory further stated that all Forensic Biology staff members have access to a short term evidence locker. In addition, the Laboratory provided excerpts from its Quality Manual and Forensic Biology Unit Manual that it found to be applicable.

This recommendation can be closed when we receive evidence that the Laboratory has implemented controls to ensure that it adheres to its policy that evidence be stored in assigned storage cabinets or refrigerators at the end of each day.

**6. Work with the Laboratory to ensure that all case files contain sufficient information in order to determine CODIS eligibility.**

Resolved. The FBI concurred with our recommendation and stated that the Laboratory has implemented a process to ensure that CODIS eligibility is documented in its case files. The FBI will work with the Laboratory to verify that the new process has been implemented and that staff are fully aware of their responsibility to correct this finding.

Although the Laboratory did not state whether it agreed or disagreed with our recommendation, the Laboratory did state in its response that it agreed with the statement in the report that, "We found 17 forensic profiles in our sample lacked adequate information in their respective case files to enable us to determine CODIS eligibility." The Laboratory stated that effective July 18, 2018, it will ensure that notes in the case file clearly support the CODIS eligibility of a DNA profile.

This recommendation can be closed when we receive evidence that the Laboratory has implemented controls to ensure that all case files contain sufficient information in order to determine CODIS eligibility.


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.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

**U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL**
950 Pennsylvania Avenue, Northwest
Suite 4760
Washington, DC 20530-0001

| **Website** | **Twitter** | **YouTube** |
| --- | --- | --- |
| oig.justice.gov | @JusticeOIG | JusticeOIG |

Also at Oversight.gov